LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Political Science

Master's Degree in International Relations – Global Studies

Chair of Security Studies

Cyber security meets diplomacy:
the EU-NATO cooperation and the Italian case

SUPERVISOR

Gen. S.A. Carlo Magrassi

CANDIDATE

Gabriele Pierini

627242

CO-SUPERVISOR

Prof. Marco Mayer

Academic Year 2016/2017

Acknowledgements

The subject of this thesis combines my two greatest passions: international security and diplomacy. A strong europeanist sentiment blended with a genuine national pride made it easy to find an interesting subject that could combine these two sectors. Less easy it has been dissertating on it. For this reason, I would like to warmly thank all of those who supported me in this work.

First of all, I would like to thank my supervisor, General Carlo Magrassi, for the priceless opportunity to combine these two passions into this dissertation. Furthermore, he undoubtedly owns the merit of leading a unique group of assistants who enriched the analysis with interesting ideas and always provided essential support. I therefore wish to thank Doctor Simone Pasquazzi, Colonel Cesario Totaro and, in particular, Colonel Antonio Colella, for always being present and pleasant. I then thank Professor Marco Mayer for having co-supervised this work.

I would also like to thank so much those who have greatly enriched the content of this thesis with their direct experience and consolidated professionalism. First, an excellent representative of the Italian diplomacy: Ambassador Luca Giansanti, Director General for Political and Security Affairs of the Italian Ministry of Foreign Affairs. Then, three excellent representatives of the Italian cyber diplomacy: Minister Plenipotentiary Gianfranco Incarnato, Vice Director General for Political and Security Affairs, Engineer Pierluigi Paganini and Doctor Luigi Martino, all members of the 2017 G7 Cyber Group.

Finally, I have to credit this thesis to the years of study I have spent both in my country and abroad, to the extracurricular projects I have taken part, to the trips I have done, to the classmates and colleagues I have met, but especially to those who have made all of these experiences possible: my family.

Index

INTRODUCTION

With the signing of a Technical Arrangement in February 2016, the European Union (EU) and the North Atlantic Treaty Organization (NATO) launched an important program of cooperation on cyber security[1]. Since then, many steps have been taken by the two organizations in that direction. Given the early stage of the cooperation and the urgent need to carry out this project with determination and effectiveness, the necessity to put together all that is at the basis of this process, and question its matter, has been perceived. This is to enable both parties to know in a detailed but concise manner the two cyber structures and their respective strategies. In order to produce the greatest possible common advantage, it is of paramount importance, in any kind of cooperation, to avoid unnecessary overlaps of tasks and focus all the efforts on the basis of different expertise.

Creating common advantage through dialogue is the primary role of diplomacy. Creating common advantage through dialogue on cyber security issues is the primary role of cyber diplomacy. In more depth, cyber diplomacy uses diplomatic tools to solve the problems that emerge in cyberspace. After having formally recognized cyberspace as a global common and fifth domain of warfare (after land, sea, air, and space)[2], it is now necessary that all the issues that concern this domain get discussed globally. Issues such as the structuring of internet governance, the respect for human rights online, the enforcement of law against cyber crime, how to respond to malicious acts arising in the cyberspace, the protection of strategic know-how, and many others, are of primary importance and cannot be abandoned to the law of the strongest as in the jungle. Currently, cyberspace is a virtual jungle where prowlers are always lurking, and danger is around every corner. Unfortunately, too often the virtual world is still considered as something abstract. However, the virtual world is a real world, based on physical structures, and as such, it has an impact on real things. Despite the fact that it is impossible to calculate an exact figure, due to the peculiar characteristics of the cyberspace that make it difficult to attribute and estimate damage, all major cyber security companies agree that cyber crime alone (without considering the social sphere) has a global annual cost of various hundreds of billions of dollars. In addition, they all agree that trends are inevitably

[1] See section *3.2 The EU-NATO cyber diplomacy* for more information on the Technical Arrangement.

[2] See section *1.1 Foreign policy and cyberspace* for the recognition of the cyber domain.

destined to grow exponentially[3].

This dissertation has a dual purpose. On the one hand, it seeks to raise awareness among all those who have little sense of the theme. The paper is not just for all those who, in one way or another, make part of the system that produces cyber security policies within the EU, NATO and on behalf of the Italian Republic. But also to the common citizens who ignore this topic, especially because of the little information the media dedicate to it. If cyber security discussions concern only one niche in society, the study of cyber diplomacy and its related topics seem to be even more elitist. Therefore, it is intended to use a simple and not so technical language to deal with a delicate and complex subject, which is absolutely necessary to be addressed in today's world. On the other hand, the dissertation is committed to answer two research questions. The first: how can the EU-NATO cooperation on cyber security be effective and not counterproductive? The second: in what way is it possible to give impetus to the Italian cyber diplomacy so that it plays a significant role in the international cyber scene? In order to try to achieve the purposes just described, this thesis will be organized as the following.

In the first chapter, the paper will deal with the increasing involvement of diplomacy, understood as a foreign policy tool, in cyberspace. In particular, it will focus on what the role of diplomacy is and how the growing use of Information and Communication Technologies (ICTs), particularly the internet, is deeply changing this role. Although ICTs bring many benefits, these necessarily involve additional risks. It will then question the role of actors in cyberspace, focusing mainly on governments. In this regard, it will cite some cases of cyber attack in which governments were the main protagonists. For the fact that the risks associated with this type of attack are global, a special kind of diplomacy that focuses only on these aspects is needed to address this issues. In this section, the paper will deal with the concept of cyber diplomacy and why it has to be necessarily distinguished from the kind of diplomacy that uses ICT tools, i.e. digital diplomacy. Before concluding with the reasons why the EU and NATO have been chosen for this research, some cases of cyber diplomacy will be analysed, evaluating the different matters and the different sorted effects. In particular, the subject of this comparisons will be the two negotiations between three of the most important actors in the cyber scene, namely the USA, Russia and China.

[3] See section *3.1.1 An overview on global cyber threat* for more info on the cyber menace.

The second chapter will be entirely devoted to the security strategies of the two international organizations. Therefore, it will be divided into two parts: the first one will analyse the European Union's strategy, while the second one will deal with the strategy of the North Atlantic Treaty Organization. The background, evolution and all the steps that have led both organizations to adopt their current cyber security strategies will be analysed in detail. Particular attention will then be given to the objectives of these strategies. Without clearly identifying the goals of either organization, it would be impossible to undertake a cooperation. The dissertation will then briefly examine the legal frameworks in which the EU and NATO incorporate such strategies as well as the agencies that the two organizations set to operate in the cyber security sector. Finally, it will deal with the funds that both organizations allocate to tackle cyber threats. All this work of analysis will be indeed necessary to see how the different structure and composition of the EU and NATO deeply model their approach to the issue. Without a general overview of the matter, it would be impossible to understand the motivations that have recently led the two organizations to cooperate, but above all to formulate weighted advice and recommendations that could benefit the project.

The third chapter will attempt to answer the first research question of the dissertation. This will be divided into two parts: the first one will focus on the status of the global cyber threat, while the second one will deal with the cyber security cooperation between the EU and NATO. Without an analysis of the threat landscape, there is no point in tackling the issue. Firstly, the thesis will analyse the current trends of the cyber threat, with an eye to the geography of the menace, the recorded cases and the motivations behind them. It will then move to the analysis of the sectors undergoing the greatest number of attacks and those in which the threat can be expected to grow. The different types of attacks employed will be analysed by taking into account the growing or decreasing tendencies for individual attacks. Finally, to conclude this part dedicated to the cyber threat, a paragraph will be entirely devoted to the future challenges of cyber security.

An evolution in technology implicates an evolution of the risks. In this part, it will be discussed of quantum computing and its application in the field of encryption; of the close relationship between big data and the internet of things (IoT); of the risks associated with cloud computing and how these can be overcome through fog computing and blockchain. Last but not least, the challenges posed by the interaction of humans with ICTs will be analysed. It will be therefore addressed the importance of cyber hygiene and the creation of an international framework for cyberspace that is recognized and accepted by all the actors are potential performers and victims of this new threat.

A new kind of threat requires a new kind of cooperation. In the second part of this chapter, the matters of the EU-NATO cooperation on cyber security will be discussed. This section will follow step by step the evolution of this recent cooperation project. A paragraph will be devoted to thoughtful evaluations and advice on how the cooperation can be effectively carried out in the near future. It will be explained why this cooperation is absolutely desirable, by showing its potential benefits and risks.

The fourth and last chapter will be entirely dedicated to the Italian case. Italy is a founding member of both the EU and NATO. Because of its strategic position, its history, and its Euro-Atlantic vocation, the country immediately covered a key role in both organizations. This is clearly demonstrated by the copious amount of decisions taken at European meetings on Italian soil, as well as by a large number of politicians who have held leading positions in the European institutions. As for NATO, Italy stands out for its steady and constant presence in the territories of crisis of the east and south sides of the Alliance, namely the Balkans, the Middle East, and North Africa. Furthermore, this role will be discussed with Ambassador Luca Giansanti, General Director for Political Affairs and Security of the Italian Ministry of Foreign Affairs.

The second paragraph of the final chapter will deal with the current status of the cyber threat in the Italian peninsula. As in the previous chapter, the trends that relate to the reasons for threats, the most affected sectors, and the types of attack performed will be analysed. This will serve to introduce the Italian cyber strategy. Again, the analysis of this strategy is intended to understand the role of the Italian diplomacy in the cyberspace. In this respect, a case of successful multilateral cyber diplomacy favoured by the Italian commitment will be analysed: the adoption of the Lucca Declaration during the last G7 Summit. It will be possible to know in detail all that preceded the signing, its reasons, the points of disagreement and what to expect for the future of such agreement by discussing it with those who actively took part in the Italian team, namely the Minister Plenipotentiary Gianfranco Incarnato, the Engineer Pierluigi Paganini and Doctor Luigi Martino. Finally, by taking into account the new Italian cyber structure, it will be attempted to answer the second research question. The dissertation will be completed by suggesting tips and recommendations for the future of the Italian cyber diplomacy.

1. DEFINING THE FRAMEWORK

1.1 Foreign policy and cyberspace

"Reduced to its fundamental ingredients, foreign policy consists of two elements: national objectives to be achieved and the means for achieving them. The interaction between national goals and the resources for attaining them is the perennial subject of statecraft. In its ingredients, the foreign policy of all nations, great and small, is the same.[4]" The definition that professor Cecil V. Crabb Jr. wrote in 1972 on the first page of his book "American Foreign Policy in the Nuclear Age" is still perfectly relevant and appropriate to easily understand how foreign policy works. Clear targets and how to hit them, that is it.

Being the activity of managing international relations[5], diplomacy is still one of the major instrument of foreign policy. Whether bilateral or multilateral, state-driven or organization-driven, the art of diplomacy has being neither abandoned nor lessened. However, time has passed and things have naturally changed, following the course of history and riding the wave of progress. The so-called "soft power", defined by the political scientist Joseph Nye as "the ability to achieve desired outcomes in international affairs through attraction rather than coercion"[6], now requires new kind of means to effectively communicate at a global level. The most relevant factor which has tremendously affected how diplomacy is conducted nowadays is the breakthrough of Information and Communication Technologies (ICTs). According to Technopedia, the term "Information and Communications Technology" refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, network-based control and monitoring functions[7]. This comprises televisions, radios, phones and mobile phones, computers and networks, satellite systems and so on and so forth, but also all the applications and services associated with them. The way all the people across the globe communicate, exchange information and behave has been completely revolutionized by these

[4] Crabb C. V. Jr., 1972, *American Foreign Policy in the Nuclear Age*, 3rd ed., Harper & Row, New York, p. 1.

[5] See section *1.2 What is cyber diplomacy? f*or an extensive definition of the term "diplomacy".

[6] Potter, E. H., 2002, Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century, McGill-Queen's University Press, Montreal & Kingston London Ithaca, pp. 84-85.

[7] Technopedia, *Definition of Information and Communication Technology*. Link: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict

technologies.

Ça va sans dire, ICTs diffused, diffuses and will diffuse differently in different regions and among different sectors within those regions[8]. For instance, because of the backwardness of infrastructures and its intrinsically different culture, the African continent approaches ICTs way much slower and less intensively than the South East Asian countries. However, these technologies are actually offering even less developed areas of the world an unprecedented chance of growth and development, by transforming them into high value-added information economies. This technological innovation contributes in cutting the divide between developing and advanced countries, making globalization and global connection processes skyrocket[9].

The internet is the connecting tool *par excellence*. Being defined as "a means of communication that enables the publication, exchange, and storage of information"[10], the internet has become pivotal to the private and public daily communication. According to the World Bank, nearly half of the world population has an internet connection and regularly surf the net[11]. Given that the number of users keeps growing, online *fora* do it as well[12]. With 2.51 billion of users worldwide[13], social networks and instant messaging platforms (like the very popular Facebook, WhatsApp, Twitter, QQ and WeChat) have become highly populated venues into the cyberspace[14], where users can interact by posting contents and discussing them. Due to this interconnectivity, the real world seems to become everyday smaller and smaller, while the digital one keeps increasing in size and impact. This results in both opportunities and challenges for national/international institutions and organizations on how to adapt in order to deal with these new policy spaces[15]. As a means of foreign policy, ICTs have changed also how diplomacy is conducted.

[8] Duque, R., Collins M., Abbate J., Azambuja C. C., Snaprud M., 2007, *History of ICT*, in *Past, Present and Future of Research in the Information Society*, Springer US, pp. 33-45.

[9] Faye, M., 2000, *Developing National Information and Communication Infrastructure (NICI) Policies and Plans in Africa*, Nigeria NICI Workshop, Abuja.

[10] Westcott, N., 2008, *Digital Diplomacy: The Impact of the Internet on International Relations*, Oxford Internet Institute, p. 3.

[11] World Bank, *Internet users (per 100 people)*. Link: http://data.worldbank.org/indicator/IT.NET.USER.P2

[12] Hocking, B., Melissen, J., 2015, *Diplomacy in the Digital Age*, Clingendael Netherlands Institute of International Relations, The Hague, p. 30.

[13] Statista, *Number of social media users worldwide from 2010 to 2020 (in billions)*. Link: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users

[14] See section *1.2 What is cyber diplomacy?* for a definition of "cyberspace".

[15] Adesina, O. S., 2017, *Foreign Policy in an Era of Digital Diplomacy*, in *Cogent Social Sciences*, 3 (1).

In his paper entitled "Baked in and Wired: eDiplomacy @ State", the researcher Ferguson Hanson outlines eight policy goals for successfully run diplomatic activity in the cyberspace that go far beyond its classic negotiation role[16]: knowledge management; public diplomacy; information management; consular communications and response; disaster response; internet freedom; external resources; and policy planning. In short, knowledge management has to do with the storage of the whole government knowledge so that it can be easily shared and used. Public diplomacy should be conducted with new communication tools in order to address key messages, influence and secure contact with the audience as it becomes larger and larger online. Information management is then fundamental to control the massive flux of information responding to emerging political and social movements. Create a consular channel of direct communication with citizens who travel from and to the country is also a priority. The use of Information and Communications Technologies is indeed extremely practical to respond to disaster or crisis situations. Furthermore, diplomacy should foster the use of technology to keep the internet a free and open space, in particular by promoting democratic activities and freedom of speech. Digital mechanisms to take advantage of external resources and expertise have an important role in diplomacy to advance national objectives. *Dulcis in fundo*, a policy planning to arrange, coordinate and oversight international policies across governments, as a response of the digitalization of bureaucracy, is the last goal for successfully run diplomatic activity in the cyberspace. These means can be achieved only by taking into considerations that the revolution in Information and Communication Technology has had four remarkable effects in the management of diplomacy[17].

First of all, the relationship between time and distance is now perceived in a new way. The transboundary effect of information technology provides real-time material captured with an ordinary mobile phone and transmitted globally. If there is an internet connection, there can be an almost instant communication, from everywhere to everywhere.

Second, the quantity of information has become enormous. The spread of technology has led to a greater geographic availability and depth of knowledge. The increasing volume of

[16] Hanson., F., 2012, *Baked in and Wired: eDiplomacy @ State*, Foreign Policy Paper Series 30, Brookings Institution, Washington DC, pp. 1-41.

[17] Barston, R. P., 2014, *Modern Diplomacy*, Routledge, New York, p. 112.

available opinions relating to national and international issues is made up of online comments, views, and data. Due to these interactions, the traditional assessment duty of diplomacy has never become so articulated and thus difficult.

Third, the line between private and public spaces is blurred. ICTs have widened the functions of personal communication systems in searching for information and applications. The constant hunt for technical development has made these systems an essential diplomatic tool.

The fourth major effect brought by Information and Communication Technologies in the management of diplomacy has to be found in the variety of new threats related to the cyberspace. In fact, it is fundamental to acknowledge that ICTs have changed and shaped not only the social, political and economic landscapes, as seen so far, but also the security one. Both in positive and negative ways.

It must not be taken lightly how certain use of computers and other devices connected on the internet infrastructures can cause misunderstandings, tensions, and conflicts within and between states. At a national level, it is not difficult to imagine how the activities conducted in the cyberspace can easily lead to disagreements, given the different interests and positions of the many political parties. However, cyberspace becomes a protagonist component of foreign policy in the case where states intensively debate issues like the respect of human rights online, the rules of behavior in the virtual environment, or the application of international law in relation to cyber attacks.

Along with the non-proliferation of nuclear and chemical weapons, terrorism and insurgency (among the many others), cyber attacks represent one of the unconventional threats to international security. Cyber security, in particular, has a complex value because, by nature, it deals with the cyberspace. In fact, the cyberspace can become the ground to a multitude of different threats, depending on who is the attacker and who is the victim, what is the purpose of the attack and what can be expected. In this matter, five main dimensions of cyber(in)security can be identified[18]: cyber activism; cyber terrorism; cyber crime; cyber espionage; and cyber warfare. Although all of them have different implications (which

[18] Maiorescu, T., 2015, *Cyber Diplomacy – A New Component of Foreign Policy*, Journal of Law and Administrative Sciences, (3), p. 91.

potentially may overlap in specific situations), each type of attack exploits the cyber domain to harm an opponent[19]. Generally, while hacktivists (namely hackers with ideal and ethical scopes) mainly promote political ideas, terrorist organizations operate online for propaganda, fundraising and recruiting scopes, whereas criminals use the internet for a countless number of different frauds that goes from the buying and selling of drugs and weapons to the theft of identities and money.

A different discourse has to be made with regard to cyber espionage and cyber warfare. In 1996, 99% of the cyber attacks were led by hacktivists and only 1% by state actors. Nowadays, these percentages are completely inverted: 99% of the most detrimental attacks are accomplished by nation state hackers through a set of stealthy and continuous hacking processes, the so-called "Advanced Persistent Threat" (APT)[20]. In these perspectives, the cyberspace becomes the terrain of diplomatic quarrels and conflicts. Just as an example, the 2013 leak of the National Security Agency's (NSA) classified information, copied and revealed by the computer professional Edward Snowden, on the cyber espionage and mass surveillance programs of the government of the United States of America (USA) on NATO allies and some friend states of the US, had a huge diplomatic impact at the global level[21]. As a consequence, many Western European countries reconsidered their position on the US-centric model of internet governance[22].

The 2007 cyber attacks on Estonian parliament, ministries, newspaper and bank websites; the 2008 cyber attacks during the Russo-Georgian war; the 2010 cyber attack towards the Iran's nuclear program; the 2014 cyber attack to Ukraine's, European and NATO allies infrastructures of Information Technology during the Russian military intervention in the country; and the 2017 cyber attack to the national press agency of Qatar (which eventually led to an ongoing diplomatic crisis) are other relevant examples in which governments were the

[19] Van Der Meer, S., 2016, *Defence, deterrence, and diplomacy: Foreign policy instruments to increase future cyber security*, in Cherian, S., Munish, S., *Securing cyberspace. International and Asian perspectives*, Pentagon Press, New Delhi, p. 96.

[20] Di Corinto, A., April 6 2017, *Cybersicurezza, l'allarme degli esperti: "Borse mondiali nel mirino degli hacker"*, La Repubblica. Link: http://www.repubblica.it/tecnologia/sicurezza/2017/04/06/news/security_analist_summit_2017-162331025/

[21] Finn, P., Horwitz, S., June 21 2013, *U.S. charges Snowden with espionage*, The Washington Post. Link: https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html

[22] Maiorescu, T., 2015, *Cyber Diplomacy – A New Component of Foreign Policy*, Journal of Law and Administrative Sciences, (3), p. 92.

main actors of cyber warfare[23]. Although national authorities are not the only players in the use of this strategy, given that attacks can be launched by non-state actors (including international and regional organizations), in this context of international instability, the trust in and between political leaders is shrinking, in particular where information is censored, the access to internet reduced and the informatics systems surveilled[24].

Due to its nature of asymmetry and trans-nationality, and given the specific features of the cyberspace, cyber security requires a strong and international public policy action. Measures of cyber security have to be intended as an equivalent matter of physical defence. In a post-Cold War era in which military confrontation is played in a space where there are almost no regulations and the impact of cyber attacks has a global reach, the fifth dimension of warfare requires far more efforts[25]. After having regulated the conduct of peace and war in the traditional domains of land, sea, air and outer space, the cyber world not only needs laws for its peaceful navigation but also a legislation for its warfare and security[26]. Being the means by which states articulate their foreign policy objectives, coordinate efforts and use dialogue and negotiations to influence foreign behaviors and decisions, secure interests and reduce the threat of international frictions, diplomacy strives to preserve peace and cooperation[27]. Therefore, along with appropriate defence capabilities[28], it is also necessary to develop diplomatic strategies to shape and outline the cyber security environment. In other words, this is the moment to enhance the so-called "cyber diplomacy".

1.2 What is cyber diplomacy?

Before providing some examples of cyber diplomacy and its conduct, it is necessary to clarify

[23] Van Der Meer, S., 2016, *Defence, deterrence, and diplomacy: Foreign policy instruments to increase future cyber security*, in Cherian, S., Munish, S., *Securing cyberspace. International and Asian perspectives*, Pentagon Press, New Delhi, p. 97.

[24] Wang, W., 2015, *Analysis on China's Cyber Diplomacy*, The Graduate School of Chinese Academy of Social Sciences, Beijing.

[25] Martino, L., 2013, *La quinta dimensione della conflittualità. La rilevanza trategica del cyberspace e i rischi di guerra cibernetica*, Centro Interdipartimentale di Studi Strategici Internazionali e Imprenditoriali (CSSII), Florence.

[26] Stang, G., 2013, *Global Commons: Between Cooperation and Competition*, European Union Institute for Security Studies, 17.

[27] Adesina, O. S., 2017, *Foreign Policy in an Era of Digital Diplomacy*, in *Cogent Social Sciences*, 3 (1).

[28] Smallenbroek, J., 2015, *Cyber Security: Cooperation or Proliferation?*, University of Groningen.

what the term “cyber diplomacy” itself means. The debate about diplomacy in the digital age has been profoundly characterized by a confusion in terminology. Used nearly in an interchangeable way, the terms “e-diplomacy”, “net diplomacy”, “virtual diplomacy”, “digital diplomacy” and “cyber diplomacy” have reflected the personal and stylistic preferences of the authors[29]. Clearly, this is not only bumbling but also inefficient for more than one reason[30]. Without considering the waste of five different and meaningful terms, this could raise confusions and misunderstandings in the diplomatic debate. In fact, while it is easy to fully agree that all the prefixes here mentioned refer to the impact of ICTs on diplomacy[31], each one of them describes different involvements and developments of this activity in the cyberspace.

“E-” is the abbreviation for “electronic”. The first general use of the term was mostly related to “e-commerce” as the internet became more and more involved in trade. The 2000 Lisbon Agenda of the European Union (EU) made an abundant use of this abbreviation, but, like the failure of the Agenda, the Union abandoned its use in recent times. Notably, “E-” was also the most used prefix in the declarations of the 2003 and 2005 World Summit on the Information Society (WSIS) of Geneva and Tunis mostly to address general actions on government, business, employment, health, learning, science and agriculture.

The prefix “net” owes its name from the term “network”. It became pretty popular in the early 2000s, in particular in Germany where it was not uncommon to refer to the so-called “Netzpolitik”. With the exception of the 2014 NETmundial Initiative (NMI) launched in Sao Paulo to create a new platform for internet governance issue, the prefix “net” almost disappeared from the context.

“Virtual” has to do with the intangible nature of the cyberspace, and in particular, of the internet. Academics mostly used (and use) the term to refer to a reality which is somehow impalpable or non-existent. Because of its ambiguity, the term “virtual” is rarely used in international documents and seldom appears in the political language.

[29] Kurbalija, J., 2015, *Different prefixes, same meaning: cyber, digital, net, online, virtual, e-*, DiploFoundation. Link: https://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e

[30] Riordan, S., 2016, *Digital diplomacy v. cyber diplomacy: terminological distinction*, Center on Public Diplomacy Blog, University of Southern California. Link: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

[31] Kurbalija, J., 2017, *An Introduction to Internet Governance*, DiploFoundation.

This is not the case for “digital”. “Digital”, by definition, refers to the use of discrete and discontinuous representations of information through the binary digits (i.e. 0 and 1) which are the basis of the whole cyberspace. While in the past “digital” was mainly used to develop circles to represent the digital divide, ultimately the term has conquered the internet vocabulary and most of the software and programmes have the word in their names. The term is copiously used also in the political language, as proven by being mentioned ten times during the presentation of his five-year policy plan for the EU by the President of the European Union Jean-Claude Junker, in 2014. The Union has an official Digital Agenda for Europe[32], the Foreign Office of the United Kingdom has opened a blog dedicated to its digital diplomacy[33] and Denmark has appointed its official digital ambassador[34].

The term “cyber” owes its name from “cybernetics”. Generally considered the originator of cybernetics, the American mathematician Norbert Wiener derived this term from the Greek “*κυβερνήτης*”, which means “governor”. The assumption, theorized into his book “Cybernetics: or Control and Communication in the Animal and the Machine” first published in 1948, is used to describe a new interdisciplinary science or feedback mechanisms, which combined communications and control theory with statistical mechanics. In his words: “we have to decide to call the entire field of control and communication theory, whether in machine or in animal, by the name Cybernetics[35]”. However, “cyber” came into current use via the American-Canadian science-fiction writer William Gibson who coined the term “cyberspace” in his novel “Neuromancer”, published in 1984. The cyberspace was conceived by the author as “a graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding[36]”. As explained by Gibson himself, because of the need to move his characters through a new dimension of the narration, he came up with this word by looking at children playing arcade games[37]. The

[32] The Digital Single Market of the European Union. Link: https://ec.europa.eu/digital-single-market/

[33] The Foreign & Commonwealth of the United Kingdom's blog on its digital diplomacy. Link: https://blogs.fco.gov.uk/digitaldiplomacy/

[34] Gramer., R., January 27 2017, *Denmark Creates the World First Ever Digital Ambassador*, Foreign Policy. Link: http://foreignpolicy.com/2017/01/27/denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy/

[35] Wiener, N., 1948, Cybernetics: or Control and Communication in the Animal and the Machine, MIT Press, p. 19.

[36] Gibson, W., 1984, *Neuromancer*, Ace Books, New York, p. 67.

[37] Smallenbroek, J., 2015, *Cyber Security: Cooperation or Proliferation?*, University of Groningen, p. 41.

growth of acceptance and usage of the prefix “cyber” followed the advancement of the internet. In particular, during the 1990s, almost everything related to internet was labeled with this term. From cyber law to cyber community, from cyber culture to cyber sex, and so on and so forth. However, in the early 2000s “cyber” lost its general use and assumed meaning principally in the security vocabulary[38]. In particular, it has to be mentioned the 2001 Cybercrime Convention of the Council of Europe held in Budapest, which is still the only international treaty in the field of internet security[39], and the appointment of an Australia's official ambassador for cyber affairs[40] as well as the first coordinator for cyber issues in the secretary’s office at the State Department of the United States of America[41].

To wrap the discourse up, nowadays “e-” is the favourite prefix for business related activities, “net” has been almost abandoned, and “virtual” is used in a broader sense of intangibility or non-existence. Although “digital” and “cyber” have been largely accepted and employed by many governments and organizations in dealing with the internet, a neat distinction is necessary when the two words are directly associated with the term “diplomacy”.

According to the Oxford Dictionary, diplomacy can be defined as “the profession, activity, or skill of managing international relations, typically by a country's representatives abroad.”[42] Using the beautiful metaphor of professor Raymond Cohen, “diplomacy is the engine room of international relations”[43]. As already underlined in the previous section *1.1 Foreign policy and cyberspace*, diplomacy is the classical means by which states manage their foreign policy interests, by coordinating negotiation efforts and foster dialogue in order to prevent the use of violence. The safeguard of national interests remains the core of its existence. This is the key reason to understand why digital diplomacy and cyber diplomacy should be universally conceived in two different ways. In particular, it has to be highlighted that there is a general

[38] Von Solms, R., Van Niekerk, J., 2013, *From Information Security to Cyber Security*, Computers & Security, 38, pp. 97-102.

[39] Kurbalija, J., 2015, *Different prefixes, same meaning: cyber, digital, net, online, virtual, e-*, DiploFoundation. Link: https://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e

[40] Official page of the Australian ambassadors and other representatives of the Department of Foreign Affairs and Trade. Link: http://dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs.aspx

[41] Official page of the first coordinator for cyber issues in the secretary’s office at the State Department of the United States of America. Link: https://www.state.gov/r/pa/ei/biog/161848.htm

[42] Oxford Dictionary, *Definiton of "diplomacy"*. Link: https://en.oxforddictionaries.com/definition/diplomacy

[43] Cohen, R., 1998, *Putting Diplomatic Studies on the Map*, Diplomatic Studies Program Newsletter, Centre for the Study of Diplomacy, Leicester, p. 1.

tendency to merge two activities which are completely different: on the one side, the use of digital tools to advance the management of diplomatic activities and, on the other side, the use of this means to seek a resolution of issues arising in the cyberspace. It is not uncommon that controversial debates arise just because one part in cause is dealing with the first aspect while the other one with the second. Even if we agree that both digital diplomacy and cyber diplomacy can be carried out by a different group of actors (including states, organizations and companies), they are very distinct kinds of activities. To avoid confusions and futile debate, which should leave space for more relevant and serious issues, the term digital diplomacy should be used to refer to the digital tools employed in the conduct of the diplomatic activity (which includes the typical duties of embassies and consulates, the tasks of ministries of foreign affairs, negotiations between states and organizations, and so on), whereas cyber diplomacy should be used to address the diplomatic tools necessary to solve issues arising in the cyberspace (like cyber security, cyber crime, cyber terrorism, and so on).

To make it clear, digital diplomacy, instead of being an end in itself, represent the whole set of actions which use ICTs to perform its activity[44]. As already explained, state and non-state actors have objectives to achieve, strategies to follow and means to seek this achievements. Nowadays, a large part of these means are digital devices and programmes. These tools help diplomats to conduct analysis of complicated situations, engage with relevant stakeholders and influence the public policy debate. With the ease of communication goes the facilitation of the diplomatic activity. Notably, these digital tools are not limited to real-time messaging, quick information exchange and social media only but include also conflict simulations, digital platform for learning, web-sourced analysis and big data. This is why a major challenge for digital diplomacy is represented by the development of digital tools which are made for the purpose of diplomatic strategies only, setting aside popular and commercial products, as well as the integration of these tools within the ordinary diplomatic bureaucracy.

However, whereas on the one side the cyberspace can provide a considerable help for diplomacy, on the other side the cyberspace itself needs the support of diplomatic efforts. Due to its relevance to national security, public safety and economic development, cyber security

[44] Riordan, S., 2016, *Digital diplomacy v. cyber diplomacy: terminological distinction*, Center on Public Diplomacy Blog, University of Southern California. Link: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

has become an important element of foreign policy. As already shown, whereas hackers and criminal organizations have targeted business since many years, it is only recently that cyber attacks have created a political risk[45]. The increase of the dependency of national critical infrastructures on ICTs and the centralization of sensitive data in networks on the cyberspace ensure that geopolitics and cyber security collide[46]. Political decisions related to the cyberspace have sound international echoes that require an international commitment.

The promotion of collaborations between governments, organizations, companies and other relevant stakeholders from both the public and the private sectors; the seek for a global jurisdiction on the conduct in the cyberspace; the identification of multilateral consultation mechanisms; the encouragement for transparency in communication; the foster of confidence building measures; the share of substantial information and best practices; the reinforce of technical cyber security capabilities; the search, identification and dissuasion of potential internal and external vulnerabilities; the identification of common advantages; the enhancement the investment in research and innovation projects; the strengthen of common cyber resilience capabilities, both in technology and in human resources; and the creation of a global culture regarding cyber security should be on the agenda of every cyber diplomatic service. In short, a shift from the dependency on perimeter and technical oriented defence capabilities towards broad, focused and developed diplomatic strategies appears to be essential in a nowadays world without borders. Cyber diplomacy at the service of cyber security.

1.3 Examples of cyber diplomacy

The practice of cyber diplomacy is not absolutely new. Already in the 1990s, in the context of the Internet Corporation for Assigned Names and Numbers (ICANN) based in Los Angeles (USA) which is the non-state/multi-stakeholder body that regulates identities online, a group of states started to discuss about internet governance[47]. At the time, the discussion has

[45] Cooper, A. F., Heine, J., Thakur, R. C., 2013, The Oxford Handbook of Modern Diplomacy, Oxford University Press, Oxford, p. 48.

[46] Bremmer, I., January 12 2011, *The geopolitics of cybersecurity*, Foreign Policy. Link: http://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity/

[47] Renard, T., 2015, *US-China Cyber Security Agreement: a Good Case of Cyber Diplomacy*, EGMONT Royal Institute for International Relations. Link: http://www.egmontinstitute.be/publication_article/us-

designed a rough general structure and generated nothing more than future speculations. Furthermore, the fact that the final approval over changes to core issue was held by the United States Department of Commerce was generally tolerated at an embryonic stage of the development of the internet.

However, it is only in the last few years, with countries having become almost completely dependent on ICTs, that cyber issues represent such a harmful threat to the architecture of the national economic systems. Many governments have already perceived that cyber diplomacy is no longer a voluntary option for global powers and started to raise suspects on the ICANN's genuine and impartial nature[48]. In fact, to defend their right to control domestic cyber activities, Russia and a group of developing countries, led by China[49], have raised objections against this model. In particular, they have purposed the use of a new voting system, which would reflect the democratic style of traditional international organizations[50].

Nevertheless, cyber diplomacy apparatuses are at an early stage of development and service. As already seen, among the many difficulties in tackling this kind of issues, the adoption of different terminology and the lack of a common proper legislation represent the biggest stumbling blocks to the homogenization of the conduct of diplomacy in the cyberspace. Moreover, as identified by the United States Department of State, cyber diplomacy encloses a broad range of interests in the cyberspace. These are not limited to internet governance and cyber security only, but include also a different set of topics which go from the military use of the internet to the economic growth and innovation[51]. Without any doubt, cyber security represents a top priority of many powers' foreign policy[52]. Among the others, the agreements between USA and China, and between Russia and China are two meaningful examples of bilateral cyber diplomacy.

china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/

[48] Kim, S., 2014, *Cyber Security and Middle Power Diplomacy: A Network Perspective*, The Korean Journal of International Studies, 12 (2), pp. 329-330.

[49] Cf. Segal, A., 2017, *Chinese Cyber Diplomacy in an Era of Uncertainty*, Hoover Institution, Aegis Paper Serier No. 1730, Stanford.

[50] Ibid.

[51] The United States Department of State, 2011, *International Cyber Diplomacy: Promoting Openness, Security and Prosperity in a Networked World*, The Office of Electronic Information, Bureau of Public Affairs, p. 1.

[52] Breene, K., May 4 2016, *Who are the cyberwar superpowers?*, World Economic Forum. Link: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

The administration of the former president of the United States of America Barack Obama has launched an ample programme to enhance America's cyber security[53]. On its five point list, along with the protection of critical infrastructure, the improvement of cyber incident reporting, the secure of federal networks, and the build of a security-savvy workforce by working with the private sector, it was listed the engagement with international partners to protect the internet[54].

Therefore, during the visit to Washington of the president of the People's Republic of China Xi Jinping on the 24th and 25th of September 2015, the USA and the East Asian emerging superpower concluded a major cyber security agreement[55]. The visit was an occasion to agree on the necessity to work together to constructively manage the differences between the two countries and to expand and deepen the cooperation on global and regional challenges, development, and bilateral relations in general. Along with military relations, law enforcement and counterterrorism, and people-to-people exchange, cyber security appeared into the discussion.

According to the final report, the USA and China agreed "to cooperate in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cyber crime, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory"[56]. Updates of results and status would be provided regularly. Furthermore, both sides agreed to designate officials at the ministerial level in order to establish a joint dialogue mechanism and a hotline for escalation of issues that may arise in this context.

Then, the two agreed that neither parts "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sections"[57]. In other words, this part states that both the USA and China will not perform or

[53] Commission on Enhancing National Cybersecurity, 2016, *Report on Securing and Growing the Digital Economy*. Link: https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf

[54] Robinson, M. R., March 23 2015, *Foreign Policy in the Age of Cybersecurity Threats*, SecurityIntelligence, Link: https://securityintelligence.com/foreign-policy-in-the-age-of-cybersecurity-threats/

[55] The White House, September 25 2015, *Fact Sheet: President Xi Jinping's Visit to the United States*, Office of the Press Secretary.

[56] Ibid.

[57] Ibid.

support cyber espionage activities against each other.

The discourse was then shifted to normative issues. To seek for international norms of states' behaviors online, the two countries endorsed July 2015 report[58] of the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, which marked an important step in addressing crucial issues on cyber security and norms of behavior in the cyberspace[59].

The 2015 USA-China agreement on cyber security may not be a panacea, but it is indeed an important leap forward in this very sensitive policy area[60]. It is important to take into considerations that cyber security has been a critical issue in the relationship between the two countries. On the one side, China has expressed grave concern over the Edward Snowden's revelations of cyber espionage activities of America and its Five Eyes partners[61]. On the other side, the United States have regularly accused China of activities of hacking and espionage against America. After the case of five Chinese military officers were accused by the Americans of computer espionage in May 2014[62], president Barack Obama even declared his readiness to impose sanctions against Chinese companies blamed of intellectual theft, just ahead the meeting in Washington with president Xi Jinping[63]. In this context, the result of this hard-earned bilateral agreement was the output of an intense cyber-diplomatic activity, which included hours and hours of preparatory gatherings and a four-days meeting between foreign affairs senior officers of the two counterparts[64].

[58] General Assembly of the United Nations, July 22 2015, *A/70/174 United Nations 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

[59] The White House, September 25 2015, *Fact Sheet: President Xi Jinping's Visit to the United States*, Office of the Press Secretary.

[60] Cf. Brown, G., Yung, C. D., January 19 2017, *Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace*, The Diplomat. Link: http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/
Cf. Brown, G., Yung, C. D., January 19 2017, *Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity*, The Diplomat. Link: http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/

[61] Reuters, June 23 2013, *China 'gravely concerned' by Snowden's claims of U.S. cyber attacks on China*, World News. Link: http://www.reuters.com/article/us-usa-security-china-idUSBRE95N01C20130624

[62] The United States Department of Justice, May 19 2014, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, Office of Public Affairs.

[63] Kopan, T., September 24 2015, White House readies cyber sanctions against China ahed of state visit, CNN Politics. Link: http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/

[64] Renard, T., 2015, *US-China Cyber Security Agreement: a Good Case of Cyber Diplomacy*, EGMONT

Even if with different conditions, measures and outcomes, the Sino-Russian joint statement of cooperation, edited in June 2016, represents another important step in the practice of cyber diplomacy[65]. The document, signed by the Chinese president Xi Jinping and the Russian president Vladimir Putin at the end of the latter's visit to Beijing, includes a section on cyber security[66]. Precisely, five out of the twenty points of the statement concern this topic.

First of all, given the extremely large presence of Chinese and Russian online users, the two countries have recognized their direct responsibility to supervise the cyberspace by building up a "new global order that is peaceful, secure, open and cooperative"[67].

Furthermore, the two parts involved have declared that it is their duty to respect the United Nations Charter's principles of non-use of force, of national sovereignty, of fundamental human rights and freedoms, and of non-interference in the international affairs of other states on the cyberspace, in compatibility with the principle of cyber sovereignty, which is, by statement, "the extension and expansion of state sovereignty into the cyberspace"[68].

Then, China and Russia have affirmed that the entire international community should strive to prevent the arisen of any kind of conflicts in the cyberspace and thus not permit the use of Information and Communication Technologies to undermine stability and peace.

The fourth point has been dedicated to the "internationalization of internet governance"[69]. Both sides have agreed that a "fair distribution of the basic resources of the internet"[70] should be the final objective of this argument. Therefore, the promotion of a democratic, truthful and multilateral internet governance system is the target to hit. In doing so, China and Russia encourage every country's government and international organizations to take action.

Royal Institute for International Relations. Link: http://www.egmontinstitute.be/publication_article/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/

[65] Wei, Y., June 21 2016, *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*, The Henry M. Jackson School of International Studies, University of Washington, Seattle.

[66] Bing, Z., June 27 2016, *The Sino-Russian Joint Statement: the past and the future of Sino-Russian relations are here*, Xinhua. Link: http://news.xinhuanet.com/asia/2016-06/27/c_129092111.htm

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] Ibid.

In the last point, China and Russia have concluded the joint statement with the commitment to keep increasing their cooperation on cyber issues.

Although all of these five points represent indeed serious and contemporary challenges for the pursuit of global cyber security, actually none of these came out of the blue[71]. An *ante litteram* work of cyber diplomacy between China and Russia started in June 2009 with the sign of the Agreement among the Governments of the Shanghai Cooperation Organisation (SCO) Member States on Cooperation in the Field of Ensuring International Information Security, informally known as the Yekaterinburg Agreement[72]. Established in 2001, the SCO is an international organization composed of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan, India and Pakistan for the purpose of cooperation in the political, military and economic sectors, with a particular focus on extremism, separatism and terrorism.

In September 2011, four members of the SCO (including China and Russia) addressed a Draft of International Code of Conduct for Information Security[73] to the United Nations General Assembly. A new Draft[74] was then submitted in 2015, giving life to a global controversy over the concept of “cyber sovereignty”. In short, while the SCO member states strongly support the regulation of this content because of its potential menace to security, Western states fear that this regulation would be a threat to fundamental human rights, in particular the freedom of expression[75]. The controversy is still ongoing, and the Chinese Foreign Ministry's Cyber Division is the most fervent and resolute actor, as emphasized at the Wuzhen World Internet Conference in December 2015[76].

[71] Cf. Guest Blogger, June 30 2016, *Despite Cyber Agreements, Russian and China a close as you think*, Council on Foreign Relations. Link: http://blogs.cfr.org/cyber/2016/06/30/despite-cyber-agreements-russia-and-china-are-not-as-close-as-you-think/

[72] See the report of the Yekaterinburg Agreement. Link: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

[73] Shanghai Cooperation Organisation, 2011, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*.

[74] Shanghai Cooperation Organisation, 2015, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*

[75] Cf. Giles, K., 2012, *Russia's Public Stance on Cyberspace Issues*, in Czosseck, C., Ottis, R., Ziolkowski, K., *2012 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, pp. 63-75.

[76] Mikheev, V., March 22 2017, *Why do Beijing and Moscow embrace cyber sovereignty?*, Russia Beyond the Headlines. Link: http://rbth.com/opinion/2017/03/22/why-do-beijing-and-moscow-embrace-cyber-sovereignty_725018

With the annexation of Crimea by the Russian Federation, which led to a cracking in the American-Russian relations, the tie between Beijing and Moscow became stronger. In April 2015, on the eve of a celebration commemorating to the defeat of Nazi Germany, president Xi Jinping and president Vladimir Putin met again. On this occasion, China and Russia signed 32 bilateral agreements on the regional interests in central Asia and, within an information security *entente*, they established a non-aggression pact between the two countries in the cyberspace[77].

In order to conclude, it is necessary to make a couple of considerations based on facts. According to the September 2015 report[78] of the American cyber security company Proofpoint, only two months after the signing of the Sino-Russian agreement on cyberspace, Chinese language tools have been used to target Russian telecommunication and military infrastructures[79]. In more depth, the number of Chinese speakers who have targeted Russia has increased by 300% from December 2015 to February 2016, as shown by the director of the global research and analysis team at Kaspersky Lab Constin Raiu, during the Kaspersky Security Analyst Summit 2016[80]. Interestingly enough, in contrast, Chinese hacking activities against American companies seem to have declined since the September 2015 agreement between president Barack Obama and president Xi Jinping[81].

Without any doubt, the bilateral cooperation between China and Russia has been enhanced in the last years with strong diplomatic efforts. However, the Sino-Russian tie on cyber security appears to be more dependent on the relationships with the USA than on the partnership in itself between the two Asian countries. Both the governments of Beijing and Moscow are thus concerned about the American advocacy for internet freedom as a priority of its foreign policy. Fearing the ongoing dominance of the United States over the internet, China and

[77] Roth, A., May 8 2015, *Russia and China Sign Cooperation Pacts*, New York Times. Link: https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html

[78] Haq, T., F., A., September 15 2015, *In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia*, Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

[79] Korolov, M., September 17 2015, *Russian military attacked, possibly by Chinese cyber group*, CSO Online. Link: http://www.csoonline.com/article/2984599/advanced-persistent-threats/russian-military-attacked-possibly-by-chinese-cyber-group.html

[80] Jackson Higgings, K., February 9 2016, *Chinese Cyberspies Pivot to Russia in Wake of Obama-Xi Pact*, Dark Reading. Link: http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242

[81] Lynch, D. J., Dyer, G., April 13 2016, *Chinese hacking of US companies declines*, Financial Times. Link: https://www.ft.com/content/d81e30de-00e4-11e6-99cb-83242733f755#axzz49iIJLMb8

Russia combine their effort to seek more geopolitical influence through the reshaping of the fifth dimension of warfare, namely the cyberspace.

1.4 Why EU and NATO?

Cyber diplomacy does not occur in superpowers' bilateral relations only. As cyber-related issues become more and more central to the needs of also medium and even small powers' foreign policies, a large number of discussion takes place at the multilateral level. The landmark decision of expanding a list[82] of confidence building measure (CBMs) to enhance stability and security in the cyberspace, adopted in March 2016 by 57 participating states of the Organization for Security and Cooperation in Europe (OSCE), is an important example. However, few governments have truly considered the diplomatic role in enhancing cyber security, neglecting both the potentiality of this tool of negotiation and the risks that the cyberspace entails. The stickiness to an old fashioned domestic approach to national security makes it difficult to effectively tackle global challenges of the future. In this context, international organizations fulfil an absolutely leading role.

Over the last twenty years, European countries have obviously faced the same cyber security challenges of the United States, Russia and China[83]. However, it is important to notice that, while the latter have tackled these challenges with a centralized military apparatus, a common budgetary policy and a single strategy of foreign policy (by benefitting from their sovereign authority), European governments have had to confront cyber threats with a mixture of both national and supranational policies. To reinforce their defences, the European countries thus resorted mainly to the European Union and to the North Atlantic Treaty Organization.

Like most regional, global and transatlantic organizations, the EU and NATO have developed objectives, instruments and practices to address the ongoing process of development of ICTs

[82] OSCE, March 10 2016, *Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risk of Conflict Stemming from the use of Information and Communication Technologies*. Link: http://www.osce.org/pc/227281?download=true

[83] Ilves, L. K., Evans, T. J., Cilluffo, F. J., Nadeau, A. A., 2016, *European Union and NATO Global Cybersecurity Challenges. A Way Forward*, in *Prism*, Center for Complex Operations, Washington DC, 6 (2), pp. 124-141.

and their annexed risks[84]. However, the overall goals of the EU and NATO have never changed: to maintaining stability and assure peace and security to their citizens[85]. More than ever, the security of the European and North American regions is now intertwined, as this stability faces a series of unprecedented security challenges coming from the Southern and the Eastern areas of the world. The EU and NATO need to tackle these menaces with a complementary and efficient strategy.

New threats require new ways of collaboration and new levels of ambition. Without losing their established shared values, the EU-NATO strategic partnership could give a new impetus to tie the transatlantic relationship. In times of uncertainty, there is a need for strong institutions. In order to do that, on the one side, it is necessary to ensure an effective and fair burden-sharing, and, on the other side, operate in accordance with their own strengths and capabilities. Each nation alone has just a single set of forces. The very same nations can double its force by being a member of an international organization and then re-double it with a collaboration between two international organizations. Together, the EU and NATO have always mobilized a broad range of forces and, at the same time, made a more efficient use of their members' resources[86]. This is the first reason why a close cooperation between the EU and NATO is necessary now more than ever.

The second main reason for enhancing the EU-NATO cooperation is linked with the fact that the European Union is building step by step its own defence[87]. More European collaboration and expenditure on defence will lead to a stronger Europe. This will strengthen not only the EU but also NATO, as half of its geopolitical interests are in the European region or next to its borders. However, without a deep and strategic dialogue between the two organizations, the risk of creating duplications is high. A constant diplomatic activity between the EU and NATO would assure the complement themselves and avoid any sort of nonsense competition.
The third and most relevant reason why the search for a more efficient EU-NATO dialogue is

[84] Pernik, P., 2014, *Improving Cyber Security: NATO and the EU*, International Centre for Defence Studies, Tallinn.

[85] NATO, December 6 2016, *(2016)178 Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.*

[86] Pernik, P., 2014, *Improving Cyber Security: NATO and the EU*, International Centre for Defence Studies, Tallinn.

[87] European Commission, November 30 2016, *IP/16/4088 European Defence Action Plan: Towards a European Defence Fund*, Press release.

needed is the fact that, having 22 members in common[88], the political and economic union and the intergovernmental military alliance share a mutual interest in becoming more resilient to cyber attacks. In the last ten years, both have officially recognized that cyber security is a major challenge for the achievement of their objectives and the reinforcement of their core values[89]. In particular, the union and the alliance have realised that all the future conflicts will see the presence of actions performed in the cyberspace. These include activities that go from cyber attacks to cyber espionage, from cyber propaganda to cyber terrorism. Therefore, a failure in cyber security is equal to a failure in a classical national security apparatus. As a consequence, this kind of failure could lead to the deterioration of a copious set of interests, both in the public and in the private sectors. Neither the EU nor NATO alone have the tools to tackle these risks.

This fragmented reality obliges the European External Action Service (EEAS) and the NATO International Staff to commit themselves into a deep diplomatic cooperation to reinforce their defensive structures (or to create new ones). This activity is fundamental in order to achieve the EU-NATO's core objective of ensuring stability on a fundamental aspect like cyber security.

[88] NATO, December 6 2016, *(2016)178 Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.*

[89] NATO, December 15 2016, *Doorstep Statement by NATO Secretary General Jens Stoltenberg at the European Council on Security and Defence*.

2. CYBER SECURITY STRATEGIES

2.1 The EU cyber security strategy

2.1.1 Evolution and background

In line with the necessity of protecting its infrastructures from the threats of cyberspace, the European Union has adopted many counter measures. The first relevant step has been the establishment of the European Network and Information Security Agency (ENISA) in 2004[90]. The original aim of the Agency was nothing more than sharing knowledge and best practices among the member states.

Following the unexpected distributed denial of service (DDoS) which blocked Estonian private and public infrastructures in 2007, the Union (beside NATO) has been dramatically forced to reconsider its approach to cyber security. As a consequence, in 2010, the EU developed the Digital Agenda for Europe[91] and the Europe 2020[92] strategy to attempt to tackle the issue with a long term view.

The very next year, after having recognised the potential impact of a cyber attack on European structures and the borderless nature of the phenomenon, the Union developed numerous Internal Security Strategies as well as the European Guidelines and Principles for Internet Resilience document[93]. At this point, the EU started understanding the importance of having global partners to address the issue and consider necessary the collaboration of both the military and civilian worlds[94].

2013 was the year of the adoption of the EU Cybersecurity Strategy[95]. The Union

[90] European Commission, January 2017, *EU cybersecurity initiatives: working towards a more secure online environment*, Factsheet.

[91] European Commission, May 19 2010, *COM(2010) 240 Digital Agenda for Europe*.

[92] European Commission, March 3 2010, COM(2010) 2020 *Europe 2020: a strategy for smart, sustainable and inclusive growth*.

[93] European Commission, March 31 2011, *COM(2011) 163 On Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'*.

[94] Christou, G., 2014, *The EU's Approach to Cyber Security*, EUSC Policy paper series, Warwick.

[95] European Commission, February 7 2013, *JOIN(2013) 1 Cybersecurity Strategy of the European Union: an*

endeavoured to safeguard Europeans assets both by dispensing more than 600 million of euros for developing cyber security projects and by adopting a specific set of legislative acts on network and information security. Besides, the strategy fosters cooperation within the member states and between the Union and external partners.

Cyber crime represented one of the three pillars of the European Agenda on Security[96] adopted in April 2015, and cyber security became a core issue of the Union's political priorities after its inclusion in the Digital Single Market Strategy[97] presented in May 2015.

In 2016 the European Union enriched its standard measures to deal with cyber threats[98] and to align the response of its member states by presenting the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[99] and by adopting the Directive on security of network and Information System (NIS Directive). The implementation of the NIS Directive by all the 28 countries will represent a milestone towards European cyber security.

In June 2017 the Council of the European Union has set a draft to develop the Cyber Diplomacy Toolbox[100] for a joint European diplomatic response to malicious cyber activities in the Union. The Toolbox would contribute to prevent conflicts arising in cyberspace and, consequentially, to assure greater stability and cooperation in international relations.

Finally, in September 2017 the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy made public their proposals for a new cyber strategy called "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[101]. This joint communication has been addressed to the European Parliament and the

Open, Safe and Secure Cyberspace.

[96] European Commission, April 28 2015, *COM(2015) 185 The European Agenda on Security*.

[97] European Commission, May 6 2015, *COM(2015) 192 A Digital Single Market Strategy for Europe*.

[98] European Commission, July 5 2016, *IP/16/2321 Commission signs agreement with industry on cybersecurity and steps up efforts to tacke cyber-threats,* Press release.

[99] European Commission, July 5 2016, *COM(2016) 410 Strengthening Europe Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*.

[100] Council of the European Union, June 7 2017, *9916/17 Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*.

[101] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, September 13 2017, *JOIN(2017) 450 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.*

Council of the European Union with the need to consider the blurring of criminal, political and strategic interests of both non-state and state actors.

2.1.2 Objectives

The European Commission has highlighted three key objectives in the cyber security sector[102]:

1. increasing cyber security capabilities and cooperation;
2. making the EU a strong player in cyber security;
3. mainstreaming cyber security in EU policies.

The first objective seeks at ensuring that all the capabilities of each Member State reach the same level of development and, furthermore, fosters an efficient cross-border cooperation and share of relevant information. The second one is more general and encourages the member states to be more ambitious in taking advantage of the growth of the cyber sector. Only by adopting the latest cutting-edge technology and by overcoming the current diversification and fragmentation in the European cyber security industry it will be possible to be competitive in a confrontation with the rest of the world. The last of the three objectives looks forward to including cyber security in the ordinary EU policy initiatives, in particular for those who deal with internet of things and smart grids.

The Cybersecurity Strategy adopted in 2013 sets five cyber security priority for the Union[103]:

1. increasing cyber resilience;
2. drastically reducing cyber crime;
3. developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. developing the industrial and technological resources for cyber security;
5. establishing a coherent international cyberspace policy for the EU and promote core EU values.

[102] European Commission, January 2017, *EU cybersecurity initiatives: working towards a more secure online environment*, Factsheet.

[103] European Commission, February 7 2013, *JOIN(2013) 1 Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*.

In their book “Cyber Security: Hacker, terroristi, spie e le nuove minacce del web”[104] the scholars Raffaele Marchetti and Roberta Mulas identify and comment these priorities. According to the two authors, to promote and improve the cyber resilience of the European Union not only implies the development of the cyber capabilities of its member states but also to promote a solid cooperation between its agencies and the private sector.

To tackle the cross border menace of cyber crime the EU and its members need an efficient legislation. This is the reason why the Union is committed to sustaining with financial means the strengthening of the member states' ability to investigate and fight cyber crime. The EU should thus also support specialized institutes of research and universities, forces of police and the private sector. Furthermore, the EU should better collaborate in supporting the activity of both EUROPOL and ICANN in tackling cyber crime and assuring accountability in the cyberspace.

The development of EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP) should focus on the investigation, answer and recovery of the most sophisticated cyber attacks, fostering the mixing of civil and military approaches. To achieve this objective, it is necessary that the High Representative of the Union and the national governments cooperate in evaluating and fostering the development of the cyber capabilities; commit themselves in drafting a political framework for the integration of cyber security in the CSDP; promote dialogue between the military and civil worlds, and between the member states and external international actors.

To effectively develop the industrial and technological resources for cyber security, the EU should promote a single market of products with high standard of quality with certification for cloud computing and the protection of data. The European Commission is in this case committed to stimulate private and public investments toward trusted, user-friendly, competitive and interoperable systems of hardware and software.

Last but not least, the EU seeks at filling the digital gap between the different member states not only by providing legal tools for tackling cyber crime but also by designing new models

[104] Marchetti, R., Mulas, R., 2017, *Cyber Security: Hacker, terroristi, spie e le nuove minacce del web*, LUISS University Press, Rome, pp. 137-138.

of cooperation between the states. Needless to say that the Union should work in favour of cooperating with external actors both at the bilateral and multilateral level.

Along with the three key objectives highlighted by the European Commission and the five cyber security priorities listed in the 2013 Cybersecurity Strategy, the EU has dealt with the issue also in the European Agenda on Security (2015), the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016), and the Cyber Diplomacy Toolbox (2017).

Set as one of the three priorities, the European Agenda on Security 2015-2020 has designed four actions to fight cyber crime[105]:

1. giving renewed emphasis to implementation of existing policies on cyber security, attacks against information systems, and combating child sexual exploitation;
2. reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016;
3. reviewing obstacles to criminal investigations on cyber crime, notably on issues of competent jurisdiction and rules on access to evidence and information;
4. enhancing cyber capacity building action under external assistance instruments.

The 2015 Digital Single Market Strategy has included cyber security in dealing with a public-private partnership (PPP) supported by the Horizon 2020 EU fund. The European Commission and the industry-led association European Cyber Security Organization (ECSO) has signed a partnership on the 5th of July 2016[106]. The goal of this partnership is to overcome fragmentation in the cyber security market, stimulate innovation and competitiveness, align the demand and supply for cyber security production and usage, and building a trustworthy relationship between the member states and industrial firms. The initiative includes a wide range of actors, which goes from producers of equipment and components to innovative small and medium enterprises (SMEs), from researchers to workers of the critical infrastructures. As a fact, the ECSO does not only consist of large companies, but also SMEs, start-ups,

[105] European Commission, April 28 2015, *COM(2015) 185 The European Agenda on Security*.

[106] European Commission, January 2017, *EU cybersecurity initiatives: working towards a more secure online environment*, Factsheet.

universities, public authorities, and clusters.

According to the European Union, this partnership could help to gather industrial and public resources to deliver innovation against a jointly-agreed strategic research and innovation roadmap; to focus on targeted technical priorities defined jointly with industry; to maximize the impact of available funds; and to provide visibility to European research and innovation excellence in cyber security.

In the July 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry the EU set the launch of additional market-oriented policy measures on cyber security. These aim at[107]:

1. stepping up cooperation across Europe;
2. supporting the emerging single market for cyber security products and services in the EU;
3. establishing a contractual public-private partnership (PPP).

To step up cooperation across Europe, the Commission strongly encourages the member states to prepare for a large scale cyber incident by cooperating together under the NIS Directive[108]. More cyber security exercises and training have to be included in the scheduled defence activities of the Union.

In order to support the emerging single market for cyber security products and services in the EU, the Commission is committed to create a certification framework for ICT products and services through labels for evaluating the level of quality of their security. Furthermore, the Commission intends to increase the value of the investments in cyber security products and services by supporting large and SMEs active in the European market.

Finally, the third aim of the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry the EU is headed to the establishment a contractual PPP with industry to develop innovation and European industrial capabilities.

[107] European Commission, July 5 2016, *COM(2016) 410 Strengthening Europe Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*.

[108] See section *2.1.3 Legal context* for more info on the NIS Directive.

The very last strategic act to boost European cyber security is the creation of a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities[109] in June 2017. Having recognised that malicious cyber activities might constitute wrongful acts under international law and upholding the principle that existing international law is applicable to cyberspace, supporting the ongoing work of the United Nations Groups of Governmental Experts on Developments (UN GGE) in the Field of Information and Telecommunications in the context of international security and the regional confidence building measures agreed by the Organization for Security and Cooperation in Europe (OSCE) to reduce the risk of conflicts stemming from the use of information and communication technologies, the EU and its member states have a strong commitment to actively support the development of voluntary, non-binding norms of responsible state behavior in cyberspace.

The creation of a Cyber Diplomacy Toolbox should foster cooperation, simplify the solution to immediate and long-term threats as well as being a deterrent to any potential aggression. The Union has affirmed that all the necessary measures within the Common Foreign and Security Policy (including restrictive measures), adopted under the relevant provision of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities. The development of this joint cyber diplomacy framework will be guided by the following six main principles:

1. serve to protect the integrity and security of the EU, its member states and their citizens;
2. take into account the broader context of the EU external relations with the State concerned;
3. provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment;
4. be based on a shared situational awareness agreed among the member states and correspond to the needs of the concrete situation in hand;
5. be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity;
6. respect applicable international law and must not violate fundamental rights and freedoms.

While, for the moment, the principles and goals of the 2013 EU Cybersecurity Strategy remain valid, the Commission and the High Representative have recently released a long and

[109] Council of the European Union, June 7 2017, *9916/17 Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*.

detailed joint communication[110] with proposals to enhance the cyber security strategy of the Union. In particular, the text focuses on three main priorities:
1. building EU resilience to cyber attacks;
2. creating effective EU cyber deterrence;
3. strengthening international cooperation on cyber security.

As for the first priority, the two European institutions aim at:
1. strengthening the European Union Agency for Network and Information Security (ENISA) by granting the Agency a permanent mandate which should provide support to the institutions, the member states, and the businesses. In particular, the reformed ENISA will have a strong advisory role both in developing and implementing cyber policies;
2. moving towards a Single Cybersecurity Market with a well-defined cyber security certification framework for schemes, products, services, and systems. In more depth, the Commission invites the relevant stakeholders to increase security in critical or high-risk applications, to apply regulatory obligations, and to use "security by design" methods in mass consumer devices;
3. implementing the Directive on the Security of Network and Information Systems (NIS Directive) in full[111];
4. increase resilience through rapid emergency response by applying a shared "Blueprint". This would provide an effective answer to large-scale cyber incidents both at the Union and member states levels;
5. creating a cybersecurity competence network with a European Cybersecurity Research and Competence Centre. The Commission will launch an assessment to examine available options;
6. building a strong EU cyber skills base by fostering ongoing educational activities for its staff;
7. promoting campaigns of cyber hygiene and awareness with the scope of trying to avoid human errors as much as possible.

In order to create an effective EU cyber deterrence, the Commission and the High

[110] European Commission, September 13 2017, *JOIN(2017) 450 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.
[111] See section *2.1.3 Legal context* for more information on the NIS Directive.

Representative are committed to provide support to the member states in:
1. the identification of malicious actors;
2. the step up of the law enforcement response for investigation and prosecution;
3. the boost of public-private cooperation against cybercrime;
4. the step up of the political response, in line with the Cyber Diplomacy Toolbox;
5. the building of cyber security deterrence through the member states' defence capability.

As for the strengthening of international cooperation on cyber security, the two institutions support:
1. the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements. In particular, the EU supports the work of both the UN GGE and OSCE;
2. the building of national resilience in third countries;
3. the deepen of the EU-NATO cooperation on cyber security, hybrid threat and defence[112].

2.1.3 Legal context

The landmark of the legal context for ensuring a high common level of cyber security in the European Union is the Directive on security of Network and Information Systems (NIS Directive)[113]. After a period of negotiations, the Directive has been agreed by the European Parliament, the Council and the Commission on the 7th of December 2015. The text was adopted by the Parliament on the 6th of July 2016 and entered into force in August of the very same year. Member states will have up to 21 months to accept the Directive into their national laws and 6 months more to identify operators of essential services.

The directive is built on three main pillars[114]:
1. ensuring member states preparedness;
2. ensuring cooperation among all the member states;

[112] See section *3.2 The EU-NATO cyber diplomacy* for more information on the EU-NATO cooperation.

[113] European Parliament and Council of the European Union, July 6 2016, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*.

[114] Ibid.

3. ensuring a culture of security.

The first pillar requires member states to be appropriately equipped against cyber malicious acts with both a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority. The second one sets the creation of both a CSIRT Network and a Cooperation Group in order to accelerate and facilitate exchange of information and strategic cooperation in cyber security among the member states. The last pillar is more general and is headed to ensure a culture of security across sectors which rely on ICTs and are vital for the European society and economy. Under the NIS Directive, all the relevant businesses will necessarily have to take appropriate security measures and to notify cyber incidents to the national authority. These include critical infrastructures like communication, energy, transport, healthcare, and finance but also digital service providers like search engines, cloud computing services and online marketplaces.

Along with the NIS Directive, three EU legislative actions contribute in fighting cyber crime: the Framework Decision on combating fraud and counterfeiting of non-cash means of payment[115], a Directive on combating the sexual exploitation of children online and child pornography[116], and a Directive on attacks against information systems[117]. The first was adopted in 2001 and defines the fraudulent behaviors that the EU states need to consider as punishable criminal offences. Due to its old drafting, the Commission needs to update the Framework with virtual currencies and new forms of money transmission. The second legislative action is more recent as it was adopted in 2011 and deals with sexual exploitation of children and child pornography online. It takes into account new developments in the cyberspace. The last action was adopted in 2013. The Directive on attacks against information systems aims at tackling large-scale cyber attacks towards the EU. It introduces through criminal sanction and strengthens national cyber crime laws. The implementation has not yet been developed by all the member states.

[115] Council of the European Union, May 28 2001, *2001/413/JHA Combating fraud and counterfeiting of non-cash means of payment*.

[116] European Parliament and Council of the European Union, December 13 2011, *Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.*

[117] European Parliament and Council of the European Union, August 12 2013, *Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*.

2.1.4 Agencies and measures

The operative body of the European cyber security structure is mainly made of three agencies[118]: the European Union Agency for Network and Information Security (ENISA), the EU Computer Emergency Response Team (CERT-EU), and the Europol's Cybercrime Centre (EC3).

The European Union Agency for Network and Information Security was set up in 2004 to help the European Commission, the governments of the member states and the relevant business community to prevent, address and respond to malicious acts in the European networks and information systems. In more depth, ENISA collects and analyses security data incidents; promotes the assessment and management of emerging risks; runs joint European cyber exercises; manages the cooperation between each member states' Computer Emergency Response Team (CERT); and support the cooperation of different actors in the field of information security. ENISA's current mandate will expire in 2020, but the Commission is currently revising its tasks and outputs in order to evaluate for a more large action and a reinforced role[119].

The EU Computer Emergency Response Team is newer and institutional-made. The CERT-EU was set up in 2012 with the aim to provide an efficient response to cyber threats and incidents arising in the cyberspace directed toward the European institutions, bodies, and agencies. The Team is made up of many different experts directly coming from the European Commission, the General Secretariat of the Council, the European Parliament, the Committee of the Regions and the Economic and Social Committee. Furthermore, CERT-EU cooperates with the CERTs of the member states.

The Europol's Cybercrime Centre is an integral part of Europol and was set up in 2013. EC3 represents the EU law enforcement community in the field of cyber security and its main role is to tackle cross-border cyber crime by serving as a hub for criminal information and intelligence. It also supports investigations and operations of the Members States with highly

[118] European Commission, January 2017, *EU cybersecurity initiatives: working towards a more secure online environment*, Factsheet.

[119] European Commission, January 18 2017, *Public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA)*.

specialized technical and digital forensic experts; coordinates training and capacity building measures; provides strategic reports and analysis; and communicates with external cyber crime related agencies, public and private partners, to enhance cooperation amongst them.

2.1.5 Funding

The European Union has obviously invested different amount of money in different periods of time. The political and economic situation, as well as the nature of the menaces arising in the cyberspace, have set various European budgets for cyber security. For the 2007-2013 period, the Union has invested €334 million in the field[120]. In particular, the endeavour of the Union has been addressed to the creation of trustworthy networks and service infrastructures. Other relevant topics like cyber crime, risk analysis for infrastructure protection, money laundering, dedicated road mapping actions, cryptology, and advanced biometric were addressed under the Seventh Framework Programme (FP7) and the Competitiveness and Innovation Programme (CIP). The Commission has been also funding the Prevention and Fight against Crime Programme (ISEC 2007-2013) which has contributed around €15 million to the fight against cyber crime since 2007.

For the 2014-2016 period, the European Union has invested €160 million in cyber security under the Horizon 2020 Research and Innovation Framework Programme (H2020). The Programme was composed of two parts, one dedicated to the protection of the European citizens and one of the European technologies. The European Structural and Investment (ESI) Funds foresee a contribution of up to €400 million for investments in trust and cyber security for the same period. The ESI Funds are directed to financing in security and data protection with the support of the Digital Service Infrastructures (DSIs) stream within the Connecting Europe Facility (CEF). The principal aim is to reach cross-border cooperation in the cyber security field, by enhancing the security and trust in communications and contributions. For the same period, the Commission has funded the successor to ISEC, the Internal Security Fund (ISF) with a total budget slightly over €1 billion available for funding actions under the ISF Police instrument, including the fight against cyber crime.

[120] European Commission, January 2017, *EU cybersecurity initiatives: working towards a more secure online environment*, Factsheet.

For the 2017-2020 period, the EU will also invest up to €450 million of the Horizon 2020 Research and Innovation Framework Programme funding several contractual public-private partnerships on cyber security and addressing funds to building engagements in third countries. As a fact, the EU has recognized a strong connection between sustainable development and cyber resilience. With the aim of developing the capabilities of third countries, the Instrument contributing to Stability and Peace (IcSP) has provided €4.5 million back in 2013, and €21.5 million over the period 2014-2017. The European Neighbourhood Instrument (ENI) has then helped countries of the Eastern Partnership (Ukraine, Moldova, Georgia, Belarus, Azerbaijan, and Armenia) to define cyber security priorities, while the Instrument of Pre-accession (IPA) has financed with €5 million countries in South-Eastern Europe and Turkey to cooperate on cyber crime[121].

Finally, in the joint communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy have advanced the idea of creating a Cybersecurity Emergency Response Fund which could complement the existing crisis management mechanisms[122]. This would allow member states to receive further help in dealing with major incidents as well as better handling risks and opportunities which derive from the use of cyber tools.

2.2 The NATO cyber security strategy

2.2.1 Evolution and background

The North Atlantic Treaty Organization started to identify the critical relevance of cyber threats for the security of its members back in 1999[123]. In fact, the biggest military alliance in the world has been exposed to cyber attacks carried out by hacktivists from Serbia, Russia, and China during Operation Allied Force in Yugoslavia. As a consequence, NATO has insert

[121] Ibid.

[122] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, September 13 2017, *JOIN(2017) 450 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, p. 8.

[123] Healey, J., Van Bochoven, L., 2011, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, p. 1.

cyber defense into its political agenda, developing an own strategy to assure more security to its members. In 2002, during the Prague Summit, the Alliance adopted the Cyber Defence Program[124] and created the first responder to prevent, detect and respond to cyber malicious acts, namely NATO Computer Incident Response Capability (NCIRC)[125].

At the time, the approach of the organisation to cyber security was merely technical, with the adoption of the 2002 Prague Capabilities Commitment[126] and the 2005 Comprehensive Political Guidance[127]. Things changed in 2007 when NATO understood the political implications of the very well-known cyber attacks that hit Estonian networks. Even though it has been impossible to clearly detect the source of the attack, this event is generally considered to be the first case of cyber warfare[128]. This obviously had posed a problem to NATO that goes over the mere defence, but the necessity to regulate the relationship between two countries at war in a new dimension not considered in international law and law of war.

The 2008 Bucharest Summit has brought out the first NATO cyber security policy, emphasizing the need to protect key information systems; to share best practices; and to provide a capability to assist Allied nations, upon request, to counter a cyber attack[129]. The Alliance then established two institutions: Cyber Defence Management Authority (CDMA) and the Cooperative Cyber Defence Center of Excellence (CCDCOE). The first, under the governance of the Cyber Defence Management Board (CDMB), became operational in 2008 aiming at managing and coordinating the allied cyber defence, mitigating risks and helping the member states to improve their own operative capabilities[130]. On the other side, the CCDCOE does not have an operational soul but rather it is focused on education, research, and development. Since 2008, its mission is to reinforce the capabilities of the Alliance, the cooperation and the share of information within NATO and between the member states and

[124] NATO, November 21 2002, *(2002)127 Prague Summit Declaration*.

[125] Healey, J., Van Bochoven, L., 2011, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, p. 2.

[126] NATO, November 21 2002, *Prague Capabilities Commitment*. Link: http://www.nato.int/cps/en/natohq/topics_50087.htm

[127] NATO, December 21 2005, *Comprehensive Political Guidance*. Link: http://www.nato.int/cps/on/natohq/topics_49176.htm

[128] Blank, S. J., 2008, *Web War I. Is Europe's First Information War a New Kind of War?*, Comparative Strategy, 27 (3), pp. 227-247.

[129] NATO, February 17 2017, *Cyber Defence*. Link: http://www.nato.int/cps/en/natohq/topics_78170.htm

[130] Healey, J., Van Bochoven, L., 2011, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, p. 2.

external actors.

In 2010, for the first time, cyber defence was included into NATO's Strategic Concept[131]. Adopted during the Lisbon Summit, NATO leaders recognized the importance of improving its capabilities in dealing with a cyber attack. Even though the Lisbon Capabilities Package[132] drafted how to detect, assess, prevent, defend, and recover from a malicious act, a full comprehension of the issue has been provided with the adoption of the Cyber Defence Policy and Action Plan in 2011[133]. The member states endorsed the Policy and Action Plan at the Wales Summit of 2014.

Two years later, at the Warsaw Summit, NATO allies committed to strengthen and enhance the cyber defences of national infrastructures and networks through the Cyber Defence Pledge[134]. The Summit represents a milestone in the evolution of NATO's cyber defence as all the 29 leaders of the member states agreed in recognizing cyberspace as an operational domain, in addition to land, sea, air, and space. This new approach toward cyberspace constitutes a pivotal step into NATO's cyber strategy based on collective defence and resilience[135]. Finally, in February 2017, defence ministers of the member states implemented this perception of the cyberspace with a roadmap and an updated Cyber Defence Plan[136].

2.2.2 Objectives

The strategy of NATO on cyber security is based on two core principles and two main references[137]. The principles are collective defence and resilience, the references are the Cyber Defence Policy and Action Plan and the Cyber Defence Pledge.

The principle of collective defence (regulated by article 5 of the Washington Treaty) is the pivotal point of NATO's security policy and the existence of the Alliance itself. In more depth,

[131] NATO, November 20 2010, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*.

[132] NATO, November 20 2010, (2010)155 *Lisbon Summit Declaration*.

[133] NATO, August 19 2011, *Defending the networks: the NATO Policy on Cyber Defence*.

[134] NATO, July 8 2016, (2016)124 *Cyber Defence Pledge*.

[135] See Section *2.2.2 Objectives* for details about NATO's cyber strategy.

[136] NATO, February 17 2017, *Cyber Defence*. Link: http://www.nato.int/cps/en/natohq/topics_78170.htm

[137] NATO, April 2017, *NATO Cyber Defence,* Factsheet.

the concept of collective defence means that an attack against an ally has to be considered as an attack against all the other members. This obliges the Alliance as a group to rescue one in case of attack. With the recognition of the cyberspace as an operational domain during the Warsaw Summit the concept of collective defence is extended also to potential cyber attacks against the Alliance or its members.

In accordance with this principle, the activities of NATO have been revolutionized both externally and internally[138]. From an external point of view, the activity of deterrence and collective defence have been extended to cyberspace. From an internal point of view, NATO is responsible for the defence of its network and has to act consequentially on three levels to provide support to its members: capacity development, capacity building, and crisis management. These three macro-areas take care respectively of improving the means for sharing information between the member states and promote a more deep knowledge of the existing threats; educate and train the personnel on technical, operational and strategical areas of cyber defence; and create the Rapid Reaction Teams (RRTs) available for the member states to respond to cyber attacks. All this set of activities is intended to thus strengthen NATO system because the security of the Alliance, its capacity to effectively answer to a call of collective defence, to manage crisis and to cooperate is largely dependent on the cyber capabilities of each member states.

Another extremely important concept of NATO's cyber security strategy is resilience. Resilience is here perceived as a consequence of deterrence measures and a guarantee for a more comprehensive approach to security. At the Warsaw Summit of 2016 it has been discussed the centrality of the cyber dimension for a set of reasons that fit all the spectrum of a cyber crisis:

1. continuity of governance and its critical services;
2. resilience of energetic supplies;
3. capacity of effectively manage uncontrolled movement of people;
4. resilience of food and hydric resources;
5. capacity of managing mass damages;
6. resilience of communication systems;

[138] Marchetti, R., Mulas, R., 2017, *Cyber Security: Hacker, terroristi, spie e le nuove minacce del web*, LUISS University Press, Rome, p. 131.

7. resilience of transportation system.

The Cyber Defence Policy and Action Plan was adopted in June 2011, while NATO was conducting air operations during the Libyan crisis. The Policy aims at boosting NATO's response capabilities and operational mechanism by providing assistance and training. The main elements of this new approach are[139]:

1. the realization that cyber defence is required to perform NATO's core tasks of collective defence and crisis management;
2. the prevention, resilience, and defence of cyber assets critical to NATO and its constituent allies;
3. the implementation of robust cyber defence capabilities and centralized protection of NATO's own networks;
4. the definition of minimum requirements for cyber defence of national networks critical to NATO's core tasks;
5. the assistance to the allies to achieve a minimum level of cyber defence to reduce vulnerabilities of national critical infrastructure;
6. the engagement with partners, other international organizations, the private sector, and academia.

The Cyber Defence Pledge of July 2016 is the main output on cyber security of the Warsaw Summit. The allies now consider cyberspace to be an operational domain along with land, sea, air, and space, and thus stating that international law applies to disputes arising in the cyberspace. In this case, the top priority of NATO is the protection of the communications and information systems owned and operated by the Alliance but the policy also provides for the integration of cyber defence into operational planning (including the civilian emergency one) and for assistance in case of cyber attack[140]. NATO policy also encourages more cooperation both at the internal and at the external levels. It aims at boosting innovation and research, enhancing information sharing, exchange of best practices, and lessons learned, with other international organizations and industries.

The acceptance of cyberspace as an operational domain does not change NATO's mandate,

[139] NATO, August 19 2011, *Defending the networks: the NATO Policy on Cyber Defence*.

[140] NATO, July 8 2016, *(2016)124 Cyber Defence Pledge*.

which action is strictly defensive, proportionate and in line with international law. As a fact, the first responsibles for their own cyber security are the allies. With the Cyber Defence Pledge they affirm their utmost intention to:

1. develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;
2. allocate adequate resources nationally to strengthen our cyber defence capabilities;
3. reinforce the interaction amongst our respective national cyber defence stakeholders to deepen cooperation and the exchange of best practices;
4. improve our understanding of cyber threats, including the sharing of information and assessments;
5. enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
6. foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;
7. expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.

2.2.3 Legal context

The fundamental document of NATO's legal framework for cyber security is the Tallinn Manual on the International Law applicable to Cyber Warfare. The Tallinn Manual is a product of the NATO Cooperative Cyber Defence Centre of Excellence and it has been published in two editions, one in 2013 and a more recent one in 2017. The documents provide an analysis of the current law concerning *jus ad bellum* and *jus in bello,* affirming that it is up to international law to regulate the actions of states into cyberspace[141]. The new edition of the Manual updates and expand the previous one. The focus of the Tallinn Manual 2.0 is not limited only to the major cyber operations that can lead to an armed conflict, but rather

[141] Schmitt, M. N., 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press. Schmitt, M. N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press.

examines in depth also the various range of criminal incidents that more often seek to damage the states. Both the 2013 and the 2017 manuals together represent an important source to comprehend the normative framework of cyberspace. In particular, the Tallinn Manual 2.0 offers a set of guidelines on how states can define rules of engagement, countermeasures, retaliation operations, and other forms of response within the context of the international law if they are to face an act of cyber aggression.

Even though NATO now consider cyber attacks as a potential reason for triggering article 5 of the North Atlantic Treaty, the Alliance's posture on cyber security still maintains a rather defensive posture[142]. The doctrine on crisis management still fails to recognize cyber threats as a force that can easily spread from one nation to another. The reason is that the members of the Alliance are far from adopting a common view on the conditions in which the use of force may apply if one of its member states suffers a malicious act on cyberspace. With more cyber laws and policies generally agreed, NATO could boost its military and political leadership role, instead of having to judge each individual case of cyber attack without the support of standard measures.

The trigger of article 5 may appear to be more obvious when the entity of the attack is of large scale, hits multiple targets and is easily detectable. However, there is an incredible need to define the policy of response mostly for small intrusions, as they account for the ordinary activity in the cyberspace. Technological advances and a skyrocket in connectivity expose the citizens to the same risks of the states, the SMEs to the same risks of the Multinational Corporations (MNCs). NATO policy on cyber security still has many zones that are not clearly and standardly regulated. These zones are the ideal places for an attack conducted without risking a triggering of article 5.

2.2.4 Agencies and measures

Although the main responsibility for cyber security remains up to the member states, NATO's

[142] Lété, B., Dege, D., 2017, *NATO Cybersecurity: a Roadmap to Resilience*, The German Marshall Fund of the United States, Policy Brief No. 23, p 3.

active response to cyber threats is also safeguarded by a various range of agencies and bodies[143]. The main actor which work directly within the Alliance is the NATO Computer Incident Response Capability (NCIRC). The NATO Computer Incident Response Capability is based in Mons (Belgium) within the Supreme Headquarters Allied Power Europe (SHAPE). NCIRC can rely on Rapid Reaction Teams (RRTs) with the intent of protecting the Alliance computer networks through an ongoing cyber defence support. The team is made up of 200 experts from all the member states and its tasks include: sharing real-time information about threats through a dedicated malware information sharing platform, as well as best practices for handling cyber threats; maintaining rapid reaction cyber defence teams that can be sent to help allies in handling cyber challenges; developing targets for allies to facilitate a common approach to their cyber defence capabilities; and investing in education, training and exercises.

The cyber defence capability of the North Atlantic Treaty Organization is also made up of a various set of associated bodies[144]: the NATO Communications and Information Agency (NCIA), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCE), the NATO Cyber Range, the NATO Communications and Information Systems School, the NATO Defence College, and the NATO School.

The NATO Communications and Information (NCI) Agency was established on 2012 in Brussels (Belgium) as a result of the merger of the NATO Consultation, Command and Control Agency (NC3A), the NATO ACCS Management Agency (NACMA), the NATO Communication and Information Systems Services Agency (NCSA), the ALTBMD Programme Office and elements of NATO HQ ICTM. The Agency works without stop and fulfils a large set of task. They include: connecting the Alliance; defending its networks; providing rapid support to NATO operations and missions; delivering critical capabilities; assisting NATO and partners through bilateral and multinational projects on developing interoperable and cost-effective capabilities in the area of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR); and supporting nations in cost-effective certification of their NATO Response Force elements by re-using solutions tried and tested in Afghanistan.

[143] NATO, April 2017, *NATO Cyber Defence,* Factsheet.

[144] Ibid.

The NATO Cooperative Cyber Defence Centre of Excellence is located in Tallinn, Estonia. Although it is not part of the NATO Command Structure, the CCDCE provides expertise and experience on cyber defence. In fact, the Centre does not have an operational cyber mission but rather complement with the NATO Computer Incident Response Capability and the Cyber Defense Management Board. Its mission is to improve information sharing and cooperation in general, but also deal with research, development, and lessons learned. Furthermore, the Center has been particularly active for providing legal support to the management of cyber defence within the Alliance. Among its various contributions, there are two editions of the Tallinn Manual on the application of international law to cyber warfare and annual joint exercises called Cyber Coalition for testing member states' cyber readiness and capabilities under NATO flagship, which is generally managed by the NATO Cyber Range located in Tartu, Estonia.

NATO also provides its personnel from the member states with a top quality education in the field of cyber security. The NATO Communications and Information Systems School is based in Latina (Italy) but it will be soon relocated to Oeiras, Portugal. The School is focused on operation and maintenance of NATO communication and information systems. The NATO Defence College, based in Rome (Italy), fosters strategic thinking on political-military matters, including on cyber defence issues. Lastly, the NATO School in Oberammergau (Germany) also provides cyber defence-related education and training to support Alliance operations, strategy, policy, doctrine, and procedures.

2.2.5 Funding

During the Warsaw Summit, the delegation leaders of NATO member countries have positively accepted an increase in budget for cyber defence for the first time since 2009[145]. The budget increase is needed to reinforce the Alliance's cyber capabilities, as well as air defence, satellite communications, the Response Force, and the chain of command and control for multinational operations that require the use of cyberspace.

[145] NCI Agency, March 27 2017, *NATO gears up for 3 billion EUR tech refresh*, Communication.

While NATO's budget for cyber security only is not currently available through open sources[146], it has been known recently that the Alliance has sought bids for business projects for a total of €3 billion[147]. The NATO Communications and Information Agency presented the call at the annual NITEC Conference, which took place in April 2017 in Ottawa (Canada). NATO expects to complete the first round in September 2071[148]. For this round, the Alliance will invest the largest part of the €3 billion budget (approximately €1.5 billion) in the expansion of satellite communication bandwidth because of its vital role in the deployment of forces. €320 million will then be devoted to the renewal of air command and control. Over €70 million will be invested in the new NATO messaging service and information services. To improve logistics for multinational operations, NATO will allocate €30 million. €27 million will be given to the improvement of service management and control in order to improve the capabilities of situational awareness and command and control in operations. Finally, the Alliance will allocate €8 million to the joint targeting system and €2 million will be used to renew NATO's command and control software for land operations.

Considering the increasingly fluid and asymmetric nature of cyber threats, one of the key objectives of increasing the budget is to seek greater partnership between public and private sectors, in particular by taking into account the presence of small and medium-sized enterprises that could be crucial in this sector. It is important to remark the presence of 1500 industry representatives who attended the discussion that led to the final decision of a necessary Alliance budget increase for cyber security. In this regard, NCIA's General Manager Koen Gijsbers underlined that the private sector, for its creative ability and spirit of ingenuity, has always established a strong asset of NATO. If the Alliance has succeeded in cutting edge technology and facing external threats for 67 years, it is also thanks to the ability of its private sector that continue to innovate and renew itself. Only a continuous and rapid innovation process can ensure NATO's resilience. In line with this mindset, these business opportunities will be followed by a new round of invitations for bids in 2018. The new round will be launched in order to renew NATO's cyber shield, invest in education and training, air command and control, ballistic missile defence, intelligence surveillance and reconnaissance, business applications and advanced software to support NATO's operations[149].

[146] Cf. NATO, June 29 2017, *Defence Expenditure of NATO Countries (2010-2017)*, Press release.

[147] NCI Agency, April 25 2017, *NATO launches first bids under major tech refresh,* Communication.

[148] Ibid.

[149] Ibid.

3. NEW THREAT, NEW COOPERATION

3.1 Attacks, challenges and prospects

3.1.1 An overview of global cyber threat

The European Union and the North Atlantic Treaty Organization share common values, strategic interests and 22 of their member states belong to both organisations. The transatlantic community is bound by a shared view of free democracies, with free electors who elect free parliaments that develop free economies. These values are increasingly threatened by state and non-state actors, who exploit cyber domination through psychological operations, fake news and other malicious acts to undermine their fundamentals.

Although at present it is impossible to find open source official data on the state of the cyber threat with respect solely to the European Union and the North Atlantic Alliance, useful information for a comprehensive and up-to-date idea of the threat can be found by consulting the 2017 Clusit Report on cyber security[150]. Each year, the very well-known association for Italian IT security publishes the aggregated statistics related to all the cyber events collected during the previous year. It should be emphasized that the statistics and comments below are related to a sample that is necessarily limited, albeit fairly significant, compared to the number of serious computer attacks actually occurred in the period under review. This is because most of the attacks do not become of public domain before a few years.

Before analysing the data relative to the cyber attacks, it is worthy to consider that the areas of origin of the victims, during the year 2016, were so subdivided[151]: 53% of the victims reside in the Americas, 16% of them in Asia, another 16% in the European continent, 3% in Africa, and only 1% in Oceania. The attacks on multinational victims represent 11% of the total, a high number that shows the trend to strike increasingly important targets of a transnational nature. On the contrary, it is extremely difficult to identify with certainty the origin of these attacks. Since cyberspace is a borderless territory in which it is relatively easy to hide its

[150] Clusit, 2017, *Rapporto Clusit 2017 sulla sicurezza ICT in Italia*, Astrea, Milano.
[151] Ibid., p. 26.

identity, detection still represents one of the main challenges of cyber security.

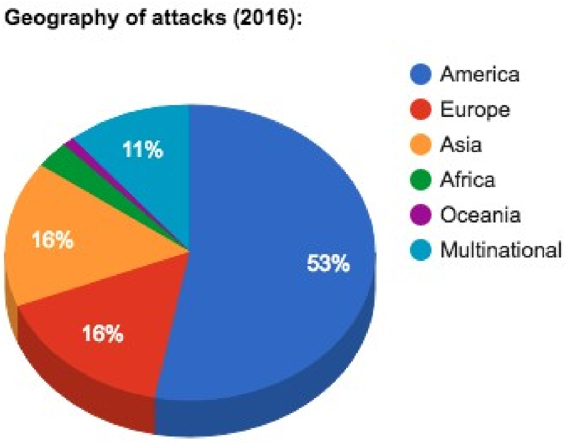

Figure 1. Geography of attacks (2016) (Clusit, 2017)

The study is based on a total sample of 1.050 known severity-related attacks that have had a significant impact on victims in terms of economic losses, reputation damage, the dissemination of sensitive (personal and non-sensitive) data, or which, however, prefigure particularly worrying scenarios that took place in the world from January 1 to December 31, 2016. In 2016, the number of events (1.050) has exceeded those of 2014 (873) and 2015 (1,012) with a rise of 3.75% from the last year[152].

From 2015 to 2016, the percentages of events motivated by cyber crime raised from 68% to 72%, while hacktivism dropped to 15% from 20%. cyber espionage remained essentially stable (9% in 2015 and 8% in 2016), whereas activities of cyber warfare have more than doubled its share (from 2.4% to 5%) even if the overall value is still low[153.]

[152] Ibid., p. 19.
[153] Ibid., p. 20.

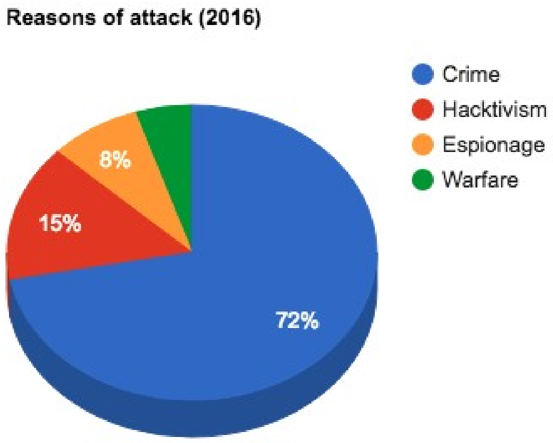

Figure 2. Reasons of attack (2016) (Clusit, 2017)

For an analysis of the trends on the reasons of the attack, the Internet Status/Security Q2 2017 Report[154] of Akamai, the Internet Security Threat Report Volume 22[155] of Symantec, and the 2017 Threats Predictions[156] di McAfee Labs have been confronted. From these data has emerged that in early 2017, cyber crime was at 75.68%, cyber espionage at 16.08%, hacktivism at 5.9% and cyber warfare at 2.34%. This suggests a remarkable growth in the field of espionage and a steady decline in hacktivism, while cyber crime remains the biggest reason behind the attacks.

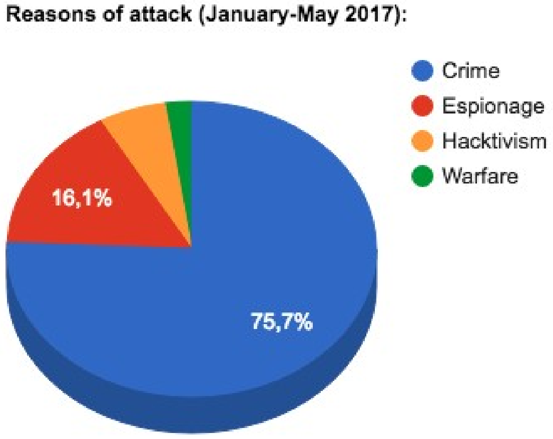

Figure 3. Reasons of attack (January-May 2017) (Akamai, Symantec, McAfee Lab, 2017)

The diversification of cyber targets is constantly raising, in particular on healthcare (+102%

[154] Akamai, 2017, *State of the internet/Security Q2 2017 Report*, 4 (2), Cambridge.
[155] Symantec, 2017, *Internet Security Threat Report (ISTR)*, 22, Cupertino.
[156] McAfee Labs, 2016, *2017 Threats Predictions*, Santa Clara.

from 2015 to 2016), retail (+70%), and banking and finance (+64%) sectors. However, the distribution of target confirms governments on top of the attackers' preferences with 21% of the total share, even if decreasing. According to Clusit, online services/cloud ranks second with 17%, followed by news and entertainment sector (13%), banking and finance (10%), and healthcare (7%). Software/hardware vendor and research/education account for 5% each, as well as a group of multiple targets. The remaining 18% is made up of critical infrastructures, retail, hospitality, telecommunications, organizations, government contractors/consulting, religion, and other[157].

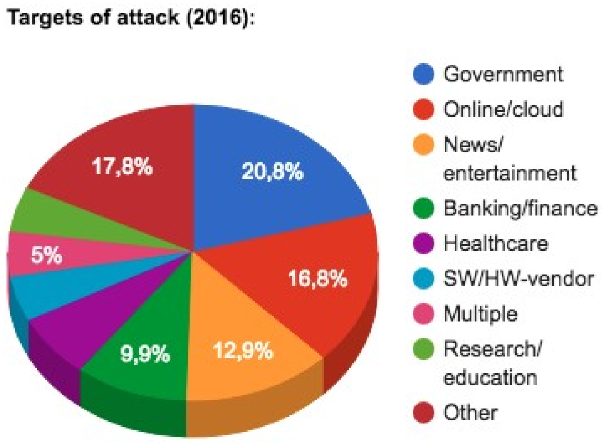

Figure 4. Targets of attack (2016) (Clusit, 2017)

From the crossing of the data of the three above mentioned reports, it has emerged that industry has faced a reduction in cyber attacks from 25.2% in 2015 to 24.8% in 2016, as well as governments from 13.7% to 11.9%. While the number of attacks towards organizations has remained stable (8.3% in 2015 and 8.2% in 2016), the one against individuals has raised from 4.9% to 9.3%. In the first half of 2017, industry was at 26.68%, government at 14.92%, organizations at 5.14%, and individuals at 12.2%. Although government is the single most targeted sector, which goes hand in hand with a steady growth in cyber espionage, it should be stressed how the industry sector still represents the major interest of cyber criminals. Obviously, for most of the non-state actors operating in the cyberspace, the biggest gains come from fraud in the private sector.

[157] Clusit, 2017, *Rapporto Clusit 2017 sulla sicurezza ICT in Italia*, Astrea, Milano, p. 24.

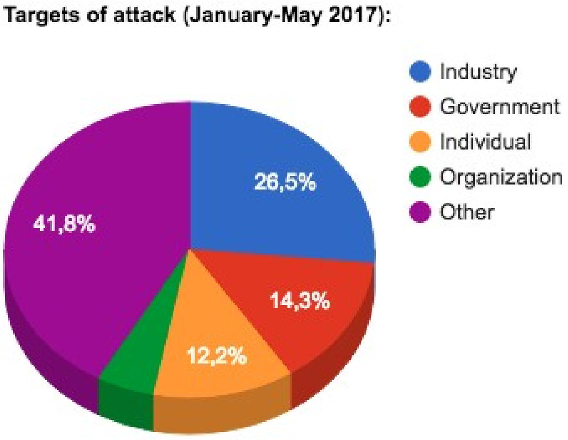

Figure 5. Targets of attack (January-May 2017) (Akamai, Symantec, McAfee Lab, 2017)

As for the types of attack employed in 2016[158], Clusit has registered the increase in malware (+ 116%), DDoS (+ 13%) and the use of "0-day" vulnerabilities (+ 333%). In particular, the category of phishing/social engineering activities has grown by 1.166%. Known vulnerabilities/misconfigurations, which had been strong last year, has shown a certain downturn (-26%) in 2016, demonstrating that although defenders have begun implementing a certain level of countermeasures, attackers can now rely on the use of malware (mostly ransomware) and social engineering techniques, deemed to be easier for achieving the vast majority of their goals. However, unknown techniques still lead the top of the list with 32% of the total, mainly because of the scarcity of accurate information that can be found in the public domain.

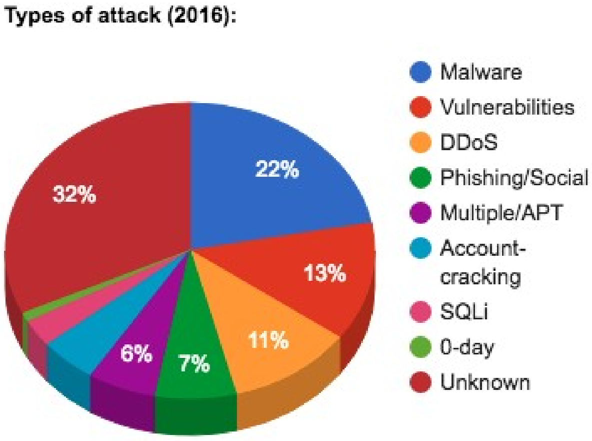

Figure 6. Types of attack (2016) (Clusit, 2017)

[158] Ibid., pp. 28-29.

According to the three reports, for the same period (2015-2016), the percentage of unknown attacks has raised from 24% to 33%. This increasing number is perfectly in line with the growing sophistication of the threat. Account hijackings also experienced a noticeable growth to 15.1% from 8.8%. Targeted attacks reported a light growth from 10.5% to 11.6%, similarly to Distributed Denial of Services (9.7 in 2015 and 11.3% in 2016) and malware (6.4% and 8.0%). Lastly, both SQL injections and defacement attacks reported a considerable drop (maybe related to the decreasing impact of hacktivism among the motivations), while malvertising is essentially stable (from 2.1 to 1.8%). In the first half of 2017, hijacking was at 14.78%, targeted attacks at 15.76%, DDoS at 3.98%, malware at 23.96%, SQLi at 1.8%, defacement at 3.1%, and malvertising at 1.4%.

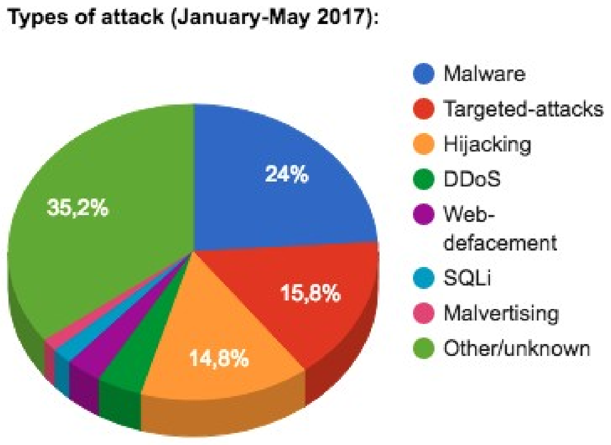

Figure 7. Types of attack (January-May 2017) (Akamai, Symantec, McAfee Lab, 2017)

Given that the analysis takes into account the most serious attacks of the recent period against primary public and private organizations, often at a global level, the fact that the sum of the banalest attacks techniques (like SQLi, DDoS, known vulnerabilities, and relatively-simple malware) represents more than half of the total, implies that attackers still succeed in making attacks against their victims with too little simplicity and low costs. On the very other side, defending requires high costs and complex structures. Based on these results, it is quite simple to realize how much the spectrum of threats that rely on the cyberspace is bound to grow more and more in the future. On the contrary, it is not trivial to guess what these threats will be. By taking into consideration both the threat landscapes and the emerging trends in technology, it can be attempted to anticipate what the future challenges of cyber security will be.

3.1.2 The future challenges of cyber security

As technology continues to evolve so do the opportunities and challenges it provides. In particular, the ever-increasing dependence on technologies exposes us to the whole set of risks associated with cyber attacks. Defending physical and virtual structures, therefore, becomes an indispensable must of governments, organizations, firms, and individuals. To this end, quantum computing could solve many of the problems currently affecting the use of cyberspace.

Quantum computers are devices that use the laws of quantum mechanics to implement computation[159]. Since quantum mechanics allows for a greater kind of parallelism than classical computer, quantum computers are expected to outperform the faster supercomputers in selected computational tasks. While currently there is no fully functioning quantum computer, a number of governments and industrial players have started to invest substantially in the field. In this respect, Google, Intel, Microsoft, IBM, and Alibaba are at the forefront. Government like the UK, USA, China, and the Netherlands have founded research centres specifically devoted to the construction of quantum computers. The main obstacle for implementation of such machines is the difficulty in controlling the noise that arises during the computation. However, fault-tolerant models have been designed and are currently under investigation. Given that it is expected a fully functioning quantum computer will be available during the next 10 years, the market for technologies related to quantum computer is projected to surpass US$5 billions through 2020[160]. The first applications of quantum computers will be in simulation of quantum mechanical systems and simulation of chemical processes. For example, the fixation of nitrogen, which today uses about 1% of the annual global production of natural gas on the planet. Simulating such processes computationally is the key to reproduce them in laboratory and substantially save resources.

What is the role of quantum computers in relation to cryptography and cyber security? The RSA algorithm, from the name of the inventors Rivest, Shamir, and Adleman, is the most used

[159] Hey, T., 1999, *Quantum Computing: an Introduction*, Computing and Engineering Journal, 10 (3), pp. 105-112.

[160] Market Research Media, June 14 2017, *Quantum Computing Market Forecast 2017-2022*, Tabular Analysis. Link: https://www.marketresearchmedia.com/?p=850

public-key cryptosystem[161]. RSA is used in many real-world applications including commercial satellite radio, satellite TV, eCommerce, and validation of websites beginning with "https://". RSA is currently not covered by a patent and it has been used since 1977. The core idea of RSA is that a large number is computationally hard to be factored into two large prime numbers. "Computationally hard" means that a computer takes long time to solve the problem. Indeed if all computers on the planet would be put together, under mild conditions, it would be impossible to break the RSA cryptosystem in less than years, a time which is sufficiently long for all practical applications to run.

In 1994, Peter Shor, a scientist at the time working at AT&T designed a "quantum algorithm", that is an algorithm running on a quantum computer, which is able to break RSA in a time exponentially smaller than the best-known algorithms that could run on standard computers[162]. This result has been a milestone in the theory of computation because it suggested that quantum computer can outperform classical computers. Since a quantum computer is still not available it is expected that RSA and related cryptosystems will be secure for at least 15-20, according to the NISTIR 9105, Report of Post-Quantum Cryptography[163]. Still, given that there is no clear understanding of the capabilities of quantum computers, it is important that cryptosystems are today secure against attacks done with quantum computers. The field of post-quantum cryptography studies specifically the type of protocols that can be safe against quantum attacks. There is a variety of such protocols. A number of agencies around the planet advice to implement only protocols that are safe against quantum attacks.

In addition to quantum computation, quantum theory suggests ways to encode information that are useful for cryptographic purposes. This topic is now called "quantum cryptography". In quantum cryptography security is not based on the hardness of computing something, but on some physical properties of the information encoded. In 1984, the first quantum cryptography protocol was invented by Charles Bennett, from IBM, and Gilles Brassard, from the University of Montreal[164]. Very importantly, their protocol, which uses a property of

[161] Rivest, R. L., Shamir, A., & Adleman, L., 1978, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 21 (2), pp. 120-126.

[162] Shor, P. W., 1994, *Algorithms for quantum computation: Discrete logarithms and factoring*, In Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on, Ieee, pp. 124-134.

[163] NIST, 2016, *NISTIR 8105 Report on Post-Quantum Cryptography*, US Department of Commerce. Link: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[164] Bennett, C. H., Brassard, G., 1984, *Quantum Cryptography: Public Key Distribution and Coin Tossing,* International Conference on Computers, Systems and Signal Processing, December 10-12 1984, Bangalore.

certain quantum mechanical states called entanglement, can be shown to be provably secure. This means that no matter how much computational power an adversary has, the protocol allows for secure communication. According to the current view of experts, quantum cryptography is the key to secure communication at the global scale. Therefore, quantum computing and quantum cryptography have to be seen as geopolitical game changers.

Another important step in the field of cyber security is related to big data. The term refers to a large volume of data that submerge a company daily, which are analysed to get relevant and useful information. Although the term is relatively new, the concept dates back to 2000s when the industry analyst Doug Laney formulated the definition of big data according to the so-called "three Vs": volume, velocity, variety[165]. All of the three Vs are continuously increasing. For this reason, also variability and complexity should be taken into account. In fact, flows of data can be highly inconsistent and coming from multiple sources.

Multiple are also the sectors that can benefit from them. Public administration, education, banks, health, manufacturing, and retail are only some of them. With the analysis of big data all of them can cut costs, reduce time, prevent failures or defects, develop new programs, identify fraudulent behavior, and take more informed decisions in general. Obviously this is possible only if the data is analysed, and it has to be noted that only a small percentage of the huge mass produced each minute receives this treatment. This has to be seen in the fact that not all the data are secure and protected, as they come from three main sources: public sources available, social media data, and streaming data[166].

The most interesting challenges for the future of cyber security related to big data come from the last two sources. Data from social network interactions, particularly useful for marketing, sales, and customer support, they usually appear in a unstructured or semi-structured form, which furthers the challenge in the ability to classify them. As regards the streaming data, the phenomenon, also known as the internet of things, is the set of data that reach IT systems from a network of connected devices[167]. Companies can collect this type of data and decide

[165] Laney, D., 2001, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, META Group, pp. 1-4.

[166] McAfee, A., Brynjolfsson, E., 2012, *Big data: the management revolution,* Harvard business review, p. 5.

[167] Xia, F., Yang, L. T., Wang, L., Vinel, A., 2012, *Internet of Things*, International Journal of Communication Systems, 25, p. 1101.

what to analyse right away and which ones to save for subsequent analysis.

Internet of things (IoT) is a neologism used for the first time during a presentation at Procter & Gamble by Kevin Ashton in 1999, with the need to name real-world objects connected to the internet[168]. The evolution of the internet has extended itself to real objects, which can now interact with the network and transfer data and information. In this way, an electronic identity can be given to all the electronic devices. However, some of them technologically advanced are called to communicate in an increasingly interconnected form. Not to mention the role of artificial intelligence. Although no machine has yet passed the Turing test to evaluate if a machine can actually think on its own, studies on machine learning and pattern recognition keep making giant steps forward[169]. In particular, defence systems that learn continually seem to be needed if you want to defend structures from constantly changing threats. Traditional antivirus software does not seem to be able to keep up with this constant evolution. Antivirus capable of learning could stem this lack. However, the theme of artificial intelligence is extremely debated, not only for its almost-infinite potential of application, but in particular because of the dilemma between benefits and risks that it involves. For this reason, artificial intelligence is one of the future challenges of cyber security.

The objects connected to the world through IoT technology are now billions, and business environments and the economy are deeply influenced by them. Some examples are thermostats, camcorders, detectors, watches, and sensors. Major research companies agreed in saying that more than 25 billion IoT devices will arrive by 2020, with different degrees of application[170]. The most relevant applications of IoT are in the fields of home automation, robotics, avionics, automotive industry, biomedical industry, wearable sector, and telemetry. This already represents an extraordinary business opportunity for a large set of sectors.

As opportunities grow, threats also grow. The greatest risk is related to the possibility that an external actor hacks and takes control of the connected device. More and more resilient security measures will be needed to enable the use of IoT technologies. Otherwise, the ever-

[168] Ashton, K., 2009, *That 'Internet of Things' Thing*, RFID Journal, p. 1.

[169] Müller, V. C., Bostrom N., 2016, *Future Progress in Artificial Intelligence: A Survey of Expert Opinion*, Fundamental Issues of Artificial Intelligence, pp. 555-572.

[170] Evans, D., 2011, *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, Cisco Internet Business Solutions Group (IBSG), p. 3.

increasing dependence on these technologies would turn out from being a major benefit to a great threat. Privacy and the protection of personal and sensitive data are other important critical points in the internet of things, in particular related to cloud computing.

Cloud computing is the technology that allows the saving of data in a virtual space, called "cloud", where these data can be accessed without the need to be on a physical machine such as a fixed computer or a laptop[171]. The simplest application of cloud computing is cloud storage that has made it possible to extensively extend the potential of electronic devices. Just think of the obvious example in addition to archiving online, email-accessible data from browsers. This service allows you to view all of our email databases from any device without having to download local messages and make them, in fact, inaccessible to other devices. The massive spread of cloud computing, however, ended with the flooding of the already crowded Internet communication lines. The continued demand for data access on the cloud has in fact caused bandwidth to grow exponentially in the space of a few years, putting the phone operators' ability to provide services tailored to the needs of users though.

This *impasse*, could be solved with fog computing (also known as "edge computing"), designed to reduce bandwidth consumption and avoid continuous access to data centres and Content Delivery Network relying instead on a more distributed and parity structure[172]. A kind of peer-to-peer network that makes it easier to access applications and resources stored on the network. Distribution network servers are replaced by thousands of devices and clients that allow faster access to resources without the need to resort to the internet backbone and so saturate the communication band. The ultimate goal, therefore, is to create a parallel network on the web and the internet, enabling users to enjoy the same services without having to go through internet backbones, web servers and all other hardware and software infrastructures needed to the operation of a cloud service.

A practical example is the smart car and the network of the information they need to be able to work best. To date, intelligent and self-contained cars refer to a centralized server from which to obtain real-time traffic information, weather conditions, and other useful data. With

[171] Mell P., Grance, T., 2011, *The NIST Definition of Cloud Computing (Technical report)*, National Institute of Standards and Technology: U.S. Department of Commerce, Special publication, 800-145.

[172] Abdelshkour, M., IoT, March 25 2015, *From Cloud to Fog Computing*, Cisco Blogs. Link: http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing

fogging, however, it will be possible to create an exclusive communication network for smart cars, whereby the connected vehicles can stay in touch and share data without affecting bandwidth usage.

Another system that involves the presence of a distributed database is the blockchain[173]. Not only tied to cryptocurrencies, on Satoshi Nakamoto's peer-to-peer electronic cash system proposed in 2008, blockchain applications can be numerous. In fact, Blockchain should not be seen as a technological solution, but as a new, decentralized approach to the concept of trust and trust. Blockchain is opposed to the traditional authentication and authorization system for transactions and transactions by a central, reliable and certified entity, with a new decentralization-based trust system for all those who take part to the "chain" of the transaction with the role of "blocks" or "nodes". Each block includes the hash (a non-invertible computer algorithmic feature that maps an arbitrary length string to a predefined length string) of the previous block, linking the blocks together. The linked blocks form a chain, with each additional block that reinforces the previous ones.

Blockchain is also a public and shared registry consisting of a number of clients. Blockchain is organized to automatically update on each of the clients participating in the network. Every operation performed must be automatically confirmed by all nodes through encryption software that verifies a private key or seed data package that is used to sign transactions. By guaranteeing the digital identity of those who have authorized it. It is therefore the role of every single human being involved in the process the fundamental actor for ensuring the security of cyberspace. It could not be otherwise.

The human part in cyberspace can be articulated into two levels: the level of individuals and firms (or private one), and the one of nations and international organizations (or public one). Both of them pose serious challenges to cyber security. In particular, at the private level there is an unprecedented need for cyber hygiene, while at the public one the absence of laws of cyberspace still represents one of the biggest issue related to cyber security.

In simple terms, cyber hygiene can be defined as the set of good practices that allow users

[173] Zheng, Z., Xie, S., Dai, H. N., Wang, H., 2016, *Blockchain Challenges and Opportunities: A Survey*, Work Pap.

who are browsing to be able to count on a high level of security[174]. In other words, cyber hygiene concerns individual responsibility that must inspire the ordinary actions of a user on the web and not technical solutions properly connected to cyber security. The user is constantly exposed to threats and attempts to break cyber criminals' security measures against his system. Hygiene is then conceived in this sense as the daily routine, occasional controls, and general behaviors in order to maintain the health of the user. Better safe than sorry, indeed. Although installing a good antivirus on the device used to connect to the network is surely the first step to make, relying entirely on this only would condone the user to almost certainly suffer an attack. This is because, as already seen, the spectrum of the threat grows more and more and the majority of the attacks are of unknown nature. It is therefore necessary to update the operating system, software, applications and everything that can be upgraded. These tips, of elemental nature, are just the basis of cyber hygiene, which provides many others (ranging from the conscious use of search engines to spot fake news, from setting effective passwords to detect activities of social engineering, and so on and so forth) that cannot be addressed here.

On the public level, states and international organizations share an important responsibility. The absence of an international law for regulating cyberspace it is a lack that cannot be neglected or ignored for ever. After acknowledging cyberspace as the fifth domain of warfare, after land, sea, air, and space, it remains to be regulated. This poses a lot of problems. In particular, it is good to note how this last domain includes everyone else. In addition, its borderless nature and boundaries make this task even more difficult. However, cyberspace issues are global as global is the nature of cyber-related threats. Therefore, the creation of a recognized global framework is increasingly needed to promote security, peace, and justice in cyberspace. Non-trivial topics such as respect for human rights on the web, the treatment of computer criminals, and the use of force as a response to a cyber attack, just to name a few, require common legal norms and standards in a global framework for cyberspace. This goal cannot be achieved without a cooperation work by governments and organizations.

[174] Paganini, P., March 6 2015, *Cleaning up the Cyber Mess: Adopting Cyber Hygiene principles*, Security Affairs. Link: http://securityaffairs.co/wordpress/34502/security/cyber-hygiene-principles.html

3.2 The EU-NATO cyber diplomacy

The European Union and the North Atlantic Treaty Alliance are major partners in the area of security and defence since many years[175]. Harbingers of cooperation between the EU and NATO were already visible during the Cold War period in the form of the Western European Union (WEU). In 1992 The Maastricht Treaty laid down the basis for a common European security and defence policy supported by NATO. However, the first tangible example of cooperation did not take place until the crisis in the Western Balkans in May 2001, where the EU and NATO held an official joint summit and adopted a common position on the crisis.
In order to define the parties as strategic partners, on the very next year, the two organizations signed the NATO-EU Declaration on a European Security and Defence Policy. In 2003, the Union and the Alliance signed the so-called "Berlin Plus" agreement which set the milestone principle of giving to the Union the possibility to use NATO forces when necessary. The Berlin Plus has been successfully implemented in Macedonia and Bosnia, where the EU has assumed the lead missions ahead of NATO, still using the Alliance's command structure. The agreement was followed by regular meetings of ministers of foreign affairs and defence, as well as ambassadors of their respective member states. However, cooperation did not gain primary importance before the stipulation of the NATO Strategic Concept in 2010. With the aim of preventing crises by ensuring security and stability in the regions at risk, the Concept has established the absolute need to cooperate in a tight and timely manner with other international organizations, with the EU in the first place.

With the rise of a various set of asymmetric and borderless challenges, to deepen the cooperation between the two organizations has seemed to be essential. In particular, neither organization had an extensive and complete range of tools to effectively tackle these security challenges on its own. The EU-NATO cooperation has to be seen as a work of complementing each other.

The cooperation on cyber security issues between the EU and NATO dates back to 2010[176]. It all started with high level staff-to-staff informal meetings and consultations that still take

[175] Mesterhazy, A., 2017, *NATO-EU Cooperation after Warsaw*, NATO Parliamentary Assembly, Defence and Security committee Report, p. 1.

[176] EEAS, February 10 2016, *EU and NATO increase information sharing on cyber incidents*, Press releases.

place annually. One year later, after the creation of Computer Emergency Response Team of the EU (CERT-EU), the NATO Computer Incident Response Capability (NCIRC) and CERT-EU gave life to an ongoing collaboration which involved other EU agencies and the NATO CCDCOE. In particular, the NATO CCDCOE established a liaison with the European Defence Agency with the extent of exchanging information on common topics. However, it is only in the last two years that the cooperation between the EU and NATO on cyber security has been more concrete.

In February 2016, the EU and NATO signed a Technical Arrangement[177] to facilitate technical info-sharing between CERT-EU and NCIRC, to provide a framework for sharing best practices and to improve advanced procedures of prevention, detection, and response to cyber incidents. The Arrangement was signed at NATO Headquarters in Brussels (Belgium), prior to the annual meeting of NATO's defence ministers, by the Head of CERT-EU Freddy Dezeure and Head of NCIRC Ian West, in the presence of the Deputy Secretary General of the European External Action Service (EEAS) Pedro Serrano, and NATO’s Assistant Secretary General for Emerging Security Challenges, Sorin Ducaru. All of them welcomed the Agreement as an important step in the EU-NATO cooperation on cyber security, hoping for greater collaboration in the field.

As part of the NATO-EU Joint Declaration[178] signed by the President of the European Council Donald Tusk, the President of the European Commission Jean-Claude Juncker and the Secretary General of NATO Jens Stoltenberg at the Warsaw Summit of July 2016, senior officials from both the organizations met again in November 2016[179] with the aim of enhancing the collaboration by setting up future practical steps. The updates took into account the recent policy updates and developments within both organizations, such as the implementation of the EU’s NIS Directive and the adoption of the NATO's Cyber Defence Pledge. Cooperation has been mainly increased in the fields of information sharing, best practices, coordinating efforts to effectively tackle cyber threats and cyber exercises, allowing European representatives to attend the NATO's annual Cyber Coalition exercise in Estonia.

[177] EEAS, February 10 2016, *EU and NATO cyber defence cooperation,* Feature stories.

[178] Council of the European Union, July 8 2016, *Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg*.

[179] EEAS, December 25 2016, *NATO and EU press ahead with cooperation on cyber defence*, Press releases.

Both the Deputy Secretary General of the European External Action Service and NATO's Assistant Secretary General for Emerging Security Challenges shared an interest in cooperating to become more resilient highlighting that the EU-NATO cooperation on cyber security is getting closer and closer.

In the following December, during the Bruxelles meeting of the ministers of foreign affairs of the Alliance, the EU High Representative Federica Mogherini and the NATO Secretary General Jens Stoltenberg presented their proposals for implementing this cooperation. With the goal of building a new era of cooperation, the High Representative and the Secretary General presented a total of 42 proposals[180]. For each of them, a number of possible forms of cooperation have been identified, as expressed in the document approved by the Council of foreign ministers of the EU and by NATO's foreign ministers. After signing, the two leaders agreed that the EU High Representative will regularly report to EU member states, and the NATO Secretary General to NATO allies, on the progress in implementing the set of concrete actions with the intention to enter as early as possible in the implementation phase of the proposals.

The 42 proposals are subdivided into 7 areas defined by the NATO-EU Joint Declaration of July 2016, namely[181]:

1. countering hybrid threats;
2. operational cooperation including maritime issues;
3. cyber security and defence;
4. defence capabilities;
5. defence industry and research;
6. parallel and coordinated exercises;
7. defence and security capacity building.

In order to understand the cooperation program between the EU and NATO, it is useful and relevant to analyse points 1, 3, 5, 6 and 7.

[180] Council of the European Union, December 6 2016, *15283/16 Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*, Brussels, pp. 5-11.

[181] Ibid.

Among the 42 proposals, much talk is dedicated to hybrid threats[182]. Ten out of the forty-two proposals are linked to the fight against hybrid threats. In particular, the EU and NATO have decided to focus on situational awareness, strategic communication, crisis response and bolstering resilience. As for the situational awareness, the two organization have agreed for setting up a European Center for Countering Hybrid Threats. The coordination centre will have to handle concrete measures to strengthen the staff-to-staff sharing of critical information between EU Hybrid Fusion Cell (established within the EU Intelligence and Situation Centre of the European External Action Service) and the newly created NATO Hybrid Analysis Cell, including the exchange of analysis of potential hybrid threats. This will better situational awareness by drawing up a shared situational picture. In fact, the Center will regularly produce joint intelligence assessments on hybrid topics. In April 2017 the EU and NATO welcomed the establishment of the Finnish Centre of Excellence for countering hybrid threats, which has an initial annual budget of around €1.5 million, with Finland providing half of the funding while the rest will be covered by the other members[183].

As for the strategic communication[184], the EU and NATO look forward to intensifying cooperation by undertaking shared trend analysis of misinformation, also including social media targeting the EU and NATO to improve and intensify the quality of positive narrative; enhance the cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS Strategic Communication division through coordinated and joint training/seminars and sharing of platforms. Information on resilience requirements has been already exchanged and the EU and NATO are looking into ways in which they can better support individual nations. The program envisages for the inclusion of partner countries in these activities.

For what concerns the crisis response[185], the two organizations will set up staff-to-staff level regular meetings to enhance preparedness. Furthermore, they seek to synchronize the two

[182] Ibid.

[183] Atlantic Cloucil, April 11 2017, *NATO and EU Members Join Finland's New Center for Countering Hybrid Threats.* Link: http://www.atlanticcouncil.org/blogs/natosource/nato-and-eu-members-join-finland-s-new-center-for-countering-hybrid-threats

[184] Council of the European Union, December 6 2016, *15283/16 Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*, Brussels, pp. 5-11.

[185] Ibid.

organisations' parallel crisis response activities in coherence with NATO's Crisis Response System and the EU's crisis response procedures, including the Integrated Political Crisis Response arrangements (IPCR).

Lastly, the EU and NATO will raise awareness on existing and planned resilience requirements for the benefit of member states/allies in the context of greater coherence between the EU Capability Development Plan (CDP) and the NATO Defence Planning Process (NDPP). Contacts between staffs will be intensified through cross-briefings on resilience requirements and experts upon request will be provided either in the pre-crisis phase, or in response to a crisis to support EU member states and NATO allies.

A particular attention has then been paid to cyber security and defence[186]. After having officially recognized cyberspace as a domain of war, intimate exchanges of integrative concepts for the planning and conduct of cyber defence missions are expected to be implemented immediately. The exchange of concepts on the integration of cyber defence aspects into the planning and conduct of missions and operations will increase the sharing of relevant concepts. The proposals emphasize the need to ensure interoperability between these tools and the classic requirements and standards. In 2017, the standards for cyber training will be harmonized and staff training courses will be open to each other. In this respect, particular importance has been given to the NATO Centre of Excellence, which will have to define specific areas that require innovation by cooperation, paying particular attention to dual-use aspects for which direct involvement of the industry is explicitly required.

The fifth point focuses on defence industry and research[187]. In particular, to further develop dialogue on industrial aspects and to enhance cooperation at staff level on defence-related research and development in common areas of interest, the EU and NATO have established a mechanism for interaction to further develop a dialogue on industrial aspects. The main focus of the interaction is directed at specific areas of common interest such as small and medium enterprises.

According to the proposals, the cooperation will then be reinforced, for the first time, through

[186] Ibid.
[187] Ibid.

coordinated exercises (parallel and coordinated exercises, PACE) and pilot projects to be implemented in 2017 and 2018[188]. Among them, NATO will lead Crisis Management Exercise 2017 (CMX 17), while the EU will coordinate the Multi-Layer Crisis Management Exercise 2018 (ML 18). Both will include hybrid elements and will test the implementation of the common proposals. The scenario predicts that a large number of member states/allies are subjected to large-scale cyber aggressions of different nature and intensely directed against critical infrastructures. Confronted with fake social media campaigns, the two supranational entities involved, namely the EU and NATO, will not have enough evidence to identify a guilty certain. Intelligence, however, points out that the mandate is an "almost democratic" country, to which are added terrorists and no-global groups[189]. The EU and NATO will then organise staff-to-staff exercises like the already existing Cyber Coalition and Cyber Europe to test the key modalities already defined in the respective Playbooks/Operational Protocols. A principle of reciprocity will be respected in leading the planning and conduct of these exercises. Lessons learned and recommendations will be then shared to the maximum extent as possible, with invitations to each other's staff to attend appropriate events of exercises, presentations, and workshops.

The last macro area of the proposals is dedicated to defence and security capacity-building[190]. In this regard, NATO and the EU support the fostering of building partners' capacity and resilience, in particular in the Eastern and Southern neighbourhoods and in the Western Balkans. In more depth, they encourage cooperation and exchange of expertise through respective centres of excellence and other relevant training activities and programmes. In Bosnia and Herzegovina, Tunisia and Moldova key areas of interaction that goes from cyber to strategic communications, from safety to ammunition storage have been already identified in three pilot projects.

In conclusion, a particular attention is dedicated to the strengthening of political dialogue between the two organizations. The EU and NATO commit themselves to continue regular

[188] Ibid.

[189] Difesa & Sicurezza, July 30 2017, *UE testa le difese dai cyber attacchi di un paese "quasi democratico"*. Link: http://www.difesaesicurezza.com/difesa-e-sicurezza/ue-testa-le-difese-dai-cyber-attacchi-di-un-paese-quasi-democratico/

[190] Council of the European Union, December 6 2016, *15283/16 Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*, Brussels, pp. 5-11.

formal and informal PSC-NAC meetings, strengthen cross briefings to respective Committees and Councils (including on operations), and further pursue in a balanced manner the practice of mutual invitations to relevant ministerial meetings.

The most recent meetings between the Union and the Alliance on cyber security took both place in Brussels during the meeting of the EU's defence ministers and during the meeting of the NATO's leader, in May 2017[191]. During the two events, the ministers and leaders discussed on how to strengthen defence and security in Europe as well as how to improve the cooperation with the member states of the Alliance. Given that NATO has experienced around 500 cyber incidents on average in every month of 2017 (with a 60% increase compared to 2016), NATO Secretary General once again highlighted the importance of cooperating to effectively tackle cyber threats and provided the positive example of warning between the EU and NATO about the recent WannaCry ransomware global attack. In fact, NATO has granted the European hub for cyber security access to NATO’s malware information sharing platform in order to ease and quick the sharing of information on cyber attacks.

In mid-September, a certification system for cybersecurity standards will be introduced for technology devices, the ENISA agency will also be legally modernized, and the updated European strategy will be published in relation to cyberspace threats. Additionally, the European Union and NATO will work together to standardize behaviors and responses in case of accidents. The Alliance's NCIRC and CERT-EU are assuming to create common standards with a severity scheme. This will determine how the two bodies will respond to security breaches[192]. In any cases, the Council of the EU has already stated that the EU-NATO cooperation on cyber security will regularly to take place on the basis of key guiding principles of openness, transparency, inclusiveness, and reciprocity, in full respect of the decision-making autonomy and procedures of both organisations and without prejudice to the specific character of the security and defence policy of any member state[193].

[191] Council of the European Union, May 18 2017, *Foreign Affairs Council, 18/05/2017*, Press releases.

[192] Council of the European Union, June 14 2017, *Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016*, Brussels, p. 4.

[193] Council of the European Union, June 19 2017, *Council conclusions on Progress report on the implementation of the common set of proposals endorsed by EU and NATO Ministers on 6 December 2016*, Press releases.

3.2.1 Assessments and thoughts on the cooperation

When considering cooperation at international or regional levels, it is impossible not to look at some internal factors. In particular, the fundamental problem of groups of states is always the same one: are we talking about a European Union of states or about a European Union as an organization? Once again, even in the cyberspace, it is useless to deny the presence of many different wills and aims within the Union. For example, the excellent NIS Directive, which represents a very important step in improving the general level of security among the states, in a couple of points declares that everything that concerns national security still remains an absolute prerogative of the states[194]. This is easily understandable obviously, though it creates a lot of problems for the cooperation process. On the contrary, at NATO level there seems to be more cohesion and collaboration in dealing with similar and shared issues. But what does this depend on? This is mainly due to the fact that the risk perception is greater at the Alliance level. Since the Alliance is born and conceived as a political treaty and a military security organization, NATO is taken far more into account when dealing with defence issues. Of course, cyber security goes beyond mere defence.

An eloquent example of this imbalance is represented by the program on cyber security of the Estonian Presidency of the Council of the European Union for the period July 1 - December 31, 2017. Estonia is generally recognized in the cyber security community as a virtuous example in the field of cyber. In particular, after the powerful cyber attack in 2007, the country has been equipped with a broad and robust cyber infrastructure defence system. The country has thus reached a very high digitization rate and most of its services today rely on cyberspace. For this reason, the country hosts many centres of excellence, including the NATO CCDCOE in Tallinn and another one in the National Defence College dedicated to the training and exercise of the allies in Tartu. As for the EU, Estonia has set its presidency to the Council of the European Union on four points related to cyber security: an open and innovative European economy, a safe and secure Europe, a digital Europe and the free movement of data, and an inclusive and sustainable Europe[195]. Despite the excellent plan

[194] Official Journal of the European Union, July 19 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, art. 1.6 and art. 7.3.

[195] Cf. Official website of the Estonian Presidency to the Council of the European Union. Link: https://www.eu2017.ee/news/insights/cybersecurity-and-estonian-presidency

related to digital market and cyber crime, unfortunately, among these points, there is no mention of the role of cyber diplomacy at the European level.

That is why today ever greater cooperation between the European Union and the North Atlantic Treaty Organization on cyber security is not only desirable but absolutely indispensable. Despite the fact that the cooperation in this field is very young, as already seen, the material and the topics discussed during the meetings are already large in number. In particular, the ideas of facilitating info-sharing and performing joint exercises are very important, as well as the establishment of the joint set of proposals necessary to implement this cooperation. Indeed without a common strategy, there can be no common work.

However, these appear to be timid steps. At this point, it is worth wondering whether it will be time to make its natural course or whether something specific will need to happen in order to implement this cooperation. In this regard, it would be desirable the creation of a linkage between the two organizations that, at the very least, could combine the different procedures of the two organizations in order to let them “speak the same language” on cyber security. Today, at the operational level, there is nothing of this kind. Despite the creation of the New Center for Countering Hybrid Threats in Finland it is a positive and important first step, it has to be noted that only nine countries have signed the Memorandum of Understanding that gave life to the Center. In particular, even if the EU and NATO have declared that they will actively participate in the activities, they have not signed it. The presence of a real linkage that represents a shared point of collection today seems to be far from becoming a reality, at least in the short run. Cooperation procedures will proceed very slowly if members do not realize the need to cooperate in the field before a serious diplomatic crisis breaks out or a viral attack involves many Euro-Atlantic actors.

On the contrary, it appears that both counterparts of the cooperations are moving fast in trying to defend their cyber infrastructure. At the moment, the EU and NATO can be seen as two parallel lines that run fast, go toward a common direction, but never touch. Or, at least, only shyly for now. This definitely creates the risk of overlapping skills and procedures. In order to prevent this from happening, it is crucial that one organization is aware of what the other one is doing. In this way, the two organizations could both contribute to cooperation and establish a joint path that does not imply that efforts are directed on both sides towards the same objects, but instead, it provides for different capabilities between the two organizations on the basis of their matured expertises. To use a well-known concept in the sector of international relations, NATO, for its features described above, could represent the role of the stick (or rather the actor enforcing hard power), while the EU could play the role of the carrot (or rather the one enforcing soft power).

In any case, this is certainly the right time to lead an inclusive EU-NATO cyber security cooperation. As mentioned above, this is due to the fact that the two organizations share the same ideals and values. Perhaps the times seem to be still a little too premature to be able to dialogue with countries or regional organizations that do not share these perspectives. Therefore, the work of cyber diplomacy between the EU and NATO should focus on two fronts: on the internal front, the goal has to be the reach of an efficient degree of cooperation that does not create overlapping but instead uses the best resources of the two organizations; and, in the external front, if it is not possible to make concrete steps with actors whose way of conceiving cyberspace is far from that one of the EU and NATO, the two should try to involve as much as possible into the dialogue those actors that, in a way or another, share similar thoughts. The important thing is that the process does not encounter any stumbling blocks but, on the contrary, keeps on going.

In particular, the EU and NATO should commit themselves to the realization of a legal framework recognizing the applicability of international law to the cyberspace. This is a priority. Now that the battlefield has been generally recognized, as well as actors and weapons, definitions and, above all, the binding acceptance of the rules of the game are lacking. Based on what happened at the UN GGE level[196], these rules should not be dictated by experts and technician but rather by decision-makers who reside at the top of political levels. In other words, it seems to be necessary to start from a more realistic perspective in which states have to resume their prerogative (which is the responsibility to protect themselves and their citizens) and to create shared rules for stability, security and peace in the cyberspace. Only then, a more pragmatic discourse that takes into account the intrinsic properties of cyberspace, where there are no borders and there is no possibility of limiting the side effects of the attack, can be undertaken. That is why the only approach to effectively

[196] See Section *4.4.1 An interview with Eng. Pierluigi Paganini and Dr. Luigi Martino*

launch a cyber diplomatic cooperation with those actors that do not share the same visions on cyberspace, is to raise awareness of the fact that side effects may involve not only the attacked and the attacker but, due to the interconnected and interdependent nature of the cyberspace, the whole international community.

4. THE ITALIAN CASE

4.1 Italy between EU and NATO

Today, it is impossible to consider the Italian diplomacy out of a European and Atlantic framework. The European and Atlantic vocation of the country represents an indisputable and indispensable priority of its foreign policy. Italy is in fact a member and founder of both the European Union and the North Atlantic Treaty Organization[197].

In 1957, six countries with a far-sighted vision signed an important treaty which established the European Economic Community (EEC) and the European Atomic Energy Community (Euratom) in the Orazi and Curiazi Hall of the Palace of the Conservators in Rome. Two years earlier, Italy, France, Germany, Belgium, the Netherlands, and Luxembourg met in Messina, Sicily, to lay the foundations of the Treaty of Rome, and in 1956 in the Venetian lagoon to approve the Spaak Report. In another Italian island, in 1941, the confined Altiero Spinelli and Ernesto Rossi stated the principles of the Ventotene Manifesto for European federalism. That vision of European integration has been consolidated and strengthened over the coming decades, with a constant expansion process both horizontally and vertically, and important milestones have been achieved. Among them, the most important one has been to secure peace for more than 60 years on the European continent, previously harassed by two world conflicts.

In this process, Italy has played a leading role. Many the conferences that lead to fundamental decisions and measures took place on the peninsula. Many the politicians who have held leading positions in European summits. The sole presidency of the Council of Ministers of the European Union was presided over by Italy for eleven times, of which the latter in the second half of 2014. This has to be summed to a constant military engagement, especially in the Balkans, the Mediterranean Sea and North Africa. Given its strategic assets, Italy's national interest focuses on ensuring that these three regions become a platform for promoting

[197] Cf. Official page of the Italian Ministry of Foreign Affairs on the role of Italy in the EU. Link: http://www.esteri.it/mae/it/politica_europea/italia_in_ue
Cf. Official page of the Italian Ministry of Foreign Affairs on the role of Italy in NATO. Link: http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

prosperity, security and stability, and not a factor of crisis and destabilization. This broadly coincides with the strategic interest of both the EU and NATO.

Despite being defeated during the Second World War, Italy is a founding member of the North Atlantic Treaty Organization and, since 1949, it participates in the construction and development process of the Alliance. In particular, because of its geographical position, the Alliance needed Italy as Italy needed the Alliance. This statement is still valid. With regard to the ongoing debate on the contribution of the allied countries[198] to the Organization, it has to be said that Italy spends on defence only 1.11% of its gross domestic product. The figure is well below the 2% Alliance benchmark. Only seven NATO countries spend less. If we look at statistics, a country like Greece seems to be a champion of the Alliance thanks to its annual defence spending of 2.4% of GDP. However, although Greece is committed to saving migrants in its shores, it does not participate in EU or NATO military missions. Looking closely at the picture and not just at the mere numbers, it emerges that Italy's contribution to security in the Balkans, the Mediterranean Sea, and the MENA region is far from being absent[199]. Especially in the fields of police training and maritime rescue.

The Italian presence of some 600 soldiers is stable in Kosovo since the outbreak of the conflict. This ensures regional stability and, given the explosiveness of the area, wards off any military escalation. The same can be said about Lebanon, where about 1,100 soldiers are present. An equal number of soldiers is located in Afghanistan. Another protagonist role played by Italy is the one in the Mediterranean Sea. The country is not only part of the fisheries control and security of piracy but has saved some 95,000 lives in the first half of 2017 only. The migratory phenomenon goes on from 2013. Overall, last year, about 6,200 Italian troops contributed to the role played by NATO in the Middle East, North Africa, the Mediterranean, the Balkans, the Horn of Africa and Afghanistan, located in a total of 18 countries. This year around 140 Italians have been deployed to Latvia in the framework of the Enhanced Forward Presence initiative of NATO. For these reasons, the Italian troops have been recently defined as the “Europe's military maestros”[200].

[198] Cf. NATO, June 29 2017, *Defence Expenditure of NATO Countries (2010-2017)*, Press release.

[199] Cf. Official page of the Italian Ministry of Defence on the troops employment in international operations. Link: https://www.difesa.it/OperazioniMilitari/Documents/Mappa_Operazioni_Militari_IT_ultima.pdf

[200] Braw, E., August 23 2017, *Europe's Military Maestros: Italy*, Politico. Link: http://www.politico.eu/article/europes-military-maestros-italy-troops-mediterranean-migrants-libya-refugees/

The Italian contribution, through a steady diplomatic push, has not been missed also during the 2016 Warsaw Summit[201]. With the NATO-EU Joint Declaration, broad consensus was reached on meaningful cooperation proposals. Due to its balance between Europeanism and Atlanticism, Italian politics is in a significant position to implement the 42 proposals put forward in the Joint Declaration. In particular, among the seven areas of cooperation, Italy has a central role to play in maritime cooperation with regard to migratory flows and the capacity building defence one of the countries of the south and east borders. The simultaneous presence of EUNAVFOR MED Sophia and Sea Guardian missions make the maritime component return to play a major role after other priorities had been put to the fore. The creation of a junction point on the Italian peninsula, often referred to as an "aircraft carrier in the Mediterranean"[202], could be a concrete step to address and manage efficiently and effectively the various initiatives to promote the stabilization and security of the Southern flank. Among these activities, the defence capacity building plays an important role. Italy has already been engaged in training both the Libyan navy and coast guard as well as both Iraqi government forces and the Kurdish Peshmerga since 2016[203]. Considering this commitment made by Italy both within the EU and NATO, the country is definitely in a favourable position to push for the concretization of cooperation initiatives.

Italy supports the need for closer cooperation between the two organizations in their efforts to promote regional security and stability through crisis management and peace-keeping operations, with a view to complementarity between the two organizations[204]. It is time for the EU and NATO to become places of consultation and coordination, where reductions on the one hand and investment increases on the other one are coordinated and decided in a sense of smart defence, intelligent defence, not a weaker defence. In a context of economic and financial constraints such as the present one, the division of labor and tasks becomes even more important.

[201] Bitonto, F., Marrone, A., Sartori, P., 2016, *Le sfide della Nato e il ruolo dell'Italia: Trump, Brexit, difesa collettiva e stabilizzazione del vicinato*, Istituto Affari Internazionali, Documenti IAI 16, p. 29.

[202] Pozzo, F., October 5 2016, *La portaerei italiana che Mussolini affondò*, La Stampa. Link: http://www.lastampa.it/2016/10/05/societa/mare/la-portaerei-italiana-che-mussolini-affond-tw0ieYL24evBbgRxeFKPxN/pagina.html

[203] Bitonto, F., Marrone, A., Sartori, P., 2016, *Le sfide della Nato e il ruolo dell'Italia: Trump, Brexit, difesa collettiva e stabilizzazione del vicinato*, Istituto Affari Internazionali, Documenti IAI 16, pp. 30-31.

[204] Cf. Statement on the EU-NATO cooperation on the official website of the Italian Ministry of Foreign Affairs. Link: http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

4.1.1 An interview with Amb. Luca Giansanti

Ambassador Luca Giansanti[205] is director general for political and security affairs at the Italian Ministry of Foreign Affairs since August 2014. He has an extensive experience in the field of international security and European affairs. Among his numerous missions, Amb. Giansanti has been ambassador to the political and security committee of the EU, permanent representative to the Western European Union (WEU), and ambassador of Italy to the Islamic Republic of Iran.

Candidate: how does Italy fit into the two different approaches of the EU and NATO?

Amb. Giansanti: by their very nature, the approaches of the two organizations are basically different. The EU has the advantage of being able to easily bring together the civil and military worlds, the soft and hard powers, while NATO is objectively a bit stricter in this. Italy has always been a strong supporter of the staff-to-staff work that underlies cooperation between the two organizations. This kind of clever approach is indispensable in order to overcome some limitations. If the cooperation relationship was between institutions and institutions, it would have found several blocks, including the issue of the two different memberships. In particular, the fact that at least two EU member states have no access to any NATO document because they have no security agreement. On the contrary, having favoured a staff-to-staff approach has allowed the encounter to be more pragmatic. This has to be credited also to the Greek pragmatism, on the one hand, and to the Turkish pragmatism, on the other, just to make an example, when facing a common challenge. Institutional issues would undoubtedly block many decisive steps of this cooperation.

Candidate: as previously demonstrated and reaffirmed now, internal divisions within Europe on foreign policy are slowing down the process of cooperation. How to overcome them?

Amb. Giansanti: unfortunately, there is no simple and immediate solution to this problem. Both the solution and the problem reside in the European capital cities. Brussels (as the capital city of both the EU and NATO) is not the problem, but it suffers from it. We have

[205] Cf. Short biography of Amb. Luca Giansanti on the website of the Italian Ministry of Foreign Affairs. Link: http://www.esteri.it/mae/it/ministero/struttura/dgaffaripoliticisicurezza/dirgen_dgaps.html

entered a historic phase in which cases such as the election of Donald Trump in the US and such as Brexit, paradoxically seem to serve as coagulants for greater political will. In addition, we have to always take into account the role of electoral phases, of which the French one just passed and the German one is coming in the short-term. We can affirm that it is necessary to align European capitals to overcome these obstacles and often surf the wave of political conditions that paradoxically arise from non-positive events, such as Brexit, so that something can finally be put into motion. Over the years, Italy has presented several innovative formulas to try to raise the issue of foreign, security and defense policy. In particular, I think of the "Schengen of defence" referred to in the joint article of the Minister Paolo Gentiloni Silveri and Minister Roberta Pinotti, a year ago. In spite of skepticism, the work is currently in progress under the European treaties. If this does not work, the hypothesis of working outside these treaties, in order to reintegrate them later, remains alive. Obviously, while all this is possible on security and defence policies, it is impossible on foreign policy because changes must necessarily born inside the institutions. Every European capital has its own problems and its own positions.

Candidate: what are the major challenges that the EU and NATO will face together in the near future?

Amb. Giansanti: beyond the external and geopolitical threats, certainly the development of military capabilities, being planned for both at this historic stage, is a challenge for the two organizations. In particular, this work seems necessary because, if we were to reach 2% of defence budget and military spending as agreed at NATO, waste would abound. Willing to reach a numerical value at all costs, even with the awareness of the current duplications within the two organizations, it would have a negative impact. The EU and NATO will need to work hard on this. Furthermore, more and more efforts will be needed to improve coordination between the two organizations. Probably, this is the main challenge that the two organizations will face in the short term. In particular, we must take into account that NATO has experience in the sector, while the EU begins to approach it seriously only since recent years. There is a need for the two to coordinate so that the measures taken are not just a *façade* but they really fill the capacitance gap. Sectors such as off-area cooperation or problems related to the Mediterranean area are much less complicated within this cooperation, because in these the primacy of one or other organization is very clear and functional. Once again, if the EU maintains its most comprehensive civil-military approach, it can play a significant role without duplicating NATO and achieving results that will benefit both.

4.2 The current status of cyber threat in Italy

Cyber threats and menaces are definitely becoming a matter of national security. As already seen, the cyber domain is an ideal place for a vast range of illicit operations that goes from the theft of confidential information to the perpetrating of material damage to infrastructures that are managed and controlled by computing systems. To safeguard the cyberspace it is therefore necessary for governments to adopt effective strategies that can tackle these risks.

However, only a few countries all over the world have already set national cyber security strategies[206]. At the general level, it can be affirmed that all those countries that have already set national cyber security strategies can be divided into three major models of development[207]. According to the first model, the top-down, the cyber strategy is entirely managed by the public sector; on the very other side, the bottom-up model considers cyber security to be managed by the private sector; and finally the hybrid model sets a collaboration between public and private sectors (even if the former sector still prevails over the latter). The third model is adopted by Italy and the large majority of the developed countries. In more depth, it fosters the public and private partnership to reach common standard levels of security also through the share of strategic information and a tight collaboration with the managers of the critical infrastructures. This collaboration ensures resilience into the cyber domain, that is a space in which is extremely difficult to detect and sanction any illegal acts. Therefore, an efficient set of prevention measures and a focus on risk mitigation are the two pillars that should hold on the whole cyber security structure of a country.

Before dealing with the Italian cyber security strategic framework, it is necessary and worth

[206] Among the EU member states, only Greece have not set a national cyber security strategy yet. Cf. ENISA on national cyber security strategies. Link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[207] Marchetti, R., Mulas, R., 2017, *Cyber Security: Hacker, terroristi, spie e le nuove minacce del web*, LUISS University Press, Rome, pp. 148-149.

to contextualize the country's global position and the current status of its cyber threat. According to the International Telecommunications Union of the United Nations, Italy ranks 31° in the Global Cybersecurity Index[208]. Being one of the most influential rankings, the Index evaluates national commitments on cyber security by dealing with five major factors: the legal measures, the technical measures, the organizational measures, the capacity building, and the cooperation with external actors. Although Italy is a founding member of both to the EU and NATO, it ranks in a rather low position among the most developed countries (even though good at the global level). The reasons have to be found mostly in the lack of national standards, certifications and benchmark for cyber security, low investments and a rather new cyber architecture. Moreover, the shortage of advanced competencies seems to slow the digital development of the economy and society.

The current status of the cyber threat in Italy is not reassuring. As highlighted by both the Clusit 2017 Report on ICT Security in Italy[209] and the Document on National Security attached to the 2016 Annual Report to the Parliament[210] of the *Dipartimento delle Informazioni per la Sicurezza* (DIS, Information Security Department), the cyber menace in Italy follows a steady trend of growth (in line with the international context) for complexity, extension and persistence.

Groups of hacktivists still represent the majority of hostile actors (52% of the total), even though the impact of their attacks is inversely proportional to their large presence. On the contrary, groups of cyber-espionage are less numerous (19%) but more dangerous to the national security[211].

[208] International Telecommunications Union, 2017, *Global Cybersecurity Index (GCI) 2017*, p. 60.

[209] Clusit, 2017, *Rapporto Clusit 2017 sulla Sicurezza ICT in Italia,* Astrea, Milano.

[210] Presidenza del Consiglio dei Ministri, 2017, *Relazione sulla Politica dell'Informazione per la Sicurezza 2016,* Documento di Sicurezza Nazionale.

[211] Ibid., p. 20.

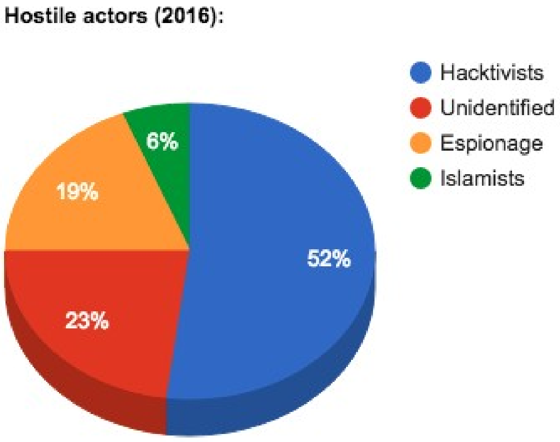

Figure 8. Hostile actors (2016) (DIS, 2017)

Even though the diversification of cyber targets is constantly raising, most of the attacks are still pointed towards the public sector (71%) and only 27% of them is oriented to the private one[212].

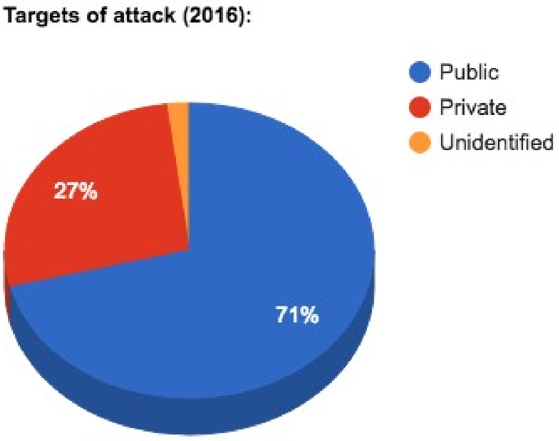

Figure 9. Targets of attack (2016) (DIS, 2017)

The public level of awareness about the cyber risks is not always adequate and the strengthening of vulnerability of institutional websites with security measures is not always foreseen. According to Kaspersky Lab, Italy is one of the less concerned countries in the world about online dangers as 92% of Italians believe they cannot become victims of cyber attacks and 46% of them do not install antivirus on electronic devices, even though 22% of Italians have been victims of cyber criminals[213].

[212] Ibid., p. 21.

[213] Cf. Kaspersky Cybersecurity Index Italy 2016. Link: https://index.kaspersky.com/country/italy-h22016-all-all

In the private sphere, banking is the first target of cyber attacks (17%), followed by press agencies and industrial associations (both at 11%). Defence, energy, aerospace and the pharmaceutical sector (each of them at 5%) are no more the bullseyes of cyber malicious acts[214].

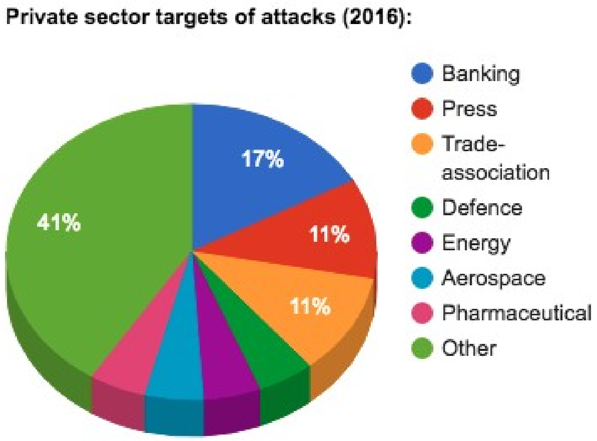

Figure 10. Private sector targets (2016) (DIS, 2017)

It can be expected a stable trend on terrorism and hacktivism, with a significant growth in attacks towards highly technological sectors, like pharmaceutical, manufacturing and those that extensively use always more interconnected technologies that deal with the internet of things (IoT). SQL injections (28%), denial of service (19%), web-defacement (13%) and malware (11%) represent the most common types of cyber attack. A qualitative growth of advanced persistent threats has to be expected as well as the increase of malicious malware that are always more customized to hit the central administrations of the public sector[215].

[214] Presidenza del Consiglio dei Ministri, 2017, *Relazione sulla Politica dell'Informazione per la Sicurezza 2016,* Documento di Sicurezza Nazionale, p. 23.

[215] Ibid., p. 24.

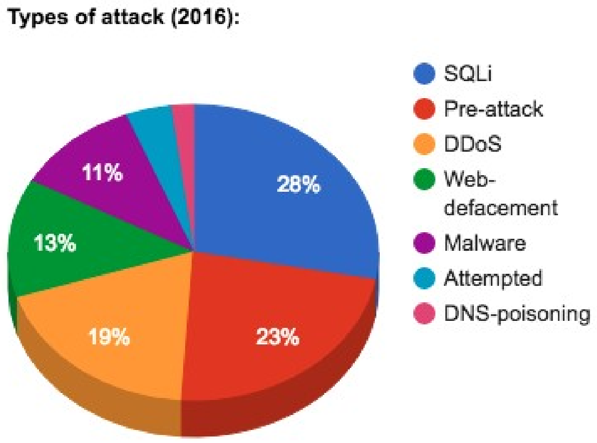

Figure 11. Types of attack (2016) (DIS, 2017)

4.3 The Italian cyber security framework

The Italian national cyber security framework has developed at the political, operational and strategical levels according to the recent European directives[216]. The process started in 2007 with the adoption of the Law 124/2007 which reformed the whole Italian intelligence apparatus and raised concern for the risks that could arise into the cyberspace.

In 2012, the *Agenzia per l'Italia Digitale* (AgID, Digital Italy Agency) was created in order to pursue the highest level of technological innovation in the organization and development of public administration at the service of citizens and businesses. The Agency has the task of ensuring the achievement of the objectives of the *Agenda Digitale Italiana* (Italian Digital Agenda) in line with the European Digital Agenda, through the digitization of services and the development of the digital infrastructures necessary to ensure the country's economic competitiveness.

With the 2015 Directive of the Presidency of the Republic, AgID was tasked of promoting the diffusion of information and communication technologies and developing a coordinated system of cyber security for public administration. While the very next year the *Team per la Trasformazione Digitale* (Digital Transformation Team) was set up under the Presidency of

[216] Cf. Sistema di Informazione per la Sicurezza della Repubblica, *Normativa di riferimento*. Link:: http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento.html

the Council of Ministers with the aim of digitizing the country's operating system to build simpler and more effective services for public administration, citizens, and businesses.

The Italian institutional architecture dedicated to the protection of cyber security was formally established with the adoption of the "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*" ("Directive on Cyber Security and National Computer Security") adopted by Decree of the President of the Council of Ministers (DPCM) Monti of January 24, 2013. The text indicates the tasks entrusted to each office and the mechanisms and procedures to be followed to reduce vulnerabilities, prevent risks and respond promptly to attacks as well as restore system functionality in the event of a crisis. The Italian cyber defence is thus divided into three macro areas of intervention: the political-strategic level that defines the organizational set-up; the operational level which outlines the various organizers for the protection of cyberspace on the national territory; and finally the tactical level that manages the situation of cyber crisis.

This cybersecurity strategic doctrine is based on two main documents adopted within the DPCM 2013: the "*Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*" ("National Strategic Framework for Cyberspace Security") and the "*Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*" ("National Plan for Cyber Security and Computer Security"). The former contains strategic guidelines, while the latter is focused on the operational level.

The Strategic Framework is concerned with defining the major cyber threats and the major vulnerabilities exploited for both technical and organizational attacks. In addition, the Framework identifies the possible tools and procedures needed to create a resilient defensive system, articulating them into six strategic priorities[217]:
1. improvement, according to an integrated approach, of the technological, operational and analysis capabilities of the concerned institutional actors;
2. strengthening the ability to defend critical national infrastructures and actors of strategic importance for the country system;
3. encouraging cooperation between national institutions and enterprises;

[217] Presidenza del Consiglio dei Ministri, December 2013, *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*.

4. promotion and diffusion of the cyber security culture;
5. strengthening the ability to counter the spread of illegal online activities and content;
6. strengthening international cooperation.

The National Plan identifies the operational guidelines, objectives to be achieved, and the lines of action to be structured in order to concretise the Framework by converting the six strategic guidelines into eleven operational guidelines to support national cyber security[218]:
1. enhancement of intelligence, police and civilian and military capabilities;
2. enhancement of the organization and methods of coordination and interaction at national level between public and private entities;
3. promotion and dissemination of the culture of computer security with education and training;
4. international cooperation and exercises;
5. operation of national structures, incident prevention, response and remediation;
6. legislation and compliance with international obligations;
7. compliance with standards and safety protocols;
8. support for industrial and technological development;
9. strategic and operational communication;
10. resources;
11. implementing a system.

The last milestone of the development of the Italian national cyber security framework is the approval of the new "*Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*" ("National Plan for Cyber Defence and Computer Security") by the Comitato Interministeriale per la Sicurezza della Repubblica (CISR, Interministerial Committee for the Security of the Republic) and the relative adoption of the recent DPCM Gentiloni Silveri on February 17, 2017. The decree is composed of 13 articles which partially replace the DPCM Monti of 2013 and, like the former decree, defines the cyber-related acts and new institutional architecture for the protection of national computer security, by specifying the breakdown of tasks and mechanisms to prevent and mitigate the threat, but also to respond to it and restore the regular activities related to the use of cyberspace. The update of the text is due to the

[218] Presidenza del Consiglio dei Ministri, December 2013, *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*.

alignment of the Italian framework with the new European standards contained in the aforementioned NIS Directive, which has to be implemented before May 9, 2018.

The new action plan of the national cyber security strategy is based on the following points[219]:
1. review of the *Nucleo per la Sicurezza Cibernetica* (Cyber Security Unit);
2. contraction of the chain of command for the management of cyber crime;
3. reducing the complexity of national architecture by suppressing/merging organs;
4. progressive unification of CERTs;
5. establishment of an ICT national assessment and certification centre;
6. foundation or venture capital fund;
7. establishment of a national research and development centre in cyber security;
8. establishment of a national encryption centre.

The political-strategic level of the Italian institutional architecture on cyber security is administered by the President of the Council of Ministers and the CISR[220]. The CISR is a consultative body for policies on information security. The Committee also establishes the budget of the already-mentioned *Dipartimento delle Informazioni per la Sicurezza*, of the *Agenzia Informazioni e Sicurezza Esterna* (AISE, External Information and Security Agency) and of the *Agenzia Informazioni e Sicurezza Interna* (AISI, Internal Information and Security Agency), and the information requirements necessary for the various ministries to carry out their activities. The Committee is chaired by the Prime Minister and the Director General of DIS is its secretary. Other members of the CISR are the *Autorità delegata* (Delegated Authority for Security), the Minister of Foreign Affairs, the Minister of the Interior, the Minister of Defence, the Minister of Justice, the Minister of Economy and Finance and the Minister for Economic Development.

If a cyber crisis occurs, the Prime Minister has to call the CISR for an emergency meeting and give directives to the intelligence department and agencies according to the above-mentioned Strategic Framework and National Plan for cyber security[221]. As already mentioned above, the

[219] Presidenza del Consiglio dei Ministri, March 2017, *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*.

[220] Gazzetta Ufficiale, May 31 2017, *Decreto del Presidente del Consiglio dei Ministri 31 Marzo 2017*, 125, art. 3 and art. 4.

[221] Ibid.

two documents are characterized by a comprehensive approach that allows the implementation of joint measures between public and private sectors in order to effectively prevent, contain, react and counteract a cyber attack.

The operational support consists of the interaction of three bodies: the so-called "CISR *Tecnico"* (Technical CIRS) as a collegiate coordination body; the *Nucleo per la Sicurezza Cibernetica* (Cyber Security Unit); and the *Comitato Scientifico* (Scientific Committee). The CISR *Tecnico* is the body responsible for strategic intelligence analysis[222]. The Technical Committee is chaired by the General Director of DIS and is composed of the executives and managers of the administrations that are members of the CISR and, periodically, of the Prime Minister's Military Adviser. Its task is to manage the coordination of research activities on information with the aim of strengthening the national cyber security by supporting CISR.
The *Nucleo per la Sicurezza Cibernetica* represents an innovation in the cyber security framework and works tied to the Prime Minister as a link between the various components of the institutional architecture involved in cyber security[223]. Initially, it was chaired by the Prime Minister's Military Adviser but the new decree collocated it within the DIS. It is now directed by one of the Vice General Directors of DIS, appointed by the Director General. It is composed by the Prime Minister's Military Adviser and one representative per each of the following institutions: AISE, AISI, Ministry of Foreign Affairs, Ministry of Interiors, Ministry of Justice, Ministry for Economic Development, Ministry for Economy and Finance, Department for Civil Protection, and AgID. In addition to the role of mediator between the parties, the *Nucleo per la Sicurezza Cibernetica* promotes the programming of institutional response to crisis situations by keeping the Computer Emergency Response Team (CERT) active in alerting and responding to cyber attacks 24 hours a day, 7 days a week. Furthermore, the Unit promotes, together with the Digital Italy Agency and the Ministry for Economic Development interministerial and international drills to test the response capacity of the nation to cyber crises. *Dulcis in fundo*, the *Nucleo per la Sicurezza Cibernetica* works as the reference point for relations with international organizations (such as the EU and NATO) and other states.

With the new decree on cyber security, the intelligence agencies have acquired a pivotal role

[222] Ibid., art. 5.
[223] Ibid., art. 8 and art. 9.

in participating to reach and maintain the desired cyber security level[224]. In particular, the General Director of DIS has the apical role of coordinating them in the informative research to guarantee cyber safety and national computer information security and can make partnerships in accordance with its role[225].

The last of the three operating bodies of support is the *Comitato Scientifico*, which has the task of supporting both the CISR *Tecnico* and the *Nucleo*. The Committee has been set up within the intelligence training school and is comprised of cyber security experts from public administrations, academia, and private entities.

Tactically speaking, the bodies involved in responding to emergency situations are the *Tavolo Interministeriale di Crisi Cibernetica* (Interministerial Cyber Crisis Table), the CERT *Nazionale* (National CERT), the CERT PA (Public Administration CERT) and the specific CERTs relative to the affected sector[226]. The task of the Table is to ensure that the reaction and stabilization activities of the various public administrations are carried out in a coordinated manner. On the other hand, National CERT deals with technical aspects of computer and telematics responses, supporting citizens and businesses through actions to raise awareness, prevent and coordinate response to large-scale cyber events. In particular, National CERT works on a PPP model through an info-sharing platform launched in 2014 with key telecommunications and energy companies in order to allow for immediate sharing of issues, experiences, and lessons learned. The fundamental info-sharing activity has also started at the institutional and international level[227]. In particular, agreements were made between National CERT and CERT PA, CERT Defence and the *Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche* (CNAIPIC, National Anti-Crime Center for Critical Infrastructure Protection). At the international level, National CERT is the reference point for the prevention, monitoring, and coordination of foreign CERTs.

It is evident that the reasons that inspired the new decree are strongly geared to boosting the efficiency and effectiveness of the national strategic protection system. The new cyber architecture appears to be characterized by a shorter chain of command, a more simple and

[224] Ibid., art. 7.
[225] Ibid., art. 6.
[226] Ibid., art. 10 and art. 11.
[227] Ibid., art. 12.

slim contour structure of support, and vertices with more operational capabilities. In addition, the roles of the various institutional actors seems to be now better defined and delimited, thus reducing the areas of overlap that exist between them. However, only time will be able to judge whether the operational structures called from this reorganization to greater engagement will actually be equipped with all the tools that it needs to best deliver the required activities for safeguarding the cyber security of Italian structures.

4.4 A successful case of cyber diplomacy: the Lucca Declaration

The Lucca Declaration, adopted by the Ise-Shima Cyber Group (ISCG) during the 43rd G7 Summit can be easily considered to be an example of successful multilateral cyber diplomacy. The Cyber Group was created in May 2016 during the Ise-Shima (Japan) Summit specifically to discuss cyber issues. On October 14 2016, during the 42nd G7 Summit, the Ise-Shima Cyber Group reunited for the first time[228]. Under the chairmanship of the Japan's Ambassador in charge of Cyber Policy and Deputy Director-General of Foreign Policy Bureau Koichi Mizushima, the delegations of Japan, Italy, France, Germany, Canada, the United States of America, and the United Kingdom discussed on how to promote international law, norms, capacity building and confidence building measures, in order to increase security and stability in the cyberspace. The ISCG then committed itself to keep working together on the topic the very next year under the Italian presidency at the 43rd G7 Summit.

In April 2017, the ISCG reunited in Lucca (Italy) during the G7 Foreign Affairs Summit. After an intense debate on cyber issues, in an attempt to establish an international code of conduct, the Group finally generated the so-called “Lucca Declaration”, formally the “G7 Declaration on Responsible States Behavior in Cyberspace”. Although the statement is not binding, the Lucca Declaration is a positive output of the activity of cyber diplomacy. In more depth, it is an important acknowledgment of the states' commitment to address the major threats in the cyberspace that today undermine the political, economic and technological sectors of the states. The Foreign Ministers of the G7 countries acknowledged the urgent need for international cooperation to promote security and stability in cyberspace and therefore,

[228] Ministry of Foreign Affairs of Japan, October 14 2016, *First Meeting of G7 “Ise-Shima Cyber Group (ISCG)”*, Press release.

having recognized "the enormous benefits for economic growth and prosperity that […] derive from cyberspace"[229] the 7 countries are "committed to an accessible, open, interoperable, reliable and secure cyberspace"[230].

The document underlines the concern of "the risk of escalation and retaliation in cyberspace"[231], in particular for those activities that "could have a destabilizing effect on international peace and security"[232], including massive denial-of-service attacks, critical infrastructure damage, or other malicious cyber activities that compromise the use and operation of a critical infrastructure.

After having recognize the basic concept of respecting human rights also online, the delegations then express their concern for the use of internet in favour of terrorism and criminal purposes in general. Therefore, they encourage to apply international law and the relative Charter of the United Nations on ICTs. Consequently, international law would provide for a global framework useful for any peaceful settlement of disputes that can arise after an illicit behavior or acts in the cyberspace. Furthermore, under certain circumstances and means, the country that is victim of these could respond with appropriate measures. In other words, in some cases that are subject to international law (Article 51 of the UN Charter) states may exercise their natural right to individual or collective defence.

The Declaration then supports the development and implementation of Confidence Building Measures (CBMs) on cyber security and fosters the engaging into work within the G7 and any other relevant international and multi-stakeholder offices that share the common vision of promoting strategic frameworks for conflict prevention, cooperation, and stability in the cyberspace.

In the last part, the "G7 Declaration on Responsible States Behavior in Cyberspace" contains a set of non-binding norms, already articulated in the 2015 United Nations Group of Governmental Experts (UN GGE) Report and in the Communiqué Final of the G20 leaders' summit in 2015. These points aim at promoting a strategic framework for conflict prevention,

[229] G7, April 11 2017, *G7 Declaration on Responsible States Behavior in Cyberspace*, Lucca, p. 1.

[230] Ibid.

[231] Ibid.

[232] Ibid.

cooperation, and stability in the cyberspace, still recognizing the applicability of existing international law[233]:

1. maintain consistency with the purposes of the UN and apply them to the use of ICTs;

2. in case of incident arising in the cyberspace, states should investigate and proceed only after having considered all the relevant information related to the ICT environment;

3. states should be aware of the use of ICTs in their territory;

4. cooperation is absolutely encouraged for sharing of information and mutually assistance;

5. human rights (including privacy and freedom of expression) have to be respected in ensuring the secure use of ICTs, under the Human Rights Council resolutions 20/8 and 26/13 as well as the General Assembly resolutions 68/167 and 69/166;

6. in providing services to the public, states should not conduct or support any ICT activities contrary to international law that intentionally damages critical infrastructure;

7. states should take appropriate measure to assure protection of their critical infrastructures from ICT threats under General Assembly resolution 58/199;

8. state should provide their help to any other state whose critical infrastructures are subjected to malicious acts and prevent malicious activities arising from their territory;

9. state should safeguard the integrity of supply chains for ICTs production;

10. states should report ICT vulnerabilities and share information on remedies to eliminate potential threats to any other states;

11. state should not act against the CERTs of other states;

12. state should not look for competitive advantages by supporting the theft of business-related information like intellectual property and trade secrets.

4.4.1 An interview with Eng. Pierluigi Paganini and Dr. Luigi Martino

Engineer Pierluigi Paganini[234] is one of the members of the 2017 G7 Cyber Group. Furthermore, he is chief technology officer at CSE Cybsec Enterprise S.p.A., member of the European Union Agency for Network and Information Security (ENISA) Treat Landscape Stakeholder Group, editor-in-chief at "Cyber Defense Magazine", professor and director of

[233] G7, April 11 2017, *G7 Declaration on Responsible States Behavior in Cyberspace*, Lucca, pp. 3-5.

[234] Cf. Short biography of Eng. Pierluigi Paganini on his blog Security Affairs. Link: http://securityaffairs.co/wordpress/author/paganinip

the Master in Cyber Security at Link Campus University, founder of the blog “Security Affairs”, and editor for some major publications in the field such as “Infosec Institute”, "Cybersecurity Startupitalia". He is the author of the books “The Deep Dark Web” and “Digital Virtual Currency and Bitcoin”.

Doctor Luigi Martino[235] is one of the members of the 2017 G7 Cyber Group. Furthermore, he is PhD research assistant at the Sant'Anna School of Advanced Studies with a thesis project on cyber security and critical infrastructure protection, assistant teacher of cyber security and international relations at the University of Florence where he is also coordinator of the Center for Cyber Security and International Relations Studies, consultant in cyber security of BV-Tech Group S.p.A., and project manager for the OSCE research project “Enhancing the Implementation of OSCE CBMs to Reduce the Risks of Conflict Stemming From the Use of ICTs”. He is the co-editor of the book “Intelligence e Interesse Nazionale”.

Candidate: the Lucca Declaration is definitely an eloquent and positive example of multilateral and international cyber diplomacy. It would not have been easy to produce a document that has been accepted, even if in a non-binding form, by all the members of the G7. In that regard, what role did the Ise-Shima Group of the 2016 G7 had and since when did you work on the project before reaching the final agreement?

Eng. Paganini: as members of the Italian group we worked on the project for about a year before the Lucca summit. The activity of cyber diplomacy requires rather lengthy preparatory times because of the need to consider what will be the plan of the other nations participating in the cooperation. The Ise-Shima Group of 2016 did not play an operative role, but fundamental under certain aspects. In particular, the Group has had the merit of recognizing the need to regulate cyberspace internationally. Although it has not played a purely operational role, it has represented an ideological starting point that is absolutely necessary to give momentum to the project.

Candidate: how many elements made up the Italian team that participated in the 2017 G7 Cyber Group?

[235] Cf. Short biography of Dr. Luigi Martino on the website of the University of Florence. Link: http://www.cssii.unifi.it/vp-90-responsabile-del-center.html

Dr. Martino: our group is made up of four members, two diplomats, and two experts. The team is headed by the Deputy Director General/Central Director for Security, Disarmament and Non-Proliferation of the Italian Ministry of Foreign Affairs Min. Plen. Gianfranco Incarnato, assisted by his vicar Cons. Leg. Marco Lapadura, who had already participated in all the works of the Ise-Shima Group in 2016. The policy part was handled by me, while Eng. Paganini has cared for the technical aspects of the matter. Despite the small number - we must bear in mind that some groups of other nations such as Germany, for example, were made up of dozens of people - having adopted a multidisciplinary approach has allowed us to do a good job anyway.

Candidate: a great job, indeed. What is the impact of the Lucca Declaration at an international level?

Eng. Paganini: the impact of the Declaration is considerable. In particular, the important element is that, for the first time in a multilateral table such as the one of the G7, the official and written need to establish rules of behavior between states in the cyberspace has been recognized. Obviously, we must bear in mind that much of the work had been done in by the UN GGE, which provided a good basis for writing norms of behavior.

Dr. Martino: the impact of the Declaration has to be estimated, however, considering that within the G7 there is a general presence of like-minded states. The sharing of the same ideals, values, and conception of cyberspace, has facilitated the unanimous cooperation and acceptance of these norms of behavior.

Candidate: the absence of relevant nations such as Russia and China in this dialogue cannot be neglected. How could other nations be involved?

Dr. Martino: surely by moving the discourse to other *fora*. With regard to Russia, the best place is the Organization for Security and Co-operation in Europe and, with regard to China, the G20. In any case, it is good to keep in mind that all these international and regional activities linked to initiatives of cyber diplomacy were legitimated by the UN GGE. The key problem is that the UN GGE is currently in stand-by because it has not reached the consensus for publishing its 2017 report. This is a setback in the world cyber diplomacy. Problems arose on the application of international law to cyber domain and, above all, humanitarian law and the concept of self defence. Despite the fact that the UN GGE was not a governmental expression, but an expression of experts and technicians, there was a formal opposition between Cuba (supported by China and Russia) and the United States of America. In the aftermath of the opposition, the US issued a statement in which they consider the UN GGE in a deadlock and intend to resort to meetings made up of like-minded states (such as the G7) or conduct bilateral activities. Now that purely theoretical issues have been addressed and it is necessary to move to a practical work, the process has run aground. When it comes to multilateral diplomacy, it has to be always kept in mind that these initiatives are based on two fundamental principles: voluntary basis and unanimity. In this way, it is enough that a single state disagrees to break-up everything.

Eng. Paganini: the inclusion of the Asian counterparts in the cooperation is absolutely essential. The dialogue was carried out in the G7 with the ambition to go beyond what was set for larger *fora*, such as the G20 or the OSCE. If we think that we are working on the cyberspace, which by definition has no bounds, such a discourse makes sense only when an increasing number of actors share the need to create norms of behavior between states and to contribute with their own experience in the growth of a certain regulatory framework in an international context.

Candidate: the creation of an international framework that is legally recognized and respected is certainly the most important requirement as well as the current challenge in the cyber security sector. What were the points that constituted more disagreements during the last G7?

Eng. Paganini: from a formal point of view, cooperation has been widely accepted by everyone. We all have recognized the need to create this very much debated framework. Obviously, when talking about regulatory framework, we must distinguish two areas: information warfare and cyber crime. The first concerns the role of actors (including states) that are confronted with other actors who use the IT tool in an information warfare context. In this context, during the G7 there were misalignments and discrepancies because, at that table, there were nations that have extremely heterogeneous backgrounds. In particular, nations such as the US and the UK have invested in this field for decades, compared to countries such as France, Japan, and Italy, where cyber is seriously taken into consideration only since around 5 years. In this respect, the adoption of a restrictive regulatory framework could be perceived by the most advanced nations as an attempt of clearing this acquired gap. Although everyone agrees on the need to create such framework, it is worth to remember that almost all the cyber operations are now run by governments, especially in the field of espionage rather than sabotage. Governments engage in the search for new methods of defence and attack, techniques that allow them to remain hidden during the attack and to make the attribution complex even when the offensive is detected. Long-term collaboration has been discussed between the intelligence agencies of Canada, Australia, New Zealand, UK and USA, known as the Five Eyes. At the G7, three of the major players were present: Canada, USA, and the UK. In addition to them, Germany, whose intelligence has always supported NSA activities in European territory. Over the past few months we have known, thanks to Snowden's revelations that German intelligence has offered technology and logistics support for massive surveillance activities to NSA. On the very other hand, a timid Japan, that owns the merit of recognizing the need for a regulatory framework during the 2016 Ise-Shima, but postponed to the Italian presidency the whole of decision-related to the drafting of the Declaration. Its approach is closely linked to an extremely collaborative culture and a strong spirit of community and responsibility. France, in recognizing the need for a Declaration, was probably the closest participant to the direction plotted by Italy. As for cyber crime, which by its nature is born and lives in the cyberspace, it continues to represent a serious problem for the economy of each country. The situation is aggravated by the development of Crime-as-a-Service models that are attracting capital and resources from ordinary crime. The number of actors offering criminals organized their services increases, and the only way to deal with these actors is to reach a shared and international agreement with rules of conduct to be established when any community actor is in some way hit by a criminal phenomenon that occurs in cyberspace. Today, the performing of detection activities has to confront with a series of very different regulatory frameworks. The sole phase of investigations into a criminal group that is, for example, made of Russians, based in Vietnam, that compromises servers in Europe and exfiltrates data in Japan, is extremely complicated because it is necessary to involve all the various states concerned by requesting the permissions necessary.

Given the quick nature of cyber phenomena, either the investigation starts immediately (with still the risk that the evidence may have been manipulated), or it will be impossible to trace the event. From the point of view of cyber crime, the need to operate in a shared legal context was widely recognized, with the triggering of series of mechanisms after an event. In this respect, Lucca's G7 was much more aligned.

Candidate: what are the next steps to be taken to ensure that the good result obtained with the adoption of the Lucca Declaration is not frustrated?

Dr. Martino: it is certainly important not to break the talk but move it to other *fora*. Obviously, all the participants involved in the issue has to actively commit themselves to the meeting. As for Italy, the country has been unanimously elected to chair the OSCE Presidency in 2018. The theme of cyber security is one of the priorities of the Italian project. The country has already launched a research project on cyber security under the title "Enhancing the Implementation of OSCE CBMs to Reduce the Risks of Conflict Stemming From the Use of ICTs" within the University of Florence. We have to hope that the timing will be sufficiently mature to carry out effective dialogue on cyber security cooperation.

4.4.2 A final remark with Min. Plen. Gianfranco Incarnato

Minister Plenipotentiary Gianfranco Incarnato[236] is deputy director general/central director for security, disarmament and non-proliferation at the directorate-general for political and security affairs of the Italian Ministry of Foreign Affairs. Furthermore, he is coordinator for cyber security issues and representative of the Ministry of Foreign Affairs at 2017 G7 Cyber Group. From October 2014 he is also sherpa and coordinator for the participation in the 2016 Summit on Nuclear Safety.

Candidate: taking into account what has been analysed and said so far, in the end, what is the merit of the Lucca Declaration in the cyber dialogue and what will its future be?

[236] Cf. Short biography of Min. Plen. Ginfranco Incarnato on the website of Aracne Editrice. Link: http://www.aracneeditrice.it/aracneweb/index.php/autori.html?auth-id=379166

Min. Plen. Incarnato: considering the turbid waters in which the last G7 was assembled, the Lucca Declaration seems to be a miracle. The many dissensions that have arisen in the discussion have been overcome because the responsibility for any failure to recognize a good conduct to be adopted in cyberspace would be fallen against the states. However, almost six months after the signing, multilateral cyber diplomacy seems to have not made significant progress. Now we need to unlock the situation before falling into the UN GGE stall. Italy is currently in a favourable position because it did not want to be part of it, even though it recognizes the importance and relevance of the project, nor does it follow the behavior of other nations that acted in inertia. This allows the country freedom of movement, which does not mean ignoring its responsibilities but, on the contrary, becoming a free actor outside of games of power. We must have the patience to prepare the ground because we run the risk of being very venerable. We need to set up a team and have our shoulders covered. Once we get that, we can go straight ahead without being afraid to be alone. In any case, we will not be alone because more than one state shares our vision and the others, once we get tight, will voice their reservations but eventually accept the negotiation. We have to look further, be creative but not too much. One goal that we set before Lucca was to build a reasonable negotiating base but with some element of ambitions that they could draw to carry on the project. Going back into the ranks did not cost us anything, but by falling back into the ranks we welcomed partners' perplexities that were spendable and not what we heard in the meetings we had. It is time to bring something different that, of course, might not work but it would still be an attempt. In particular, we would like to start a real negotiation. In the preparatory phase of the G7, we have also begun a discourse on the type of convention to which the negotiation could be inspired. The Biological Weapons Convention signed in 1972, approved after an extended effort from the international community, seems to be a good basis for reference. As with the cyber threat, the biological threat is difficult to identify. Despite a long and troubled negotiation period, an agreement was reached for the 1972 Convention, I do not see why there could not be a similar agreement to apply to the cyberspace.

4.5 What role for the Italian cyber diplomacy? Advice and recommendations

At this point, it is worthy to make some considerations about the role of Italy in the field of cyber diplomacy also by taking into account the new cyber structure of the country. Based on what has been analysed in the previous paragraphs and discussed with Eng. Pierluigi Paganini, Dr. Luigi Martino and Min. Plen. Gianfranco Incarnato, it can be stated that Italy is only at the starting point of its cyber adventure. Recent efforts in the sector within the administration do nothing but place the country at a basic level to be competitive from an international point of view. Surely, the funding of €150 million announced in 2015[237] is an important signal, but the amount is a minimum in order to be able to try to assure a decent level of protection. In any case, the direction taken is definitely the good one. In line with the European NIS Directive, the Gentiloni Decree has above all the merit of putting Italy at a level of maturity similar to that of other countries, at least as regards the institutional level. This has introduced novelties that were absolutely necessary. In particular, the strengthening of the strategic role of DIS in the field of cyber security; the centrality of the Cybernetic Security Center on the prevention, preparation and response of the Italian government in the event of cyber crime; and the establishment of a national assessment and certification centre for verifying the security conditions and the absence of vulnerabilities on products, equipment and IT systems.

Appointing the deputy director of DIS with proxy to cyber security could be an important step to make this system even better. Whoever will cover this role, it is important that this figure will not just be a coordinator of activities but rather a decision-maker. In other words, it should be proactive and not bureaucratic. If this role becomes a mere function of public administration, it will obviously be covered by all the diseases that the public administration has in general. This must necessarily be part of a larger design, both nationally and internationally.

With regard to the cyber structure of the country, it is pivotal to set goals that become policies to be implemented as soon as possible. The key element to ensure this is that national cyber structures, like CISR ministries, intelligence services, AgID and CERTs, are aligned. The agencies and ministries involved must necessarily establish, if it is not already present, dialogues that are continuous, streamlined and effective in order to pursue a common line within a long-term strategy. To do this, an increasing investment in economic terms and in

[237] Redazione, October 31 2016, *Italia: 150 milioni di euro previsti per la sicurezza cibernetica*, Startupitalia. Link: http://cybersecurity.startupitalia.eu/53212-20161031-italia-150-milioni-cybersecurity

human resources it is a priority.

In particular, it is time to ensure that the money already allocated is spent with due knowledge and as soon as possible. As for human capital, it is now more than ever necessary a talent-building policy. The most advanced cyber nations have been doing this for several years. Fostering programs in universities and research centres can only have a positive impact on the industry. Often there is a tendency to consider this sector as a closed and elitist one, but it is good to change this perspective by creating a culture of cyber security that involves the common citizens at 360°. A solid and comprehensive information campaign appears absolutely necessary. Let us remember that, in the vast majority of times, it is still the human factor to represent the weak link in the cyber chain. If we want to protect the safeguard of citizens, we must necessarily instruct them on what they have to do and do not.

Investments have to be put in a nice long-term design, otherwise it will be difficult to understand how to spend without wasting them. Launching a public-private partnership with mixed investment could create a virtuous circle, as it is happening much in Israel, the UK or Estonia, which remains the virtuous European example. The theme is very much debated, which is obviously good, but one of the Italian problems is that it does not have a valued industry for cyber security although there is an increasing number of companies operating in the sector. There is a growing array of start-ups, small and medium sized enterprises that are interested in the cyber industry. It is profitable then to let these innovators to work along with those security companies that are already solid and stable, so that cooperation with the public space can be rich from both innovation and stability. It is dramatic to see an overwhelming majority of foreign companies carrying on activities funded by Italy in order to develop technology. At that point, the country will always be an importer of technology. This means that it will never be competitive at the industry level. This has not to be perceived as autocracy, but as a national security discourse. Otherwise, there is the risk of being at the mercy of security vendors which are competing within each other, and that does nothing but slow down the process. Italy (as every other country) definitely need to look abroad, but in another perspective.

This perspective is represented by cyber diplomacy. As seen, this activity is gaining importance and is steadily growing. A testimony to the relevance of this kind of diplomacy as a tool of foreign policy is demonstrated by the existence of more than twenty cyber offices in foreign affairs ministries all around the world. Among them, the most famous one is definitely the one created about six years ago by then secretary of state Hillary Clinton and led by Chris Painter, generally recognized as the most famous cyber diplomat[238]. Among his many merits[239], it has to be acknowledged the achievement of a historic agreement with China that has finally made it clear that no state should exploit the media to steal intellectual property and trade secrets from another state to make an advantage to its own commercial sector. More importantly, Painter's activity has established and trained a body of cyber-officers at US missions around the world to perform cyber diplomacy as a new tool of foreign policy.

Unfortunately, at the moment, there are too few Italian cyber security experts who are recognized internationally. Just as the number of diplomats sensitive to this issue. In particular, the IT structure of the Italian Ministry of Foreign Affairs itself has already been targeted by cyber attacks in 2016[240]. In addition, from 2013 to 2016, the Permanent Representation of Italy to the European Union in Brussels has been subjected to stealing of sensitive data through its computer network[241]. On the basis of the Italian institutional strategy reorganized by the Gentiloni Decree, all international cooperation activities must be carried out by the Italian Ministry of Foreign Affairs. The strategy should focus on both short and long terms given that the problem will not run out in a few years, but instead, the cyber era has just begun. The main problem for ensuring this strategy seems to be the lack of a structure and actors to carry out this strategy. The creation of a cyber unit within the Farnesina, with a well-defined system of tasks and roles, which is constantly updated on the basis of new threats and needs, not only represents a good idea because of its sectorial activity but especially because of the importance that the matter covers. This would ensure a constant cyber dialogue which is not just relegated to international *fora*, and would serve as a support

[238] Sulmeyer, M., Roncone., G., August 23 2017, *The Making of a Cyber Diplomat*, The Cipher Brief. Link: https://www.thecipherbrief.com/column/cyber-advisor/back-basics-u-s-cyber-diplomacy

[239] Painter, C., August 1 2017, *The Case for Diplomacy in Cyberspace*, Medium Digital Diplomacy. Link: https://medium.com/digital-diplomacy/the-case-for-diplomacy-in-cyberspace-8ca1ca8c97b3

[240] Kirchgaessner, S., February 10 2017, *Russia suspected over hacking attack on Italian foreign ministry,* The Guardian. Link: https://www.theguardian.com/world/2017/feb/10/russia-suspected-over-hacking-attack-on-italian-foreign-ministry

[241] Bulfon, F., August 14 2017, *Dalle carte della Nato ai report su Siria e Libia: i segreti della Farnesina rubati da russi e cinesi*, La Repubblica. Link: http://www.repubblica.it/tecnologia/sicurezza/2017/08/14/news/dalle_carte_della_nato_ai_report_su_siria_e_libia_i_segreti_della_farnesina_rubati_da_russi_e_cinesi-173004383/

for citizens and Italian enterprises abroad who operate in the cyberspace according to the paradigms of the nation they are currently in. A group of experts and technicians, whether they are workers in the public or private, should then support the work of the unit. This structure should take place in a stable nature and not on the basis of the Italian presidency at the G7 or the OSCE, just to make two recent examples. All this has to be included under the aegis of a coordinator that will allow the dialogue of the unit with all the other actors and agencies that are part of the cyber national structure, the Presidency of the Council of Ministers *in primis*. In addition, it goes without saying, courses and updates for employees on the dangers of cyber space and the good practices to be adopted in the regular conduct of the activities within the Ministry of Foreign Affairs and its international missions, are at the very basis of this growing process.

The cyber theme within the Ministry of Foreign Affairs cannot be missed. It is definitely true that the cyber security topic concerns the sectors of defence, economy, development and much more, but the confrontation with other international actors, such as nations, should be discussed at the level of Ministry of Foreign Affairs. It always has to keep in mind that the cyberspace has an unbounded and global nature. After having recognized this as a domain of warfare, diplomacy cannot ignore its context and its developments.

Diplomacy has and must continue to play a key role in building cooperation and coalitions to respond to shared threats to global commons. Human rights, acts of violence, global governance and many more aspects, fill the cyberspace without an internationally accepted answer. This space, because of its nature, requires an inclusive and coordinated approach. A balance between interests and values. At the moment, the future of the Italian cyber diplomacy appears to be uncertain. The only certainty is that it will be necessary to speed up by taking ambitious decisions and implementing effective cyber policies as soon as possible.

CONCLUSION

When in 1988, Robert Morris, son of a National Security Agency officer, launched a computer worm from Cornell University that infected between 4,000 and 6,000 machines, about 5% of all computers connected to ARPANET network in those years, made for the first time computer safety a worldwide priority[242]. No one would have expected the first cyber attack in history to be conducted from the inside. The Advanced Research Projects Agency Network (ARPANET) is nothing more than the internet ancestor. The network was born in a project promoted in 1969 by the Defence Advanced Research Projects Agency (DARPA), a US Defence Department agency, in order to optimize the speed of information exchange between universities and research laboratories[243]. However, for its distributed network architecture, this tool proved to be very useful for the military during the Cold War because it avoided any kind of blockade in internal communications which could arise after a Soviet attack on telephone lines. The invention of a data transmission suite from one node to another through Transmission Control Protocol/Internet Protocol (TCP/IP) completed the project. Its use has grown to a massive extent. Today, there are 3.3 billion of regular internet users worldwide, of which 29 million are only in Italy[244]. The original ARPANET project, which ignored any defence and protection system, has now evolved and become the largest network of digital interactions.

It is important not to confuse the internet with the cyberspace. While the internet refers to the concept of a network of networks, cyberspace refers to virtual reality as a whole, where the internet is only a part of it. In 2010, the Pentagon formally recognized cyberspace as a new domain of warfare, the fifth after earth, sea, air, and space. The same thing happened in 2016 within the Atlantic Alliance when NATO defence ministers expressed their support for this position. Although in a different way, in 2011 China, Russia, Tajikistan and Uzbekistan (within the Shanghai Cooperation Organization) also acknowledged the presence of common challenges in the sphere of information security. States therefore claim a prominent role in enforcing security within this domain, which, like the other four, is now considered to be a

[242] Orman, H., 2003, *The Morris worm: A fifteen-year perspective*. IEEE Security & Privacy, 99(5), p. 4.

[243] Gillies, J., Cailliau, R., 2000, *How the Web was Born: The Story of the World Wide Web*, Oxford University Press, Oxford, p. 25.

[244] World Bank, *Internet users (per 100 people)*. Link: http://data.worldbank.org/indicator/IT.NET.USER.P2

global common. A global common is a place beyond the jurisdiction of individual countries, a resource that no one can claim as its own and to which security access should therefore be guaranteed. However, these guarantees are subject to a heated debate. Different geopolitical interests mixed with different ways of conceiving the cyberspace and its policies make it impossible at this time to reach an international agreement for the creation of a shared and respected framework. In particular, cyber diplomacy faces the toughest role of elaborating rules for the narrow circle of sovereign states operating in the cyberspace, which however share that space with a myriad of non-sovereign and hard to identify actors. While states must necessarily represent the actors who have the last word on internal security, on the other hand, they would have to accept themselves to be bound by rules of behavior in a promiscuous space. Unfortunately, today, the time seems to be still a little too premature to be able to create this project efficiently.

These problems lead the efforts of cyber diplomacy to focus on bilateral or multilateral *fora* of like-minded states. But it is not all gold that glitters. With regard to the former, chapter 1 has proved with the examples of agreements between USA and China and between Russia and China, three of the most important actors in the cyber scene, that outputs were different. Only two months after the signing of the Sino-Russian agreement, the number of Chinese speakers who have targeted Russia has increased by 300% from December 2015 to February 2016. In contrast, Chinese hacking activities against American companies seem to have declined since the September 2015 agreement between President Barack Obama and President Xi Jinping. This is because the Sino-Russian tie on cyber security appears to be more dependent on the relationship with the US than on the partnership itself between the two Asian countries. Both the governments of Beijing and Moscow are concerned about the American advocacy for internet freedom as a priority of its foreign policy. Fearing the ongoing dominance of the United States over the internet, China and Russia just combine their efforts to seek more geopolitical influence through the reshaping of the cyberspace.

As for multilateral *fora*, discussed in chapters 2, 3 and 4, cyber diplomacy measures have been used within the United Nations Group of Governmental Experts, the Organization for Security and Cooperation in Europe and the Group of 7. Since 2004, the UN GGE has come together in five different compositions and has adopted increasingly detailed and proactive reports on the need to develop a code of conduct to apply in cyberspace. Unfortunately, last June, the fifth UN GGE recognized the impossibility of reaching a consensus because of an opposition between Cuba (supported by Russia and China) and the United States. On the line of this work, the OSCE has set itself the objective of developing Confidence Building Measures (CBMs) to be approved at different times in order to improve transparency, stability, and cooperation in this area. For now, work continues in a serene way because the adopted sets are rather theoretical. In the wake of this work, the G7 has also played an important role in cyber diplomacy. In particular, during the last G7 Summit, a Declaration on Responsible States Behavior in Cyberspace was approved. Although this is not binding, the Declaration is an important step in accepting state responsibility. It is important to remember that the Lucca Declaration has been accepted among like-minded countries, members of one organization. That is why, at the moment, the best place to be able to pursue cyber security cooperation programs seems to be that of bilateral cooperation between international organizations that share the same values and interests. The program launched in February 2016 with the signing of a Technical Arrangement between the European Union and the North Atlantic Treaty Organization is currently one of the most important of these.

In addition to trying to raise awareness among the average citizen about the importance of the general topic of cyber security, the objective set out in the introduction of this thesis was to answer two questions that would help somehow all those who, in one way or another, make part of the system that produces cyber security policies within the EU, NATO and on behalf of the Italian Republic. Because of the recent nature of this agreement and its absolutely importance, the first of these two questions concerns this cooperation program. How can EU-NATO cooperation on cyber security be effective and not counterproductive?

It has been tried to provide for an answer to this difficult question by first analysing in detail the different cyber strategies recently adopted by the two organizations, an indispensable operation to understand the reasons for the cooperation. In particular, in chapter 2, the objectives, legal frameworks, agencies, measures and funds that make up these strategies have been investigated. The analysis has shown how the different nature of the two organizations deeply models these strategies and the perception member states and allies have of them. In particular, because of the fragmentation within the EU foreign policy (or rather, policies), confirmed by the declaration contained in the fundamental NIS Directive, where all that concerns national security remains the absolute prerogative of the states, that the European member countries fail to be united on the cyber front. On the contrary, there seems to be much more cooperation and cohesion in dealing with the issue within NATO. This is mainly due to the fact that risk perception is greater within an alliance born and conceived as a military pact.

Before focusing on the issue of cooperation between the two organizations, the focus of the analysis has briefly shifted to the global landscape of the cyber threat. From the analysis of threat geography trends, recorded cases, motivations behind the attacks, and the different types used, it emerged that the spectrum of cyberspace threats is expected to grow in the future. This is due to its simplicity and low cost with which attackers successfully run cyber attacks, while defending from such attacks requires high costs and complex defence structures. It was then shown how the cyber security industry will face several challenges. Among these, the advent of quantum computing, which will have a revolutionary impact on cyber security, especially with regard to cryptography. Absolute importance will also have to be given to the close relationship that binds big data and the internet of things; the trade off between the benefits and risks associated with cloud computing and how these can be secured with fog computing and blockchain. The paragraph was concluded by pointing out once again the absolute importance of the human factor in cyber security. To ensure that risks do not overcome the benefits of interaction between people and ICTs, it is vital to develop a culture of security through indoctrination of cyber hygiene and the creation of an international framework to both punish those who attack and to protect those who are victims of these attacks, in a universal and binding manner. The main players in cyberspace will necessarily need to consider these new themes and the new potential threats that these bring with them along with the benefits.

As repeatedly highlighted in the text, a new type of threat requires a new kind of cooperation. In the second part of chapter 3, the matter of the EU-NATO cooperation on cyber security has been analysed. From a careful analysis of the steps taken so far, it has emerged that, due to the intrinsic characteristics of the two organizations, the very nature of cyberspace and the numerous risks involved, greater cooperation between the EU and NATO not only is desirable but absolutely indispensable. Although cooperation has only begun recently, many points have already been discussed. However, these appear to be only first and timid steps. In particular, without the creation of a physical linking point that allows a constant dialogue between the two organizations, there is a risk that the efforts of both will not match the needs and end up creating unnecessary and counterproductive overlaps. On the contrary, it is desirable that the two exploit their very different characteristics and potentials, such as efficient EU soft power capability, and equally strong NATO hard power, so as to contribute by filling gaps. Without such a meeting point, the process is likely to proceed too slowly. In addition, both the EU and NATO should work together to create a framework for cyberspace that is recognized and implemented by all members and allies with the aim of extending this involvement to third countries.

Finally, the focus of chapter 4 was entirely devoted to the Italian situation. First, the role of the country between the EU and NATO has been analysed. The theme has been enriched by the interview with the Director General for Political and Security Affairs of the Italian Ministry of Foreign Affairs, Ambassador Luca Giansanti. The country has always played an important role in the two organizations. This is not only because Italy is a founding member of both, but above all because of its strategic position and its active, timely and steady engagement in the major areas of crisis of the Union and of the Alliance. Defined as the “Europe's military maestros”, Italian troops drive operations that ensure stability and support in the precarious territory of Kosovo, Lebanon, and Libya. Moreover, due to its physical structure of “aircraft carrier in the Mediterranean Sea”, Italy contributes almost autonomously to the rescue of thousands and thousands of migrants crossing the waves of the Mediterranean Sea in an attempt to reach the European coast. For these reasons, its balance between Europeanism and Atlanticism, the country can certainly be a driving force for the development of the EU-NATO cooperation program in at least two of the seven cooperation areas agreed during the NATO-EU Joint Declaration of July 2016, namely maritime cooperation and security capacity building. As for the contrast to hybrid threats and the cyber security sector, unfortunately, Italy is not currently able to play the very same special role.

In the second paragraph of chapter 4, the Italian status of the cyber threat has been analysed by taking into account the trends and the main factors. It has emerged that the Italian case does not differ much from the global situation, reinforcing the notion that the fifth domain does not make national distinctions. For its intrinsic nature, a cyber attack can in fact be carried out by anyone to anyone, anywhere from any place. In a sense, the cyber domain nullifies space and time, making it extremely difficult to understand its dynamics. All those countries that do not want to be subjected to this new paradigm in a negative way should work in order to adopt structures and measures as appropriate as possible. Like all the most developed and non-developed countries, Italy is striving to do so. The second research question of the thesis concerns the country. In what way is it possible to give impetus to the Italian cyber diplomacy so that it plays a significant role in the international cyber scene?

In order to attempt to answer this question, the new Italian cyber architecture and the most important example of success of cyber diplomacy in the country, that is, the adoption of the Lucca Declaration during the last Italian G7 presidency have been analysed. The topic has been enriched with a discussing with those who actively took part in the Italian team, namely the Minister Plenipotentiary Gianfranco Incarnato, the Engineer Pierluigi Paganini and Doctor Luigi Martino. It has emerged that Italy is only at the starting point of its cyber adventure, but the direction taken is indeed positive. Recent changes in the Italian cyber structure, which were absolutely necessary, have made Italy finally reach a basic level to be competitive on the international level. It is now necessary to implement these new policies as soon as possible. In particular, priorities are aimed at aligning all those structures that are part of the cyber architecture; increasing in the economic and human resources to be allocated to the sector; launching public campaigns aimed at promoting awareness of cyber security; setting up public-private partnerships that also include start-ups and SMEs in order to create innovation and stop being technology importer. As for cyber diplomacy, the Italian Ministry of Foreign Affairs should align itself as soon as possible to the main actors in the cyber scene and set up a unit devoted entirely to cyber diplomacy, coordinated with the other actors who deal with cyber issues and supported by a group of experts, with well defined strategy, hierarchy and roles, both in the national territory and abroad. On the one side, this would ensure the existence of a constant cyber dialogue which is for now relegated to international *fora* only. On the other side, the unit would also provide support for Italian citizens and businesses based abroad and operating in the cyberspace under the paradigms of the country in which they are located. Only in this way the future of Italian cyber diplomacy will cease to be uncertain and will guarantee Italy a place among the most influential actors of the current cyber scenario.

BIBLIOGRAPHY

Adesina, O. S., 2017, *Foreign Policy in an Era of Digital Diplomacy*, in *Cogent Social Sciences*, 3 (1).

Akamai, 2017, *State of the internet/Security Q2 2017 Report*, 4 (2), Cambridge.

Ashton, K., 2009, *That 'Internet of Things' Thing*, RFID Journal, p. 1.

Barston, R. P., 2014, *Modern Diplomacy*, Routledge, New York, p. 112.

Bennett, C. H., Brassard, G., 1984, *Quantum Cryptography: Public Key Distribution and Coin Tossing,* International Conference on Computers, Systems and Signal Processing, December 10-12 1984, Bangalore.

Bitonto, F., Marrone, A., Sartori, P., 2016, *Le sfide della Nato e il ruolo dell'Italia: Trump, Brexit, difesa collettiva e stabilizzazione del vicinato*, Istituto Affari Internazionali, Documenti IAI 16, p. 29-31.

Blank, S. J., 2008, *Web War I. Is Europe's First Information War a New Kind of War?*, Comparative Strategy, 27 (3), pp. 227-247.

Christou, G., 2014, *The EU's Approach to Cyber Security*, EUSC Policy paper series, Warwick.

Clusit, 2017, *Rapporto Clusit 2017 sulla sicurezza ICT in Italia*, Astrea, Milano.

Cohen, R., 1998, *Putting Diplomatic Studies on the Map*, Diplomatic Studies Program Newsletter, Centre for the Study of Diplomacy, Leicester, p. 1.

Cooper, A. F., Heine, J., Thakur, R. C., 2013, The Oxford Handbook of Modern Diplomacy, Oxford University Press, Oxford, p. 48.

Council of the European Union, May 28 2001, *2001/413/JHA Combating fraud and counterfeiting of non-cash means of payment*.

Council of the European Union, July 8 2016, *Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg*.

Council of the European Union, December 6 2016, *15283/16 Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*, Brussels, pp. 5-11.

Council of the European Union, May 18 2017, *Foreign Affairs Council, 18/05/2017*, Press releases.

Council of the European Union, June 7 2017, *9916/17 Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").*

Council of the European Union, June 14 2017, *Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016*, Brussels, p. 4.

Council of the European Union, June 19 2017, *Council conclusions on Progress report on the implementation of the common set of proposals endorsed by EU and NATO Ministers on 6 December 2016*, Press releases.

Crabb C. V. Jr., 1972, *American Foreign Policy in the Nuclear Age*, 3rd ed., Harper & Row, New York, p. 1.

Duque, R., Collins M., Abbate J., Azambuja C. C., Snaprud M., 2007, *History of ICT*, in *Past, Present and Future of Research in the Information Society*, Springer US, pp. 33-45.

EEAS, February 10 2016, *EU and NATO cyber defence cooperation,* Feature stories.

EEAS, February 10 2016, *EU and NATO increase information sharing on cyber incidents*, Press releases.

EEAS, December 25 2016, *NATO and EU press ahead with cooperation on cyber defence*, Press releases.

European Commission, March 3 2010, COM(2010) 2020 *Europe 2020: a strategy for smart, sustainable and inclusive growth*.

European Commission, May 19 2010, *COM(2010) 240 Digital Agenda for Europe*.

European Commission, March 31 2011, *COM(2011) 163 On Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security'.*

European Commission, February 7 2013, JOIN(2013) 1 Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace.

European Commission, April 28 2015, COM(2015) 185 The European Agenda on Security.

European Commission, May 6 2015, COM(2015) 192 A Digital Single Market Strategy for Europe.

European Commission, July 5 2016, IP/16/2321 Commission signs agreement with industry *on cybersecurity and steps up efforts to tacke cyber-threats,* Press release.

European Commission, July 5 2016, COM(2016) 410 Strengthening Europe Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.

European Commission, November 30 2016, *IP/16/4088 European Defence Action Plan: Towards a European Defence Fund*, Press release.

European Commission, January 2017, *EU cybersecurity initiatives: working towards a more secure online environment*, Factsheet.

European Commission, January 18 2017, *Public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA)*.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, September 13 2017, *JOIN(2017) 450 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.

European Parliament and Council of the European Union, December 13 2011, *Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.*

European Parliament and Council of the European Union, August 12 2013, *Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*.

European Parliament and Council of the European Union, July 6 2016, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*.

Evans, D., 2011, *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, Cisco Internet Business Solutions Group (IBSG), p. 3.

Faye, M., 2000, *Developing National Information and Communication Infrastructure (NICI) Policies and Plans in Africa*, Nigeria NICI Workshop, Abuja.

G7, April 11 2017, *G7 Declaration on Responsible States Behavior in Cyberspace*, Lucca, p. 1, 3-5.

Gazzetta Ufficiale, May 31 2017, *Decreto del Presidente del Consiglio dei Ministri 31 Marzo 2017*, 125, art. 3-12.

General Assembly of the United Nations, July 22 2015, *A/70/174 United Nations 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

Gibson, W., 1984, *Neuromancer*, Ace Books, New York, p. 67.

Giles, K., 2012, *Russia's Public Stance on Cyberspace Issues*, in Czosseck, C., Ottis, R., Ziolkowski, K., *2012 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, pp. 63-75.

Gillies, J., Cailliau, R., 2000, *How the Web was Born: The Story of the World Wide Web*, Oxford University Press, Oxford, p. 25.

Hanson., F., 2012, *Baked in and Wired: eDiplomacy @ State*, Foreign Policy Paper Series 30, Brookings Institution, Washington DC, pp. 1-41.

Healey, J., Van Bochoven, L., 2011, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, The Atlantic Council of the United States, Washington, p. 1.

Hey, T., 1999, *Quantum Computing: an Introduction*, Computing and Engineering Journal, 10 (3), pp. 105-112.

Hocking, B., Melissen, J., 2015, *Diplomacy in the Digital Age*, Clingendael Netherlands Institute of International Relations, The Hague, p. 30.

Ilves, L. K., Evans, T. J., Cilluffo, F. J., Nadeau, A. A., 2016, *European Union and NATO Global Cybersecurity Challenges. A Way Forward*, in *Prism*, Center for Complex Operations, Washington DC, 6 (2), pp. 124-141.

International Telecommunications Union, 2017, *Global Cybersecurity Index (GCI) 2017*, p. 60.

Kim, S., 2014, *Cyber Security and Middle Power Diplomacy: A Network Perspective*, The Korean Journal of International Studies, 12 (2), pp. 329-330.

Kurbalija, J., 2017, *An Introduction to Internet Governance*, DiploFoundation.

Laney, D., 2001, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, META Group, pp. 1-4.

Lété, B., Dege, D., 2017, *NATO Cybersecurity: a Roadmap to Resilience*, The German Marshall Fund of the United States, Policy Brief No. 23, p 3.

Maiorescu, T., 2015, *Cyber Diplomacy – A New Component of Foreign Policy*, Journal of Law and Administrative Sciences, (3), pp. 91-92.

Marchetti, R., Mulas, R., 2017, *Cyber Security: Hacker, terroristi, spie e le nuove minacce del web*, LUISS University Press, Rome, pp. 131-138, 148-149.

Martino, L., 2013, *La quinta dimensione della conflittualità. La rilevanza trategica del cyberspace e i rischi di guerra cibernetica*, Centro Interdipartimentale di Studi

Strategici Internazionali e Imprenditoriali (CSSII), Florence.

McAfee, A., Brynjolfsson, E., 2012, *Big data: the management revolution,* Harvard business review, p. 5.

McAfee Labs, 2016, *2017 Threats Predictions*, Santa Clara.

Mell P., Grance, T., 2011, *The NIST Definition of Cloud Computing (Technical report*), National Institute of Standards and Technology: U.S. Department of Commerce, Special publication, 800-145.

Mesterhazy, A., 2017, *NATO-EU Cooperation after Warsaw*, NATO Parliamentary Assembly, Defence and Security committee Report, p. 1.

Ministry of Foreign Affairs of Japan, October 14 2016, *First Meeting of G7 "Ise-Shima Cyber Group (ISCG)"*, Press release.

Müller, V. C., Bostrom N., 2016, *Future Progress in Artificial Intelligence: A Survey of Expert Opinion*, Fundamental Issues of Artificial Intelligence, pp. 555-572.

NATO, November 21 2002, *(2002)127 Prague Summit Declaration*.

NATO, November 20 2010, (2010)155 *Lisbon Summit Declaration*.

NATO, November 20 2010, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*.

NATO, August 19 2011, *Defending the networks: the NATO Policy on Cyber Defence*.

NATO, July 8 2016, (2016)124 *Cyber Defence Pledge*.

NATO, December 6 2016, *(2016)178 Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.*

NATO, December 15 2016, *Doorstep Statement by NATO Secretary General Jens Stoltenberg at the European Council on Security and Defence*.

NATO, April 2017, *NATO Cyber Defence,* Factsheet.

NATO, June 29 2017, *Defence Expenditure of NATO Countries (2010-2017)*, Press release.

NCI Agency, March 27 2017, *NATO gears up for 3 billion EUR tech refresh*, Communication.

NCI Agency, April 25 2017, *NATO launches first bids under major tech refresh,* Communication.

Official Journal of the European Union, July 19 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, art. 1.6 and art. 7.3.

Orman, H., 2003, *The Morris worm: A fifteen-year perspective*. IEEE Security & Privacy, 99 (5), p. 4.

Pernik, P., 2014, *Improving Cyber Security: NATO and the EU*, International Centre for Defence Studies, Tallinn.

Potter, E. H., 2002, Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century, McGill-Queen's University Press, Montreal & Kingston London Ithaca, pp. 84-85.

Presidenza del Consiglio dei Ministri, December 2013, *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*.

Presidenza del Consiglio dei Ministri, December 2013, *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*.

Presidenza del Consiglio dei Ministri, 2017, *Relazione sulla Politica dell'Informazione per la Sicurezza 2016*, Documento di Sicurezza Nazionale.

Presidenza del Consiglio dei Ministri, March 2017, *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*.

Rivest, R. L., Shamir, A., & Adleman, L., 1978, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 21 (2), pp. 120-126.

Schmitt, M. N., 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press. Schmitt, M. N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press.

Segal, A., 2017, *Chinese Cyber Diplomacy in an Era of Uncertainty*, Hoover Institution, Aegis Paper Serier No. 1730, Stanford.

Shanghai Cooperation Organisation, 2015, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*

Shanghai Cooperation Organisation, 2011, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*.

Shor, P. W., 1994, *Algorithms for quantum computation: Discrete logarithms and factoring*, In Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on, Ieee, pp. 124-134.

Smallenbroek, J., 2015, *Cyber Security: Cooperation or Proliferation?*, University of Groningen, p. 41.

Stang, G., 2013, *Global Commons: Between Cooperation and Competition*, European Union Institute for Security Studies, 17.

Symantec, 2017, *Internet Security Threat Report (ISTR)*, 22, Cupertino.

The White House, September 25 2015, *Fact Sheet: President Xi Jinping's Visit to the United States*, Office of the Press Secretary.

The United States Department of Justice, May 19 2014, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, Office of Public Affairs.

The United States Department of State, 2011, *International Cyber Diplomacy: Promoting Openness, Security and Prosperity in a Networked World*, The Office of Electronic Information, Bureau of Public Affairs, p. 1.

Van Der Meer, S., 2016, *Defence, deterrence, and diplomacy: Foreign policy instruments to increase future cyber security*, in Cherian, S., Munish, S., *Securing cyberspace. International and Asian perspectives*, Pentagon Press, New Delhi, pp. 96-97.

Von Solms, R., Van Niekerk, J., 2013, *From Information Security to Cyber Security*, Computers & Security, 38, pp. 97-102.

Wang, W., 2015, *Analysis on China's Cyber Diplomacy*, The Graduate School of Chinese Academy of Social Sciences, Beijing.

Wei, Y., June 21 2016, *China-Russia Cybersecurity Cooperation: Working Towards Cyber Sovereignty*, The Henry M. Jackson School of International Studies, University of Washington, Seattle.

Westcott, N., 2008, *Digital Diplomacy: The Impact of the Internet on International Relations*, Oxford Internet Institute, p. 3.

Wiener, N., 1948, Cybernetics: or Control and Communication in the Animal and the Machine, MIT Press, p. 19.

Xia, F., Yang, L. T., Wang, L., Vinel, A., 2012, *Internet of Things*, International Journal of Communication Systems, 25, p. 1101.

Zheng, Z., Xie, S., Dai, H. N., Wang, H., 2016, *Blockchain Challenges and Opportunities: A Survey*, Work Pap.

WEBLIOGRAPHY

Abdelshkour, M., IoT, March 25 2015, *From Cloud to Fog Computing*, Cisco Blogs. Link: http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing

Atlantic Cloucil, April 11 2017, *NATO and EU Members Join Finland's New Center for Countering Hybrid Threats.* Link: http://www.atlanticcouncil.org/blogs/natosource/nato-and-eu-members-join-finland-s-new-center-for-countering-hybrid-threats

Bing, Z., June 27 2016, *The Sino-Russian Joint Statement: the past and the future of Sino-Russian relations are here*, Xinhua. Link: http://news.xinhuanet.com/asia/2016-06/27/c_129092111.htm

Braw, E., August 23 2017, *Europe's Military Maestros: Italy*, Politico. Link: http://www.politico.eu/article/europes-military-maestros-italy-troops-mediterranean-migrants-libya-refugees/

Breene, K., May 4 2016, *Who are the cyberwar superpowers?*, World Economic Forum. Link: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Bremmer, I., January 12 2011, *The geopolitics of cybersecurity*, Foreign Policy. Link: http://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity/

Brown, G., Yung, C. D., January 19 2017, *Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace*, The Diplomat. Link: http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/

Brown, G., Yung, C. D., January 19 2017, *Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity*, The Diplomat. Link: http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/

Bulfon, F., August 14 2017, Dalle carte della Nato ai report su Siria e Libia: i segreti della Farnesina rubati da russi e cinesi, La Repubblica. Link: http://www.repubblica.it/tecnologia/sicurezza/2017/08/14/news/dalle_carte_della_nato_ai_report_su_siria_e_libia_i_segreti_della_farnesina_rubati_da_russi_e_cinesi-173004383/

Commission on Enhancing National Cybersecurity, 2016, *Report on Securing and Growing the Digital Economy*. Link: https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf

Di Corinto, A., April 6 2017, *Cybersicurezza, l'allarme degli esperti: "Borse mondiali nel mirino degli hacker"*, La Repubblica. Link: http://www.repubblica.it/tecnologia/sicurezza/2017/04/06/news/security_analist_summit_2017-162331025/

Difesa & Sicurezza, July 30 2017, *UE testa le difese dai cyber attacchi di un paese "quasi democratico"*. Link: http://www.difesaesicurezza.com/difesa-e-sicurezza/ue-testa-le-difese-dai-cyber-attacchi-di-un-paese-quasi-democratico/

ENISA on national cyber security strategies. Link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Finn, P., Horwitz, S., June 21 2013, *U.S. charges Snowden with espionage*, The Washington Post. Link: https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html

Guest Blogger, June 30 2016, *Despite Cyber Agreements, Russian and China a close as you think*, Council on Foreign Relations. Link: http://blogs.cfr.org/cyber/2016/06/30/despite-cyber-agreements-russia-and-china-are-not-as-close-as-you-think/

Gramer., R., January 27 2017, *Denmark Creates the World First Ever Digital Ambassador*, Foreign Policy. Link: http://foreignpolicy.com/2017/01/27/denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy/

Haq, T., F., A., September 15 2015, *In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia*, Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

Jackson Higgings, K., February 9 2016, *Chinese Cyberspies Pivot to Russia in Wake of Obama-Xi Pact*, Dark Reading. Link: http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242

Kaspersky Cybersecurity Index Italy 2016. Link: https://index.kaspersky.com/country/italy-h22016-all-all

Kirchgaessner, S., February 10 2017, *Russia suspected over hacking attack on Italian foreign* *ministry,* The Guardian. Link: https://www.theguardian.com/world/2017/feb/10/russia-suspected-over-hacking-attack-on-italian-foreign-ministry

Kopan, T., September 24 2015, White House readies cyber sanctions against China ahed of state visit, CNN Politics. Link: http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/

Korolov, M., September 17 2015, *Russian military attacked, possibly by Chinese cyber group*, CSO Online. Link: http://www.csoonline.com/article/2984599/advanced-persistent-threats/russian-military-attacked-possibly-by-chinese-cyber-group.html

Kurbalija, J., 2015, *Different prefixes, same meaning: cyber, digital, net, online, virtual, e-*, DiploFoundation. Link: https://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e

Lynch, D. J., Dyer, G., April 13 2016, *Chinese hacking of US companies declines*, Financial Times. Link: https://www.ft.com/content/d81e30de-00e4-11e6-99cb-83242733f755#axzz49iIJLMb8

Market Research Media, June 14 2017, *Quantum Computing Market Forecast 2017-2022*, Tabular Analysis. Link: https://www.marketresearchmedia.com/?p=850

Mikheev, V., March 22 2017, *Why do Beijing and Moscow embrace cyber sovereignty?*, Russia Beyond the Headlines. Link: http://rbth.com/opinion/2017/03/22/why-do-beijing-and-moscow-embrace-cyber-sovereignty_725018

NATO, November 21 2002, *Prague Capabilities Commitment*. Link: http://www.nato.int/cps/en/natohq/topics_50087.htm

NATO, December 21 2005, *Comprehensive Political Guidance*. Link: http://www.nato.int/cps/on/natohq/topics_49176.htm

NATO, February 17 2017, *Cyber Defence*. Link: http://www.nato.int/cps/en/natohq/topics_78170.htm

NIST, 2016, *NISTIR 8105 Report on Post-Quantum Cryptography*, US Department of Commerce. Link: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

Official page of the Australian ambassadors and other representatives of the Department of Foreign Affairs and Trade. Link: http://dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs.aspx

Official page of the Italian Ministry of Defence on the troops employment in international operations. Link:

https://www.difesa.it/OperazioniMilitari/Documents/Mappa_Operazioni_Militari_IT_ultima.pdf

Official page of the Italian Ministry of Foreign Affairs on the role of Italy in NATO. Link: http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

Official page of the Italian Ministry of Foreign Affairs on the role of Italy in the EU. Link: http://www.esteri.it/mae/it/politica_europea/italia_in_ue

Official page of the first coordinator for cyber issues in the secretary's office at the State Department of the United States of America. Link: https://www.state.gov/r/pa/ei/biog/161848.htm

Official website of the Estonian Presidency to the Council of the European Union. Link: https://www.eu2017.ee/news/insights/cybersecurity-and-estonian-presidency

OSCE, March 10 2016, *Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risk of Conflict Stemming from the use of Information and Communication Technologies*. Link: http://www.osce.org/pc/227281?download=true

Oxford Dictionary, *Definiton of "diplomacy"*. Link: https://en.oxforddictionaries.com/definition/diplomacy

Paganini, P., March 6 2015, *Cleaning up the Cyber Mess: Adopting Cyber Hygiene principles*, Security Affairs. Link: http://securityaffairs.co/wordpress/34502/security/cyber-hygiene-principles.html

Painter, C., August 1 2017, *The Case for Diplomacy in Cyberspace*, Medium Digital Diplomacy. Link: https://medium.com/digital-diplomacy/the-case-for-diplomacy-in-cyberspace-8ca1ca8c97b3

Pozzo, F., October 5 2016, *La portaerei italiana che Mussolini affondò*, La Stampa. Link: http://www.lastampa.it/2016/10/05/societa/mare/la-portaerei-italiana-che-mussolini-affond-tw0ieYL24evBbgRxeFKPxN/pagina.html

Redazione, October 31 2016, *Italia: 150 milioni di euro previsti per la sicurezza cibernetica*, Startupitalia. Link: http://cybersecurity.startupitalia.eu/53212-20161031-italia-150-milioni-cybersecurity

Renard, T., 2015, *US-China Cyber Security Agreement: a Good Case of Cyber Diplomacy*, EGMONT Royal Institute for International Relations. Link: http://www.egmontinstitute.be/publication_article/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/

Report of the Yekaterinburg Agreement. Link: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

Reuters, June 23 2013, *China 'gravely concerned' by Snowden's claims of U.S. cyber attacks on China,* World News. Link: http://www.reuters.com/article/us-usa-security-china-idUSBRE95N01C20130624

Riordan, S., 2016, *Digital diplomacy v. cyber diplomacy: terminological distinction*, Center on Public Diplomacy Blog, University of Southern California. Link: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

Robinson, M. R., March 23 2015, *Foreign Policy in the Age of Cybersecurity Threats*, SecurityIntelligence, Link: https://securityintelligence.com/foreign-policy-in-the-age-of-cybersecurity-threats/

Roth, A., May 8 2015, *Russia and China Sign Cooperation Pacts*, New York Times. Link: https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html

Short biography of Amb. Luca Giansanti on the website of the Italian Ministry of Foreign Affairs. Link: http://www.esteri.it/mae/it/ministero/struttura/dgaffaripoliticisicurezza/dirgen_dgaps.html

Short biography of Dr. Luigi Martino on the website of the University of Florence. Link: http://www.cssii.unifi.it/vp-90-responsabile-del-center.html

Short biography of Eng. Pierluigi Paganini on his blog Security Affairs. Link: http://securityaffairs.co/wordpress/author/paganinip

Short biography of Min. Plen. Ginfranco Incarnato on the website of Aracne Editrice. Link: http://www.aracneeditrice.it/aracneweb/index.php/autori.html?auth-id=379166

Sistema di Informazione per la Sicurezza della Repubblica, *Normativa di riferimento*. Link: http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento.html

Statement on the EU-NATO cooperation on the official website of the Italian Ministry of Foreign Affairs. Link: http://www.esteri.it/mae/it/politica_estera/organizzazioni_internazionali/nato.html

Statista, *Number of social media users worldwide from 2010 to 2020 (in billions)*. Link: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users

Sulmeyer, M., Roncone., G., August 23 2017, *The Making of a Cyber Diplomat*, The Cipher Brief. Link: https://www.thecipherbrief.com/column/cyber-advisor/back-basics-u-s-cyber-diplomacy

Technopedia, *Definition of Information and Communication Technology*. Link: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict

The Digital Single Market of the European Union. Link: https://ec.europa.eu/digital-single-market/

The Foreign & Commonwealth of the United Kingdom's blog on its digital diplomacy. Link: https://blogs.fco.gov.uk/digitaldiplomacy/

World Bank, *Internet users (per 100 people)*. Link: http://data.worldbank.org/indicator/IT.NET.USER.P2

ABSTRACT

With the signing of a Technical Arrangement in February 2016, the European Union (EU) and the North Atlantic Treaty Organization (NATO) launched an important program of cooperation on cyber security. Since then, many steps have been taken by the two organizations in that direction. Given the early stage of the cooperation and the urgent need to carry out this project with determination and effectiveness, the necessity to put together all that is at the basis of this process, and question its matter, has been perceived.

This thesis has a dual purpose. On the one hand, it seeks to raise awareness among all those who have little sense of the theme of cyber security. In fact, the dissertation is not just for all those who, in one way or another, make part of the system that produces cyber security policies within the EU, NATO and on behalf of the Italian Republic. But also to the common citizens who ignore this topic, especially because of the little information the media dedicate to it. If cyber security discussions concern only one niche in society, the study of cyber diplomacy and its related topics seem to be even more elitist. Therefore, it is intended to use a simple and not so technical language to deal with a delicate and complex subject, which is absolutely necessary to be addressed in today's world. On the other hand, the dissertation is committed to answer two research questions. The first: how can the EU-NATO cooperation on cyber security be effective and not counterproductive? The second: in what way is it possible to give impetus to the Italian cyber diplomacy so that it plays a significant role in the international cyber scene?

The first chapter had the task of defining the framework in which these issues were analysed. In more depth, this part has dealt with the increasing involvement of diplomacy, understood as a foreign policy tool for achieving national objectives, in cyberspace. The analysis has focused on how the growing use of information and communication technologies (ICTs), which are all the technologies used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, network-based control and monitoring functions, is deeply changing this role. Among them, the internet is the connecting tool *par excellence*. The fact that, according to the World Bank,

nearly half of the world population has an internet connection and regularly surf the net, has also changed how diplomacy is conducted.

First of all, the relationship between time and space is now perceived in a new way. The transboundary effect of information technology provides real-time material captured with an ordinary mobile phone and transmitted globally. If there is an internet connection, there can be an almost instant communication, from everywhere to everywhere. Second, the quantity of information has become enormous. The spread of technology has led to a greater geographic availability and depth of knowledge. The increasing volume of available opinions relating to national and international issues is made up of online comments, views, and data. Due to these interactions, the traditional assessment duty of diplomacy has never become so articulated and thus difficult. Third, the line between private and public spaces is blurred. ICTs have widened the functions of personal communication systems in searching for information and applications. The constant hunt for technical development has made these systems an essential diplomatic tool. The fourth major effect brought by information and communication technologies in the management of diplomacy has to be found in the variety of new threats and targets related to the cyberspace. With the growth of technology, the threats which derive from it are also expected to grow.

Governments are among the targets most affected by these threats and among those who most frequently perform the attacks. In this chapter, cases where governments have been the main protagonists of cyber attacks were cited. Among the others, the 2007 cyber attacks on Estonian parliament, ministries, newspaper and bank websites; the 2008 cyber attacks during the Russo-Georgian war; the 2010 cyber attack towards the Iran's nuclear program; the 2014 cyber attack to Ukraine's, European and NATO allies infrastructures of information technology during the Russian military intervention in the country; and the 2017 cyber attack to the national press agency of Qatar (which eventually led to an ongoing diplomatic crisis).

Due to the specificity, the ever-increasing frequency, and the unbounded effects of such attacks, a new kind of diplomacy that focuses only on cyber space issues is therefore necessary. Creating common advantage through dialogue is the primary role of diplomacy. Creating common advantage through dialogue on cyber security issues is the primary role of cyber diplomacy. In more depth, cyber diplomacy uses diplomatic tools to solve the problems that emerge in the cyberspace. The cyber diplomacy has to be necessarily distinguished from the kind of diplomacy that uses ICT tools, i.e. digital diplomacy. Issues such as the structuring of internet governance, the respect for human rights online, the enforcement of law against cyber crime, how to respond to malicious acts arising in the cyberspace, the protection of strategic know-how, and many others, are of primary importance and cannot be abandoned to the law of the strongest as in the jungle. Currently, cyberspace is a virtual jungle where prowlers are always lurking, and dangers are around every corner. Unfortunately, too often the virtual world is still considered as something abstract. However, the virtual world is a real world, based on physical structures, and as such, it has an impact on real things.

When in 1988, Robert Morris, son of a National Security Agency (NSA) officer, launched a computer worm from Cornell University that infected between 4,000 and 6,000 machines, about 5% of all computers connected to ARPANET network in those years, made for the first time computer safety a worldwide priority. No one would have expected the first cyber attack in history to be conducted from the inside. The Advanced Research Projects Agency Network (ARPANET) was nothing more than the internet ancestor. The network was born in a project promoted in 1969 by the Defence Advanced Research Projects Agency (DARPA), a Defence Department agency of the United States of America (USA), in order to optimize the speed of information exchange between universities and research laboratories. However, for its distributed network architecture, this tool proved to be very useful for the military during the Cold War because it avoided any kind of blockade in internal communications which could arise after a Soviet attack on telephone lines. The invention of a data transmission suite from one node to another through Transmission Control Protocol/Internet Protocol (TCP/IP) completed the project. Its use has grown to a massive extent. Today, there are 3.3 billion of regular internet users worldwide, of which 29 million are only in Italy. The original ARPANET project, which ignored any defence and protection system, has now evolved and become the largest network of digital interactions. Despite the fact that it is impossible to calculate an exact figure, due to the peculiar characteristics of the cyberspace that make it difficult to attribute and estimate damage, all major cyber security companies agree that cyber crime alone (without considering the social sphere) has a global annual cost of various hundreds of billions of dollars. In addition, they all agree that trends are inevitably destined to grow exponentially.

However, it is important not to confuse the internet with the cyberspace. While the internet refers to the concept of a network of networks, cyberspace refers to virtual reality as a whole, where the internet is only a part of it. In 2010, the American Department of Defence formally recognized cyberspace as a new domain of warfare, the fifth after earth, sea, air, and space. The same thing happened in 2016 within the Atlantic Alliance when NATO defence ministers expressed their support for this position. Although in a different way, in 2011 China, Russia, Tajikistan, and Uzbekistan (within the Shanghai Cooperation Organization) also acknowledged the presence of common challenges in the sphere of information security. States therefore claim a prominent role in enforcing security within this domain, which, like the other four, is now considered to be a global common. A global common is a place beyond the jurisdiction of individual countries, a resource that no one can claim as its own and to which security access should therefore be guaranteed. However, these guarantees are subject to a heated debate. Different geopolitical interests mixed with different ways of conceiving the cyberspace and its related policies make it impossible, at this time, to reach an international agreement for the creation of a shared and respected framework. In particular, cyber diplomacy faces the toughest role of elaborating rules for the narrow circle of sovereign states operating in the cyberspace, which however share that space with a myriad of non-sovereign and hard to identify actors. While states must necessarily represent the actors who have the last word on internal security, on the other hand, they would have to accept themselves to be bound by rules of behavior in a promiscuous space. Unfortunately, today, the time seems to be still a little too premature to be able to create this project efficiently.

These problems lead the efforts of cyber diplomacy to focus on bilateral or multilateral *fora* of like-minded states. But all that glitters is not gold. With regard to the former, chapter 1 has proved with the examples of agreements between the USA and China and between Russia and China, three of the most important actors in the cyber scene, that outputs can be very different. Only two months after the signing of the Sino-Russian agreement, the number of Chinese speakers who have targeted Russia has increased by 300% from December 2015 to February 2016. In contrast, Chinese hacking activities against American companies seem to have declined since the September 2015 agreement between President Barack Obama and

President Xi Jinping. This is because the Sino-Russian tie on cyber security appears to be more dependent on the relationship with the US than on the partnership itself between the two Asian countries. Both the governments of Beijing and Moscow are concerned about the American advocacy for internet freedom as a priority of its foreign policy. Fearing the ongoing dominance of the United States over the internet, China and Russia just combine their efforts to seek more geopolitical influence through the reshaping of the cyberspace.

As for multilateral *fora*, discussed in chapters 2, 3, and 4, cyber diplomacy measures have been used within the United Nations Group of Governmental Experts (UN GGE), the Organization for Security and Cooperation in Europe (OSCE) and the Group of 7 (G7). Since 2004, the UN GGE has come together in five different compositions and has adopted increasingly detailed and proactive reports on the need to develop a code of conduct to apply in cyberspace. Unfortunately, last June, the fifth UN GGE recognized the impossibility of reaching a consensus because of an opposition between Cuba (supported by Russia and China) and the United States. On the line of this work, the OSCE has set itself the objective of developing Confidence Building Measures (CBMs) to be approved at different times in order to improve transparency, stability, and cooperation in this area. For now, work continues in a serene way because the adopted sets are rather theoretical. In the wake of this work, the G7 has also played an important role in cyber diplomacy. In particular, during the last G7 Summit, the Declaration on Responsible States Behavior in Cyberspace has been approved. Although this is not binding, the Declaration is an important step in accepting states' responsibility. However, it is important to remember that the Lucca Declaration has been accepted among like-minded countries, members of one organization. That is why, at the moment, the best place to be able to pursue cyber security cooperation programs seems to be that of bilateral cooperation between international organizations that share the same values and interests. The program launched recently between the European Union and the North Atlantic Treaty Organization is currently one of the most important of these.

Three are the main reasons why greater cooperation between the EU and NATO is not only desirable but indispensable. The first one is that new threats require new ways of collaboration and new levels of ambition. Without losing their established shared values, the EU-NATO strategic partnership could give a new impetus to tie the transatlantic relationship.

In times of uncertainty, there is a need for strong institutions. In order to do that, on the one side, it is necessary to ensure an effective and fair burden-sharing, and, on the other side, operate in accordance with their own strengths and capabilities. Each nation alone has just a single set of forces. The very same nations can double its force by being a member of an international organization and then re-double it with a collaboration between two international organizations.

The second main reason for enhancing the EU-NATO cooperation is linked with the fact that the European Union is building step by step its own defence. More European collaboration and expenditure on defence will lead to a stronger Europe. This will strengthen not only the EU but also NATO, as half of its geopolitical interests are in the European region or next to its borders. However, without a deep and strategic dialogue between the two organizations, the risk of creating duplications is high. A constant diplomatic activity between the EU and NATO would assure the complement themselves and avoid any sort of non-sense competition.

The third and most relevant reason why the search for a more efficient EU-NATO dialogue is needed is the fact that, having 22 members in common, the political and economic union and the intergovernmental military alliance share a mutual interest in becoming more resilient to cyber attacks. In the last ten years, both have officially recognized that cyber security is a major challenge for the achievement of their objectives and the reinforcement of their core values. In particular, the union and the alliance have realised that all the future conflicts will see the presence of actions performed in the cyberspace. Therefore, a failure in cyber security is equal to a failure in a classical national security apparatus. As a consequence, this kind of failure could lead to the deterioration of a copious set of interests, both in the public and in the private sectors. Neither the EU nor NATO alone have the tools to address these risks.

The second chapter of the thesis has been entirely devoted to the security strategies of the two international organizations. Therefore, it has been divided into two parts: the first one has analysed the European Union's strategy, while the second one has dealt with the strategy of the North Atlantic Treaty Organization. The background, evolution and all the steps that have led both organizations to adopt their current cyber security strategies have been analysed in detail. Particular attention has then be given to the objectives of these strategies. Without a clear identification of the goals of either organization, it would be impossible to undertake a cooperation. The dissertation has then briefly examined the legal frameworks in which the EU and NATO incorporate such strategies as well as the agencies that the two organizations have set up to operate in the cyber security sector. Finally, it has dealt with the funds that both organizations allocate to tackle cyber threats. The analysis has shown how the different nature of the two organizations deeply models these strategies and the perception member states and allies have of them. In particular, because of the fragmentation within the EU foreign policy (or rather, policies), confirmed by the declaration contained in the fundamental NIS Directive, according to which all that concerns national security remains the absolute prerogative of the states, the European member countries fail to be united on the cyber front. On the contrary, there seems to be much more cooperation and cohesion in dealing with the issue within NATO. This is mainly due to the fact that risk perception is greater within an alliance born and conceived as a military pact.

Before dealing with the issue of cooperation between the two organizations, the focus of the analysis has briefly shifted to the global landscape of the cyber threat. From the analysis of threat geography trends, recorded cases, motivations behind the attacks, and the different types used, it has emerged that the spectrum of cyberspace threats is expected to grow in the future. This is due to its simplicity and low cost with which attackers successfully run cyber attacks, while defending from such attacks requires high costs and complex defence structures.

It has then been shown how the cyber security industry will face several challenges. An evolution in technology necessarily implicates an evolution of the risks. Among these, the advent of quantum computing, which would have a revolutionary impact on cyber security, especially with regard to cryptography. Absolute importance will also have to be given to the close relationship that binds big data and the internet of things; the trade off between the benefits and risks associated with cloud computing and how these can be secured with fog computing and blockchain. The paragraph has been concluded by pointing out once again the absolute importance of the human factor in cyber security. To ensure that risks do not overcome the benefits of interaction between people and ICTs, it is vital to develop a culture of security through indoctrination of cyber hygiene practices and the creation of an international framework to both punish those who attack and to protect those who are victims of these attacks, in a universal and binding manner. All the actors are potential performers and victims of this new threat. The main players in cyberspace will necessarily need to consider these new themes and the new potential threats that these bring with them along with the benefits.

As repeatedly highlighted in the text, a new type of threat requires a new kind of cooperation. In the second part of chapter 3, the matter of the EU-NATO cooperation on cyber security has been analysed. From a careful analysis of the steps taken so far, it has emerged that, due to the intrinsic characteristics of the two organizations, the very nature of cyberspace and the numerous risks involved, greater cooperation between the EU and NATO not only is desirable but absolutely indispensable. Although cooperation has only begun recently, many points have already been discussed. In particular, the ideas of facilitating info-sharing and performing joint exercises are very important, as well as the establishment of the joint set of proposals necessary to implement this cooperation. Indeed without a common strategy, there can be no common work. However, these appear to be only first and timid steps. In particular, without the creation of a physical linking point that allows a constant dialogue between the two organizations, there is a risk that the efforts of both will not match the needs and end up creating unnecessary and counterproductive overlaps. On the contrary, it is desirable that the two exploit their very different characteristics and potentials, such as efficient EU soft power capability, and equally strong NATO hard power, so as to contribute by filling gaps. Without such a meeting point, the process is likely to proceed too slowly. In addition, both the EU and NATO should work together to create a framework for cyberspace that is recognized and implemented by all members and allies with the aim of extending this involvement to third countries.

Finally, the focus of chapter 4 has entirely been devoted to the Italian situation. First, the role of the country between the EU and NATO has been analysed. The theme has been enriched by an interview with the Director General for Political and Security Affairs of the Italian Ministry of Foreign Affairs, Ambassador Luca Giansanti. The country has always played an important role within the two organizations. This is not only because Italy is a founding member of both, but above all because of its strategic position and its active, timely and steady engagement in the major areas of crisis of the Union and of the Alliance. Defined as the "Europe's military maestros", Italian troops lead operations that ensure stability and support (mostly) in the precarious territory of Kosovo, Lebanon, and Libya. Moreover, due to its physical structure of "aircraft carrier in the Mediterranean Sea", Italy contributes almost autonomously to the rescue of thousands and thousands of migrants crossing the waves of the Mediterranean Sea in an attempt to reach the European coast. For these reasons, its balance between Europeanism and Atlanticism, the country can certainly be a driving force for the development of the EU-NATO cooperation program in at least two of the seven cooperation areas agreed during the NATO-EU Joint Declaration of July 2016, namely maritime cooperation and security capacity building. As for the contrast to hybrid threats and the cyber security sector, unfortunately, Italy is not currently able to play the very same special role.

The second paragraph of the final chapter has dealt with the current status of the cyber threat in the Italian peninsula. As in the previous chapter, the trends that relate to the reasons for threats, the most affected sectors, and the types of attack performed have been analysed. Again, the analysis of this strategy necessarily served to introduce the Italian cyber strategy and is intended to understand the role of the Italian diplomacy in the cyberspace. It has emerged that the Italian case does not differ much from the global situation, reinforcing the notion that the fifth domain does not make national distinctions. For its intrinsic nature, a cyber attack can in fact be carried out by anyone to anyone, anywhere from any place. In a sense, the cyber domain nullifies space and time, making it extremely difficult to understand its dynamics. All those countries that do not want to be subjected to this new paradigm in a negative way should work hard in order to adopt structures and measures as appropriate as possible. Like all the most developed and non-developed countries, Italy is striving to do so.

From a deep analysis of the new Italian cyber architecture, it has emerged that Italy is only at the starting point of its cyber adventure, but the direction taken is indeed positive. Recent changes in the Italian cyber structure, which were absolutely necessary, have made Italy finally reach a basic level to be competitive on the international level. In line with the European NIS Directive, the Gentiloni Decree has above all the merit of putting Italy at a level of maturity similar to that of other countries, at least as regards the institutional level. This has introduced novelties that were absolutely necessary. In particular, the strengthening of the strategic role of the intelligence agencies, through the *Dipartimento delle Informazioni per la Sicurezza*, in the field of cyber security; the centrality of the *Nucleo per la Sicurezza Cibernetica* on the prevention, preparation and response of the Italian government in the event of cyber crime; and the establishment of a national assessment and certification centre for verifying the security conditions and the absence of vulnerabilities on products, equipment and IT systems. It is now necessary to implement these new policies as soon as possible and establish others. In particular, priorities are aimed at aligning all those structures that are part of the cyber architecture; increasing in the economic and human resources to be allocated to the sector; launching public campaigns aimed at promoting awareness of cyber security; setting up public-private partnerships that also include start-ups and SMEs in order to create innovation and stop being technology importer.

The speech has then focused on the Italian cyber diplomacy. In this respect, a case of successful multilateral cyber diplomacy favoured by the Italian commitment has been analysed: the adoption of the Lucca Declaration during the last G7 Summit. It has been possible to know in detail all that preceded the signing, its reasons, the points of disagreement and what to expect for the future of such agreement by discussing it with those who actively took part in the Italian team, namely Minister Plenipotentiary Gianfranco Incarnato, Engineer Pierluigi Paganini and Doctor Luigi Martino. The Lucca Declaration, formally the "G7 Declaration on Responsible States Behavior in Cyberspace" was signed by Italy, USA, UK, France, Germany, Canada, and Japan in April 2017 during the last G7. Although the statement is not binding, the Declaration is a positive output of the activity of cyber diplomacy. In more depth, it is an important acknowledgment of the states' commitment to address the major threats in the cyberspace that today undermine the political, economic, and technological sectors of the states. The impact of the Declaration has to be estimated, however, considering that within the G7 there is a general presence of like-minded states. The sharing of the same ideals, values, and conception of cyberspace, has facilitated the unanimous cooperation and acceptance of these norms of behavior. The absence of relevant nations such as Russia and China in this dialogue cannot be neglected. Surely, it will be necessary to move this discourse to other *fora*. With regard to Russia, the best place could be the Organization for Security and Co-operation in Europe (OSCE) and, with regard to China, the Group of 20 (G20). The creation of an international framework that is legally recognized and respected is certainly the most important requirement as well as the current challenge in the cyber security sector. However, while there is a general positive cooperation in the field of cyber crime, cooperation in the field of information warfare is far from being a reality. However, sooner or later, states will either cooperate or accept the fact that the responsibility for a failed cooperation will fall on them.

Finally, in the last paragraph of the chapter, there has been a quest to find an answer to the second research question set in the introduction of the thesis. In what way is it possible to give impetus to the Italian cyber diplomacy so that it plays a significant role in the international cyber scene? As for the Italian cyber diplomacy, the Italian Ministry of Foreign Affairs should align itself, as soon as possible, to the main actors in the cyber scene and set up a unit devoted entirely to cyber diplomacy. This unit would necessarily be coordinated with the other actors who deal with cyber issues and supported by a group of experts, with well defined strategy, hierarchy and roles, both in the national territory and abroad. On the one side, this would ensure the existence of a constant cyber dialogue which is for now relegated to international *fora* only. On the other side, the establishment of a trained body of cyber diplomats and officers at Italian missions around the world, to perform cyber diplomacy as a new tool of foreign policy, would also provide support for Italian citizens and businesses based abroad and operating in the cyberspace under the paradigms of the country in which they are located. In addition, it goes without saying, courses and updates for employees on the dangers of cyber space and the good practices to be adopted in the regular conduct of the activities within the Ministry of Foreign Affairs and its international missions, are at the very basis of this process of growth. Only in this way the future of the Italian cyber diplomacy will cease to be uncertain and will guarantee Italy a place among the most influential actors of the current cyber scenario.