Department of POLITICAL SCIENCE

Master's Degree in International Relations

European Studies

Chair of INTERNATIONAL PUBLIC POLICIES

DEALING WITH EMERGING THREATS:

DIFFERENT PRIORITIES AND RESPONSES IN A COMPETITIVE WORLD

Prof. Raffaele Marchetti	Prof. Gianfranco Pellegrino
SUPERVISOR	CO-SUPERVISOR

Clarissa Guerrini

635172

CANDIDATE

Academic Year 2018 - 2019

Clarissa Guerrini 635172

Dealing with emerging threats:

different priorities and responses in a competitive world

Index

Introduction

The research question (RQ) behind this thesis is “if and why states and international organizations have different perspectives of emerging threats, although the majority of threats are global and demand a comprehensive approach to be solved?”. Such a question can find easily a response if divided in two part. The first part concerns an in-depth analysis about emerging threats (chapter 2), while the second present a pragmatical focus on states and international organisations security approach (chapters 3,4,5). Nonetheless, it is important to clarify at the beginning (1 chapter) the term “security” and the evolution of the concept of “threat”, which represent the key of lecture of the entire text. Among the most dangerous emerging threats, only three are going to be considered to circumscribe the broad spectrum of the current global challenges, namely climate change, biological weapons and cyber-threats.

Thus, the thesis is going to present both a descriptive and a case studies section, which will be the actual base to draft the conclusive analysis and give and answer to the RQ. The case studies analysis is going to show - besides some obvious similarities - evident differences in the national approaches and in the multilateral responses among the considered entities. This is clear especially in the American, Russian and Chinese approach as well as in the NATO and SCO security strategies. It is not surprising that these two IOs are less global and cooperative than UN and EU, since they are influenced by strong leading countries like the US, China and Russia. Overall, the UN has the more global and comprehensive approach in dealing with emerging threats, but its power is limited by the contradictions of the Security Council, where the power of states prevails over the common good. Finally, the case of the EU and Italy is quite controversial. Both has adopted reforms and vision with a global scope until now, but the realist pressure in the current international scenario has led Italy towards a populist turning and the EU to adopt a more defensive approach in its IR. Taking everything into account, each entity presents its peculiarities and priorities, which makes difficult to find a common ground to deal with new threats.

The reason behind such a diversity can be found in the theory of the “red zone”, enshrined by the Italian analyst Edoardo Camilli in the framework of a research carried on by the Italian intelligence. According to Camilli, the choice of the priorities to include in the national security strategy depends on the environment in which each state operates. This environment is affected by external inputs, like threats and international interests, to which the state must respond. Nonetheless, the rising complexity of the international system and the proliferation of several global threats demand to circumscribe the area of analysis to better grasp these changes. Then, the area of reference becomes a “red zone” generated by the interaction between inputs from the international system (threats and opportunities) and the state's ability to respond to these inputs, defending itself and promoting its own interests. In other words, the shape and the extent of this area depend only on state's capabilities. Thus, more a state is strong - in term of "smart power" (the union of hard and soft power) - bigger the red zone will be. Following this reasoning, states prefer to focus on domestic security when they are uncapable to do otherwise. Such a weakness is the result of internal features, such as the lack of cohesion, ineffective institutions and loss of government legitimacy. These states are less able to turn resources into power and generate strategic plans to address global threats because the ruling elite is concerned only by its own political survival.

Another hypothesis which justifies state subjective approach concerns the matter of values. In effect, people have always interpreted the reality through the filter of cultural values and historical experiences, creating different perceptions of facts and, thus, security. Indeed, the strategic culture intervenes on the behaviour of the states influencing the understanding of the other, the morale of the troops in war and the politics of alignment and alliances. Moreover, this determines a state's sensitivity to threats, for instance towards those suffered throughout history. These are the reason why a national security strategy cannot be completely objective.

According to these theories, the fact that in a globalized world, with global challenges to face, the majority of states focus on internal security rather than global one is not a contradiction. In fact, it must be considered that globalization has enhanced instability worldwide, which result in states' insecurity and consequent loss of power. State has responded to that adopting a closed and prudent approach, trying to restore their strength.

To sum up, nowadays it is impossible to build a homogeneous and objective global security strategy. However, to deal with new threats and maintain peace worldwide, states and international organizations should engage to find some common grounds and overcome their ancient grudges.

Chapter 1. The evolution of traditional threats

The matter of security has traditionally occupied a priority position in the hierarchy of public goods supplied by states, not only because it is linked to the exercise of the "monopoly of force" - which is the main feature of a state - as theorized by Max Weber, but also because it is a "preparatory" (Foradori and Giacomello 2014: 292) public good. In other words, it is not possible to provide other services, such as welfare, education and health, in an unstable or insecure environment. The reasons that led to the lack of security are represented by poverty, destitution and disease in weak or current failed states, for example in Somalia, Libya and Syria. Thus, security is a fundamental dimension, a basic condition of social living.

On an academic level, security studies arose in the 1980s as an evolution of "strategic studies" to justify non-state and non-military security threats. Since the publication of *People, States and Fear* by Barry Buzan (1983) this field of analysis has developed. According to Buzan, security is not just an objective fact, but can be a subjective and individual condition, influenced by emotions and psychological attitudes. Recent studies have proposed the following example: why is the Iranian nuclear program so frightening? And why, on the other hand, do we not perceive the Indian or the Israeli threat as a threat? Therefore, the content and meaning of security change over time influencing people's perception of the menace.

Moreover, today the state is no longer - or not only - the main security actor, and security is no longer just international but "global" (Foradori and Giacomello 2014: 292). The term global security refers to the extent and the interconnected nature of threats emerged in the era of globalization. Two brief examples about Libya and Syria, weak states characterized by several threats, might clarify this concept. As a matter of fact, the current fragility in Libya or Syria is stirring up terrorism and insurrections. Such disorders are exploited by criminal networks to increase income, selling arms and drug. Furthermore, the instability can be projected in the so-called "democratic countries" through migratory flows and crisis in energy supplies. Consequently, the western and technologically advanced states struggle to defeat the root causes of instability. Nevertheless, the instability has been enhancing in the last few years by tools of scientific and technological progress - like nuclear physics and cyber-technology. As a result, new global threats are complex, and states demand new approaches to deal with security. At this point, it is important to analyse in-depth the meaning of security to understand such approaches and be clear about the definition of "threats"[1].

[1] See Foradori and Giacomello (2014: 292)

1.1.The meaning of security in a competitive world

In the last few years, an increase in global and catastrophic conflicts has made the study of security central to policymakers and academics, who seek to understand, predict and prevent threatening behaviours in global politics. At the beginning, the security studies approach has followed a realist disposition, which defined security as the capacity to resist negative change and defend national interest. According to realism, the State is the ultimate guarantor of security and "no state will never sacrifice its interests to serve the larger community" (Frankel 1996: 15). At the base of the realism is the assumption that there is a sense of threat in the international system, an anarchy that menaces the Nation-State power. This is the reason why "the ultimate concern for states should not be for power but for security" (Waltz 1988: 616) and each State should deal with that through the use of force (Waltz 1959: 160). To sum up, the traditional security studies literature requires a powerful State and explores how states maintain the integrity of their borders and protect their communities from external threats of violence.

In 1994, a change in the paradigm occurred with the UN Human Development Report and the introduction of the term "human security". The report argued that "the concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy […]. It has been related more to nation-states than to people". On the contrary, the report sought to orient the referent object of security towards individuals and what makes them insecure in their everyday life. Security was defined as safety from chronic threats, such as hunger, disease and repression, and protection from sudden and hurtful disruptions in the patterns of daily life.

Today, it is undeniable that under the concept of security are issues beyond territorial conflicts and inter-state aggression, as in the case of the unconventional threats, analysed in the following section. In this sense, the term "security" encompasses different sectors of analysis, which are, according to Barry Buzan, the military, the political, the economic, the societal and the environment (Buzan 1991; Buzan et al. 1998: 7). The consequences of such a "broadening" in the security agenda can be positive or negative. On one hand, it provides greater scope to address non-military threats that are currently impinging on the health and safety of individuals and communities. On the other, it does create a problem because if "ordinary" issues in economics, society and politics are brought under the security umbrella then the "extraordinary" measures become ordinary, endowing actors - usually governments - with greater power. As a result, the risk of losing social and civil right may occur and the state assumes a major and more powerful role. This is one of the main reasons why state security agenda tend still to focus on national interests rather than individual safety. Thus, despite an apparent change in security approach, the realist paradigm and the centred role of the State in security still remains. Following such a reasoning, the definition of the menaces depends on national interests.

1.2.The definition of "threat"

The definition of the menace is the first step that allows to contrast and prevent potential threats. This is the base to apply a proper strategy and, consequently, safeguard security.

By definition, "threat" means a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done. This definition describes threats at the level of individuals, referring to harms against human life and health. As mentioned in the previous section, when the menace is considered as "global" the focus on security scaled up to encompass wider political communities, such as nation, state, regional body, religious community or civilization. By the way, the analysis shifts towards the well-being of the community at the aggregate level and the physical space occupied by people[2].

According to the Head of the Italian Delegation to the NATO Parliamentary Assembly, Andrea Manciulli, impressive changes regarding the type of security threats are occurring. At the macro-level, it is re-emerging a sort of "strategic confrontation"- in some cases even deterrence - between great powers. In addition, at a very micro-level new tensions such as cyber or hybrid threats, are changing the nature of confrontation. Overall, the current world presents an unconventional scenario, where smaller actors are able to threaten much bigger and stronger adversaries exploiting the asymmetry of the threat and the use of high-tech tools[3].

Manciulli's speech demonstrates how innovative and unpredictable current threats can be. Furthermore, considering the subjective nature of threats and the central role of the state, emphasized in the previous section, it is difficult to define which are these menaces. At the same time, it is impossible to face and defeat threats without targeting them. Thus, it is necessary to try to interpreter them retracing the most important phases in the history of global threats because - as the historian William Lund said - "we study the past to understand the present, and we understand the present to guide the future" (William Lund 1914).

The chapter will proceed targeting some of the most dangerous global menaces, assessing such a dangerousness through different factors, such as the speed of expansion, the extent of the damage, the effectiveness of the remedies and the capacity of response of each State.

[2] See Harman and Williams (2013:12)

[3] See Manciulli (2018: 15-16)

Traditionally, the most common and ancient threat is war, considered dangerous because of the extension of time, territory and physical harm inflicted to people. However, according to Stephen Walt (Stephen Walt 1991: 212) "the war in itself was ceasing to be the most serious global threat to human life", because new global challenges with worse effects are arising. As Miall (Miall *et al* 2005: p. 28) note, since the end of 20th century the number of inter-state wars has declined. Nevertheless, wars within a state's boundaries, the so-called intra-states wars, have increased after the Cold War, provoking a higher risk for the civil society rather than professional soldiers[4]. Overall, it is important to make a distinction between conventional war and unconventional one, which are not battles in the traditional sense and present innovative tools.

1.3.Conventional vs unconventional war

By definition, war is a period of fighting or conflict between countries or states. Since the end of the 20th century the confrontation between sovereign states has become rarer, leaving room to atypical armed conflicts. At this point, new words such as "new war" and "asymmetric war" gained popularity, appearing in various contexts, and the distinction between "conventional" and "unconventional" war arise[5].

"Conventional wars" are conflicts between regular armed forces of sovereign states. In such a situation, uniforms and clear lines of battle allow belligerents to identify one another and distinguish soldiers from civilians[6]. In the past, conventional wars have always been the only mean to protect national security, expand territories and gain power. This regular warfare can be defined by two major characteristics. Firstly, the military discipline that transformed wild bunches of warriors into effective instruments of political authority[7] and, secondly, the uninterrupted development of "repower", encouraged by the Western technological development and the end of the Renaissance and directly associated with the gradual adoption of linear tactics[8].

On the contrary, "unconventional war" is more problematic to define, due to the wide range of activities included in the definition and their complex interconnections. Basically, it easier to describe the features of an unconventional warfare rather than adopt a general definition. Indeed, this kind of war is characterized by the following "asymmetries", as described in the following table:

[4] See Harman and Williams (2013: 14)

[5] See Nagao (2011: 1)

[6] See Mockaitis (2017: 9)

[7] This change was concomitant with the birth of modern statehood as the sole legitimate provider and user of organized violence.

[8] It makes possible to combine rear with movement, thus giving birth to the modern idea of manoeuvre. This trend paved the way for the emergence of the idea of front and a rear, which is still today a central feature of our representation of war.

Asymmetries in **objectives**	Asymmetries in **time**	Asymmetries in **protagonists**	Asymmetries in **modus operandi**	Asymmetries in **space**
Less clear because less connected to the traditional paradigm of interstate war;	A “timeless” perception of such a war;	A variety of both state and non-state actors are involved;	An original mix of traditional and new weapons / tactics and because the distinction between combatants and non-combatants is eroded;	The distinction between “front” and “rear” or “war front” and “home front” disappears while the battle occurs everywhere simultaneously.

[Source: Marcuzzi 2018]

The aforementioned characteristics are coined by contemporary analysts also to define “asymmetric warfare”, “compound wars,” or “irregular wars”. Sometimes, these terms are included in the unconventional war spectrum, while on other occasion “unconventional war” is employed just to describe non-states actors against states whose armed forces they could never hope to defeat by conventional means[9].

The reason why traditional war has evolved towards an asymmetrical nature reside in the increasing role of people in armed conflicts. This resulted by massive social changes like the French Revolution and the birth of nationalism. Essentially, in the last century states declined as a form of sovereignty, sided by the international governance. Such a situation paved the way for more complex network of organized violence, including conventional forces, terrorist organizations, organized crime, so on and so forth. In addition, the distinction between war and peace faded away, to the point of facing today a “low-intensity endemic warfare” (Marcuzzi: 3).

As a result, the British General Rupert Smith wrote that “War no longer exists” (Smith 2005), referring to the end of traditional warfare, such as “battles in the field between men and machinery or war as a massive deciding event in a dispute in international affairs”. The last example of real field battle took place in the Golan Heights and in the Sinai desert in 1973 and then “new wars” replaced that henceforth. Subsequently, various types of combat broke the paradigm of interstate industrial warfare, namely that of “war amongst the people”,

[9] See Mockaitis (2017: 9-10)

where “all the people - anywhere - are the battle field”. (Ibid.) Partisan warfare was the herald of this relatively new form of warfare since the second World War and several decolonization conflicts were of the same nature[10].

Despite the novelty introduced by this new warfare, war has always been in a certain sense non-symmetrical. Indeed, 500 years BC the famous Chinese philosopher Sun Tzu said that war exploits different asymmetrical means of fighting in order to “avoid strength, strike weakness, and be unpredictable”[11]. In the 19th century this concept was resumed by Carl von Clausewitz. Currently, examples of asymmetrical means of fighting are guerrilla tactics, insurgency, revolutionary warfare and terrorism.

Guerrilla warfare can be employed by different actors for different purposes. At the beginning, it referred to the unconventional forces that harassed French troops in Spain during Napoleonic occupation. These ordinary Spanish peasants ambushed supply columns and small military units. They often wore no uniforms and melted back into the general population when confronted by superior conventional forces. Frustrated by their inability to identify these irregulars, French troops decided to retaliate entire Spanish communities, thus establishing a pattern of attack and reprisal that has characterized unconventional warfare to the present day. Those who operate in support of conventional forces or to resist foreign occupation are usually called “partisans” or “resistance” fighters. Resistance groups sprang up all over occupied Europe during World War II, although they varied greatly in competence and effectiveness[12].

On the contrary, “insurgency” is a sophisticated political movement to gain control of a country from within, in much the same way that a virus gains control of healthy cells. Insurgents develop a comprehensive strategy employing an information campaign to win support for their cause, guerrilla warfare to attack the police and military, and terror to frighten government supporters and to keep their own adherents in line. Because it requires a degree of education and political sophistication among the ordinary people, insurgency is a modern phenomenon. A spate of successful insurgencies took place during the period of decolonization following World War II. More recently, the United States and its allies have faced insurgencies in Iraq and Afghanistan[13].

Finally, terrorism generally refers to a movement by nonstate actors (an organization or network) to effect political or social change through the use of terror. A clear distinction must be made between “terror” and “terrorism.” “Terror” is a weapon or tactic employed by a variety of actors to achieve a result through frightening people. States have used terror for centuries, primarily to keep their own subjects peaceful and compliant. Instead, the term “terrorism” should be reserved for a campaign of violence that uses terror but has

[10] See Marcuzzi (2018: 2)
[11] See Marcuzzi (2018: 3)
[12] See Mockaitis (2017: 10)
[13] Ibid.

not risen to the level of insurgency.[14] It was precisely the terrorist attack on September 11th in the US that further changed the "war" paradigm, towards not only "asymmetrical" but also "hybrid" conflicts (Mockaitis 2017: 10). Hybrid conflicts are a new type of confrontation, which is dangerous because it can exploit the full spectrum of new threats as an asymmetric conflict but inscribed in the context of a conventional war. Hence, despite a clear distinction between conventional and unconventional war exists, throughout history these two types of operations have mixed and evolved towards the hybrid conflicts.

1.4. Hybrid conflicts

The concept of hybrid war emerged in the last few years, reflecting the new global awareness provoked by the 9/11 terrorist attack. Although the instruments employed in this hybrid context are surely new - due to the technological development - the logic behind them is a sort of Trojan Horse tactic[15]. By empirically examining recent example of hybrid conflicts, such as the military confrontation between Israel and Hezbollah in 2006 and the Russian intervention in Georgia in 2008, a more complete understanding of this phenomenon can be produced.

The Israeli-Hezbollah confrontation in Lebanon provided further stimulus to the debate about "hybrid wars". Throughout the war, Hezbollah displayed a complex and adaptive threat, created by the synergy between regular and irregular aspects. As a matter of fact, a lethal combination of conventional weaponry, such as anti-ship missiles, Kornet anti-tank missiles and Katyusha rockets, was employed with improvised weaponry and ambush attacks. Hezbollah fought many traditional battles, but also maintained an ability to disengage when it was advantageous, turning to terrorist attacks. In this way, Hezbollah won at the expense of the numerically, technologically and allegedly superior Israeli military. Moreover, such a victory was sustained by Hezbollah's exploitation of the media and a deceiving political result for the Israeli government[16].

In August 2008, the war between Georgia and Russia broke out. Along with the conventional conflict, Georgia experienced massive cyber-attacks against its government, banking services and media websites, which denied Georgian citizens and the international community important services and information from both sides about what was going on. The latter strategy evolved into General Valery Gerasimov's 2014 doctrine of "non-linear war", that inspired the following Russian actions in Ukraine. These examples show the Russian desire to employ all the available tools, both regular and irregular, to achieve politically decisive outcomes. It was in this occasion that US thinkers called such a "non-linear" war "hybrid war"[17]. From that moment, the term "hybrid war" is employed to describe the most frequent conflicts in the 21st century.

[14] Ibid.
[15] See Minuto Rizzo (2017: 117)
[16] Ibid.
[17] See Marcuzzi (2018: 3)

Following Thomas Huber and the British military theory, hybrid warfare was just an extension of compound warfare, which mixes regular and irregular force. Thus, hybrid warfare provides simply more advanced tools. Conversely, American scholars have argued that a hybrid threat is a dynamic combination of conventional, irregular, terrorist, and criminal capabilities adapting to counter traditional assets - meaning those held by the West. According to this definition, General George Casey, former Chief of State of the US Army, insisted that a key component of a hybrid threat is its "decentralization" - putting an emphasis on the fact that hybrid warfare is specifically meant at tackling Western opponents. As a result, there is a gap in common understanding between the US and its closest allies about this subject[18]. The conflicting interpretations about hybrid warfare generates confusion, expanded this concept over time. Today, the term "hybrid war" embracing any aspect of modern conflicts - including terrorism, economic warfare, mass migration, organized crime and so on - instead of being limited to a specific portion between irregular and conventional warfare. Another issue that arises with the definition of "hybrid war" is its effectiveness. The effectiveness of hybrid warfare depends on the specific logic of a situation and on the tools employed. In the case of Russia in Ukraine, hybrid warfare has been very effective operationally and tactically, but less strategically. That means Russia acts with military precision but failed to deter the West from assisting Ukraine or from imposing sanctions. Different was the case of DAESH. DAESH has been defeated operationally despite its tactical capabilities. However, it still poses a significant risk to the West, not just for the returning of foreign fighters, but because the borders in the Middle East have been radically questioned.

In conclusion, hybrid warfare is perceived by the West as very threatening due to the current spread of latent tensions and the unprecedented impact of intrusive technology. Since new technologies are growing increasingly cheap and available, there are positive consequences in terms of mass involvement and sometimes empowerment, but it also means to face an increased number of different channels of vulnerability. For instance, in a modern warfare a vastly-pervasive and manipulated media can influence the dynamic of the conflict. Through the cyberspace, it is also possible to inflict the greatest harm to opponents remaining anonymous, escaping the "attribution of responsibility". Moreover, by extending conventional war to include the people, hybrid forces amplify their otherwise limited power and extend the conflict both in time and space. Consider the absence of any laws prohibiting cybercrime in some countries or the complete lack of control over biological or chemical agents in others, the hybrid warfare can erode the modern notion of the state as the custodian of the monopoly of legitimate violence, impeding to provide security to the population[19]. Consequently, one common response to face "hybrid threats" is the so-called "resiliency". The term resilience appears for the first time during the North Atlantic Alliance's Summit of Warsaw in July 2016, along with the common "deterrence" (already introduced in the Cold War era). Resiliency affects the preparation of civil

[18] See Marcuzzi (2018: 7)

[19] See Marcuzzi (2018: 6)

society more than military measures, following the idea that a not-military menace requires non-military solutions. It consists in a reinforcement of the internal structure of a state - not only in term of physic and material resources but concerning the psychological and political aspect of populations. The key points of this strategy are well-informed and aware citizens. By this point of view, the European Union - which has not yet developed its proper Armed Forces - has the great opportunity to become a civil power and contribute to global security by developing new tools, such as diplomatic, economic and political - to face future challenges. After all, relying on the traditional (even if tested) instruments of reaction to the threat could prove to be not only ineffective, but even counterproductive[20].

To sum up, hybrid conflicts are dangerous because able to turn non-military tools into weapons, difficult to identify. Among these unconventional tools it is evident the role of the cyberspace. There are other relevant and less evident means that can be employed, such as the use of virus and micro-organisms to sow chaos and the damage of basic natural resources to weaken a population. These are all new terrible strategies which are based on the exploitation of the current global challenges. A turning point in the history towards these unconventional "weapons" was the discovery and evolution of the Weapons of Mass Destruction.

1.5.The proliferation of Weapons of Mass Destruction

The term "Weapons of Mass Destruction" (WMD) describes a specific category of armament associated with a new political and strategical issue. WMD are a controversial instrument which has signed the passage towards unconventional strategies. These weapons, defined as "any weapon capable of horrific human or material destruction. WMD may be nuclear, chemical, biological or radiological" (Miller C., 2005: 81), are "conventional" - even though more technological and dangerous than traditional ones - because appear as part of the traditional military armament. Nevertheless, WMD are not conventional because they are employed in a new strategical scenario. The most common and known tactic is "deterrence", defined as the threat to use nuclear weapons without their actual employment. In brief, a state owns and creates nuclear bombs to prevent a nuclear attack against itself. Thus, the final aim is not an actual war but discouraging enemy attacks. The reason behind this new strategy is due to the power of such an armament. Indeed, a real nuclear war can provoke the so-called MAD, the mutual assured destruction.

On the contrary, the use of biological/bacteriological and chemical weapons would lead to a different scenario. Such weapons are produced by scientists - as in the case of nuclear - but it is easier and cheaper to produce them. Hence, in the last few years criminal groups or individuals have been able to produce bio and chemical bombs with all their pervasive and terrible effects. Currently, biological/bacteriological and chemical weapons are used in hybrid scenario, representing one of the worst emerging threat worldwide. In this sense,

[20] See Minuto Rizzo (2017: 119)

all the WMD are “unconventional” or, at least, employed as non-traditional instruments in hybrid warfare. Despite the recent awareness about the concept of “hybrid war” and these weapons, cases of WMD employment have been already noticed in the 20th century.

The development of the weapons of mass destruction responded to the desire of overwhelming the enemy in the most conflictual phase of the world. As long as war remained confined to local dimensions, without the support of a strong technological research, the conflicts were limited to the use of “conventional weapons”. Conventional weapons were really effective in such a limited sphere and the evolution concerned only new tactics. For instance, the Roman commander Manius Aquillius poisoned the wells of besieged enemy cities in about 130 BC and Mongols used to throw dead corpses inside besieged cities, creating a sort of old-fashioned biological weapons. However, the term “Weapons of Mass Destruction” appeared for the first time in 1937, pronounced by the Archbishop of Canterbury, William Cosmo Gordon Lang, during a sermon. The Archbishop was referring to the carpet-bombing against the city of Guernica during the Spanish civil war, underlining the mass destructive potential of conventional weapons. Beyond the destructive potential of the carpet-bombing, at the beginning of the 20th century a chemical weapon had already been tested. It was asphyxiating gas, used during the First World War on the Western front. The appearance of these new weapons already occurred during a battle at the Belgian town of Ypres in 1915 by the German troops against the French positions. The attack of Ypres was the first time that weapons definable as "of mass destruction" were used on a large scale during a battle. Few years later, during the Second World War, the first large-scale use of biological weapons occurred, employed by Unit 731 of the Japanese army. This secret department aimed to test and verify the use of biological vectors and their effects, using different contamination systems - such as poisoning of wells and sprinkling via aerial - and testing the potential of products on prisoners and the civilian population. The activities of Unit 731 emerged at the end of the war and they are the first example of experimentation at a higher level of biological weapons.

The birth of nuclear weapons was very different. The potential of the atom was object of study since the end of the XIX century and, thanks to scientists like Enrico Fermi and Robert Oppenheimer ,the United States succeeded in developing the first atomic bomb. The so-called “Manhattan Project" achieved in a few years a war application of atomic power, which put an end to the Second World War. The American nuclear attack against the two Japanese cities of Hiroshima and Nagasaki in 1945 was a dramatic event which would have influence the global scenario in the following years. As a consequence, this new threat posed by the US led the USSR to develop a nuclear bomb in turn, to counterbalance the power of the Atlantic bloc. By the end of 1949 the Soviets were able to set up their own nuclear weapons, compensating the lack of technology and Russian delay with spying operations against the Americans. Thus, the Cold War era has been marked by a “nuclear balance” and in the meanwhile new unconventional means arose, such as spying operations to carry on the technological competition and the information war. Moreover, nuclear weapons did not limit their presence in Russian and American arsenals, but they were developed by France, the United Kingdom, China, North Korea, Pakistan, India and Israel, aggravated tensions worldwide. The world was and is still burdened by the presence of such an apocalyptic weapon.

The other WMD appeared more sporadically during the Cold War, however there were cases in which they were used in some conflicts, such as in the Iran-Iraq war, or in disturbing accidents, as in the case of Sverdlovsk. Despite these sporadic examples, the post-bipolar world saw a more active presence of chemical and biological weapons, as in the case of asphyxiating gases or bacteriological attacks carried on by infra-state articulations, sometimes identifiable as terrorists. These attacks took place in areas with a very high urban density and demonstrate how dangerous the use of such instruments in our societies can still be. Dealing with a fragile geopolitical scenario and a wide range of weapons of mass destruction, led to sign various international conventions that regulate the subject. Nonetheless, it cannot be excluded that any fanatic groups or organization may use chemical, biological or radiological elements. Indeed, the aforementioned armament can be employed in unconventional conflict to favour weak non-states actors against sovereign states.

Taking everything into account, these threats has been the first to require a comprehensive approach connected the institutions that deal with security, like the Armed Forces, and the subjects that - internally or abroad - monitor the activities of extremist, fundamentalist groups and international terrorists. Furthermore, the vulnerabilities of important international treaties and some regional crises constantly threaten the process of reducing or at least containing the proliferation of weapons of mass destruction[21]. As this historical excursus pointed out, during the Cold War the United States and the Soviet Union conceived the idea of maintaining the bipolar conflict within the threshold of nuclear deterrence, turning a potential war into “a limited war”. In the meanwhile, actual wars did occur in the Middle East and between India and Pakistan and several latent tensions exploded at the end of the bipolar confrontation. In those conflicts, the trinity given by the combination of government, a state’s armed forces and the nation as formalized by Clausewitz did not exist. There is no longer an effective government that centrally governed the country, and there were mere armed groups, not state’s armed forces. There was no nation as a political concept, and there were only people driven by passion and hatred.

Finally, the shocking terrorist attack on 9/11 occurred and the U.S. armed forces with its allies mounted an attack against the Taliban. This was the true beginning of an era of fear, insecurity and instability. Currently, unconventional struggles prevail worldwide, fought no more in the inter-states’ context but as a form of asymmetric war between a state and a non-state actor. In this scenario global threats not only emerge but are exploited by both, states and malicious actors.

[21] See Felician (2010: 5-8)

Chapter 2. The new frontier of the "emerging threats"

Nowadays, it is enough to open a newspaper or turn on the TV to understand what kind of challenges our world is facing. For instance, the planet is suffering more and more the effects of climate change, which are more and more evident and worsened by the reckless behaviour of human beings. This year has been remarkable in that sense, especially thanks to activists like Greta Thunberg, who have heavily debated about the alarming condition of global warming.

Moreover, hybrid threats stemming from terrorism and criminal networks are becoming more dangerous than before, exploiting high-tech knowledge and improved weapons. Along with this, scientific research - usually used to heal from diseases - can now be employed to build bio-weapons, making the risk of bioterrorism more real than ever.

In the meanwhile, beyond the physical space, the cyber-space is turn into a place for the proliferation of criminal activities and cyber-attacks are is targeting more frequently politicians, celebrities as well as common people.

2.1. Climate Change issues

Three decades ago, when serious debate on human-induced climate change began at the global level, a great deal of statesmanship was on display. There was a preparedness to recognize that this was an issue that transcended nation states, ideologies and political parties which had to be addressed proactively in the long-term interests of humanity as a whole. This was the case, even though the existential nature of the risk was less clear than today[22].

Global institutions such as the United Nations Framework Convention on Climate Change (UNFCCC) - established at the Rio Earth Summit in 1992 - were developed to take up this challenge and change the fossil-fuel-dominated world order. As a consequence, despite the diplomatic triumph of the 2015 Paris Agreement, the debate around climate change policy has never been more dysfunctional[23]. Indeed, international agreements talk of limiting global warming to 1.5-2 degrees Celsius (°C), setting in the meantime the world on a path of 3-5°C of warming. Only 1°C more of warming is dangerous, but this cannot be admitted, and the planetary future is hostage of myopic national self-interest. Action is delayed on the assumption that unproven technologies will save the situation, but actually the risk remains[24].

[22] See Spratt and Dunlop (2018: 4)

[23] Ibid.

[24] See Spratt and Dunlop (2018: 4)

In 2017, the scientists Xu and Ramanathan illustrated a potential 2050 scenario, taking into account the effect of climate change. That was an original way of thinking about the potential impacts of global warming, not imposing a sure scientific projection of what will occur but searching to raise awareness about the topic. The project was divided in three phases: the first one between 2020-2030, the second between 2030-2050 and finally the 2050 outcomes[25].

According to the scientists, between 2020–2030 the warming would lock at 1.6 °C and the failure of a global, climate-emergency mobilization of labour and resources to build a zero-emission economy and carbon drawdown would lead global greenhouse emissions to peak ten years before Paris Agreement’s predictions. Moreover, carbon dioxide levels would have reached 437 parts per million by 2030, which is would be an unprecedented in the last 20 million years[26]. Then - in the second phase - a consistent reduction in fossil-fuel energy intensity would occur, leading a warming of 2.4°C by 2050 plus another 0.6°C, due to the activation of a number of carbon-cycle feedbacks, such as a reduction of the uptake and storage of carbon by land and ocean sinks, a higher levels of ice albedo and several cloud feedbacks. At this point, the warming would reach the total of 3°C by 2050. Despite this dramatic result, such predictions are far from an extreme scenario, because the low-probability (5% of probability), high-impact warming can exceed 3.5 - 4°C by 2050[27].

Finally, sea levels would rise 0.5 metres by 2050 and 2 - 3 metres by 2100. Overall, thirty-five percent of the global land area, and fifty-five percent of the global population would be subjected to more than twenty days a year of lethal heat conditions, beyond the threshold of human survivability. The jet stream would be destabilized, affecting the intensity and geographical distribution of the Asian and West African monsoons and, together with the further slowing of the Gulf Stream, impinging on life support systems in Europe. North America would suffer from devastating weather extremes including wildfires, heatwaves, drought and inundation. The summer monsoons in China would fail, and water flows into the great rivers of Asia would be severely reduced by the loss of more than one-third of the Himalayan ice sheet. Glacial loss would reach seventy percent in the Andes, and rainfall in Mexico and central America falls by half. Aridification would emerge over more than thirty percent of the world’s land surface, severe in Southern Africa, the Southern Mediterranean, West Asia, the Middle East, inland Australia and across the South-Western United States. As a result, several ecosystems would collapse, including coral reef systems, the Amazon rainforest and the Arctic. Nations and regions characterized by the impossibility to provide artificially-cooled environments for their populations would become unviable. Water availability would decrease sharply in the most affected regions at lower latitudes, such as dry tropics and subtropics, affecting about two billion people worldwide and making agriculture impracticable. A significant drop in food production and increasing numbers of

[25] See Xu and Ramanathan (2017)
[26] Ibid.
[27] Ibid.

extreme weather events would occur, including heat waves, floods and storms. As a consequence of the decline in crop yields and in the nutrition content of food crops would be inadequate to feed the global population and food prices will skyrocket[28].

Therefore, these conditions would contribute to the displacement of billions of people. In practice, some of the world's most populous cities - including Chennai, Mumbai, Jakarta, Guangzhou, Tianjin, Hong Kong, Ho Chi Minh City, Shanghai, Lagos, Bangkok and Manila - would be abandoned, not to mentioned that the ten percent of Bangladesh would be inundated. In this scenario, nations around the world would be overwhelmed by the scale of change and pernicious challenges, such as pandemic disease. The internal cohesion of nations would be under great stress, both as a result of a dramatic rise in migration and changes in agricultural patterns and water availability. The flooding of coastal communities around the world, especially in the Netherlands, the United States, South Asia, and China, has the potential to challenge regional and even national identities. Violent struggles between nations over resources would explode, such as for the Nile and its tributaries, and a nuclear war is possible. The social consequences range from increased religious fervour to outright chaos. Into a world of outright chaos, political panic becomes the norm and the end of human civilization becomes closer[29].

Such a catastrophic future scenario demonstrates that climate change is the worsen emerging threats, because imply several other issues, like the lack of resources and migration flows and, as ultimate effect, the permanent and drastic destruction of human beings. Thus, global warming is defined as the greatest threat to human life on the planet, which can be compared only to a nuclear war[30]. However, nuclear war lethal effects are not underestimated and controlling systems and economic interests discourages to any possible nuclear actions. On the contrary, climate change is underestimated because its effects are less evident, not immediate and can affect negatively economic interests. Nonetheless, at the end the result would be the same.

In spite of all, climate change is not inevitable and a new approach to climate-related security and risk-management can be adopt. These menaces can be avoided and reduced building a zero-emissions industrial system very quickly, which is possible only with a global mobilization of resources on an emergency basis and a common understanding of the phenomenon. Moreover, it is important to grasp the strengths and limitations of scientists' projections. Indeed, a 2013 study by Prof. Naomi Oreskes and fellow researchers examined a number of past predictions made by climate scientists. They found out that scientists have been "conservative in their projections of the impacts of climate change" and that "at least some of the key attributes of global warming from increased atmospheric greenhouse gases have been under-predicted, particularly in IPCC assessments of the physical science" (Oreskes, Brysse, O'Reilly and Oppenheimer 2013: 327-337).

[28] See Xu and Ramanathan (2017: 315-323)

[29] Ibid.

[30] See Spratt and Dunlop (2019: 3)

They concluded that climate scientists are not biased toward alarmism but rather the reverse of "erring on the side of least drama, whose causes may include adherence to the scientific norms of restraint, objectivity, scepticism, rationality, dispassion, and moderation" (Ibid.). This may cause scientists "to underpredict or downplay future climate changes" (Ibid.). In this sense, there was a first realization in 2007, when security analysts claimed that scientific predictions in the climate-change arena had been under-estimated in the two previous decades. During the Intergovernmental Panel on Climate Change (IPCC) the problem persists, presenting assessment reports on general climate models, which do not include all of the processes that can contribute to system feedbacks, compound extreme events, and abrupt and/or irreversible changes. For instance, the IPCC's Fifth Assessment Report in 2014 projected a sea-level rise of 0.55-0.82 metre by 2100, adding that "levels above the likely range cannot be evaluated". Recently, another IPCC's report projected that global warming would rise at the current rate of ~ 0.2°C per decade, reaching the 1.5°C mark around 2040[31]. Nevertheless, the acceleration of anthropogenic emissions, the decrease of aerosol loading, and the change of ocean circulation conditions have currently changed the previous predictions, and the 2°C boundary will be passed in 2045. Currently, the global warming is estimated at 3°C or more by 2100, considering the commitments by nations to the 2015 Paris Agreement. Such a value was categorized in 2017 as "catastrophic" (Xu and Ramanathan 2017) and "beyond adaptation" (Spratt and Dunlop 2018).

The Global Challenges Foundation (GCF) explains that if climate change was to reach 3°C, most of Bangladesh and Florida would drown, while major coastal cities - Shanghai, Lagos, Mumbai - would be swamped, likely creating large owes of climate refugees. Most regions in the world would see a significant drop in food production and increasing numbers of extreme weather events, whether heat waves, foods or storms. This likely scenario for a 3°C rise does not take into account the considerable risk that self-reinforcing feedback loops set in when a certain threshold, the so-called "tipping-point" (Schellnhuber 2018), is reached, leading to an ever-increasing rise in temperature. Potential tipping-points include the melting of the Arctic permafrost releasing methane into the atmosphere, forest dieback releasing the carbon currently stored in the Amazon and boreal forests, or the melting of polar ice caps that would no longer reflect away light and heat from the sun.[32] Moreover, reports should underline that the intersection between climate change and other pre-existing national security risks can provoke the multiplication of threats and accelerate global instability, contributing to escalating cycles of humanitarian and socio-political crises, conflict and forced migration[33]. For example, nowadays such a situation is showing across the Middle East, the Maghreb and the Sahel with social breakdown and conflicts, which contribute to the European migration crisis. According to the Emeritus Director of the Potsdam Institute, Prof. Hans Joachim Schellnhuber, "climate change is now reaching the end-

[31] See Spratt and Dunlop (2019: 5)

[32] See Global Challenges Foundation (2017)

[33] See Spratt and Dunlop (2019: 4)

game, where very soon humanity must choose between taking unprecedented action or accepting that it has been left too late and bear the consequences". (Schellnhuber 2018: 3).

To sum up, analysis of climate-related security threats in an era of existential risk must have a clear focus on these extremely serious outcomes that fall outside the human experience of the last thousand years, that are higher than is generally understood. Traditionally, risk is assessed as the product of probability and damage. Nonetheless, when the damage is beyond quantification, this process breaks down. A peculiarity of existential risks is the impossibility to learn from mistakes, without a concrete possibility to rely on the institutions, moral norms, or social attitudes developed from experience. An approach different from traditional practice will focus on the high-end, unprecedented possibilities, instead of assessing middle-of-the-road probabilities on the basis of historic analogue. Thus, a tough, objective look at the real risks - especially at those threaten the survival of human civilization - is a prudent risk-management.

The first step is a normative view of the targets, based on the latest science within a qualitative, moral framework, to avoid catastrophic consequences. Then, action is determined by the imperative to achieve the target. It requires a policy that is integrated across national, regional and global boundaries, and which recognizes that issues such as climate, energy, the ecological crisis and resources overuse are inextricable[34].

Theoretically speaking, reducing this risk and protect human civilization means to carry on a massive global mobilization of resources in the coming decade to build a zero-emissions industrial system and set in train the restoration of a safe climate. Actually, research into climate change impacts and adaptation is particularly complex due to many uncertainties surrounding the various ecosystems' responses, as well as the difficulty associated with contextualizing the heterogeneity in impacts and adaptive capacity (Kreigler *et al.* 2012). In many parts of the world there has been very limited funding available especially where there has been a history of skepticism regarding the scope and magnitude of the predicted outcomes. Despite the limits of research, it is generally acknowledged that the key to mitigating the potential effects lies in a country or a population's adaptive capacity. Many developed countries appear to have refocused their priorities and rather than trying to reduce greenhouse emissions and slow the potential effects, they are instead investing in researching adaptation strategies to reduce adverse consequences. Given that these strategies require significant financial investment, it follows that developing nations - who have extremely limited finances and therefore a limited capacity to adapt - will be impacted more severely. Many of these countries already have high rates of disease and debility and are less able to cope successfully with stresses of all kinds, including the environmental and social impacts of climate change (NCCARF and WHO 2013).

Beyond the difficulties and the heterogeneity of climate change effects, the actual enemy is the massive inertia of global leaders. According to the researchers David Spratt, Director for Breakthrough National Centre

[34] See Spratt and Dunlop (2019: 7)

for Climate Restoration, and Ian T. Dunlop, a former international oil, gas and coal industry executive, at the social level lies a certain reluctance because the priority is given to short-term economic considerations. Thus, the priority has been ensuring that the emissions-reduction paths developed for policymakers would not be economically disruptive. Actually, rapid reduction of carbon emissions is still excluded by policymakers, deeming that it will be too economically dislocating, and discussion around policy choices gives primary emphasis to the role of markets. Global leaders have accepted the continuing expansion of fossil fuels in the first half of the 21st century, trying to counteract their climate impact with a massive expansion of carbon capture and storage to draw down excess carbon from the atmosphere.

The final result - after three decades of global inaction - is climate change as an existential threat, which implies large negative consequences, such as reductions in global and national population, mass species extinction, economic disruption and social chaos. The risk is immediate, extended and nourished by the use of fossil fuels[35].

2.2. The rise of biological warfare

Beyond the physical harm that can be inflicted to the population and its resources by the effects of climate change, the action of certain viruses or microorganisms can imperceptibly have the same effects. This well-known fact is defined as biological threat. Its origins were noble, based on intense studies which aimed to eradicate diseases that had afflicted the human beings for centuries, such as scourges. Nevertheless, the research led soon to discover how the presence of pathogenic viruses and microorganism can reduce people possibilities of working in short or long term and, in certain cases, lead directly to death. Such a finding led to deliberately infect or attack people with these viruses or micro-organisms to create an advanced tool of warfare. Humans can be affected by bio-weapons directly or indirectly. Indeed, pathogenic entities are able not only to target people, but also animals and plants. For instance, virus and bacteria can kill animals, destroy crops and the contaminate water, undermining humans' livelihood, weakening enemy resistance and forcing the opponent to surrender.

According to the Commission on Weapons of Mass Destruction, biological weapons and toxins "kill by using pathogens to attack cells and organs in human bodies, although they can also be used to target crops and livestock on a massive scale. Some are contagious and can spread rapidly in a population, while others, including anthrax and ricin, infect and kill only those who are directly exposed" (WMD Commission 2006: 32). The US Department of Defence defined the biological warfare as "the employment of biological agents to produce causalities in personnel or animals, or damage to plants or materiel; or defence against such employment" (Department of defence 2001: 67) and biological weapons as "an item of materiel which

[35] See Spratt and Dunlop (2018: 39)

projects, disperses or disseminates a biological agent including anthropoid vectors” (Ibid.) .

The recent international rejection of using biological weapons - not yet accepted by the international community as a whole - occurred after centuries of pathogenic virus and micro-organisms employment, such as the harmfulness of corpses used to contaminate the aquifers of the enemy. The first “biological” attack occurred in 1347, when the Tartar troops launched corpses of plague victims into the Genoese port of Caffa. Such an event is considered as the starting point of the “Black Plague” terrible spread, the most devastating epidemic in history. Then, diseases began to spread among the indigenous population because of Spanish Conquistadores arrival in the New World and similar case occurred among the Maori populations in Australia, infected by syphilis after going with some prostitutes. Despite the lethal consequences of these type of attacks, these were not example of biological weapons systematic use. Indeed, in the aforementioned cases the deliberate use of disease-causing agents in warfare was a marginal event in the course of a conflict and a systematic approach require a true understanding of the nature of the disease itself. Hutchinson claimed that the scientific advances of nineteenth and twentieth centuries turned the biological weapons into the most terrifying of all weapons of mass destruction. Despite biological weapons remained on the agenda of many governments, during the first decades of the last century the scientific interest was more towards chemical weapons. The 1925 Geneva Protocol prohibited the use of “asphyxiating, poisonous or bacteriological” weapons, but it did not prohibit the research and accumulation of these substances and, in addition, biological war is often associated with chemical warfare. Nonetheless, bio-threat is actually more dangerous and insidious than chemical one, because chemical agents are not able to expand beyond the attacked area - or at least remain less concentrated losing their lethality – while a virus that affects a person, can infect the others distant with the same danger. Moreover, the incubation of the disease can make an affected person appears healthy, contributing to spread sneakily the pathology.

Generally speaking, the dangerousness of biological weapons depends on the type of agents involved, which are basically five:

Virus	**Bacteria**	**Microorganisms**	**Mushrooms**	**Toxins**
Microorganism compose of a piece of genetic material, like *Rna* or *Dna,* surrounded by a protein coat .	Any of a vast and ubiquitous group of prokaryotic microorganisms that exist as single cells, in clusters or single cells' aggregates.	A living thing that on its own is too small to be seen without a micro-scope.	Non-motile, non-photosynthetic and chiefly multicellular organisms that adsorb nutrients from dead or living organisms.	Any various specific poisonous substances that are formed biologically. The term is sometimes extended to include synthetic poisonous substances.
Smallpox, Ebola or Venezuelan equine *encephalitis.*	*Bacillus antracis*, *Yersinia pestis* that causes bubonic plague or *Francisella tularensis* which causes tularemia.	*Rickettsiae*, that cause Q fever and typhoid.	*Aspergillusfungi.*	*Botulinum, ricin* and *saxitoxin,* produced by microorganisms, plants or animals.

[Sources: Kelle 2007 and Hutchinson 2003]

All of these substances have different characteristics and can affect human beings with diversified modalities and effects. Some of the agents indicated can also hit animals or be capable of affecting crops. If these substances are employed for military purposes, their dangerousness is very high, because they can be spread easily, resist to temperature, atmospheric agents, antibiotics and drugs, adapt in different vectors (bombs, artillery shells, missiles), have small size and cheap cost of production. Moreover, when the agent infects a human being it can kill or debilitate him for a long time. Fortunately, these features as a whole are not combined in a single agent. Nonetheless, it should not be forgotten that "modern bioengineering techniques can be used to enhance existing biological agents and make them ideal biological weapons" (Croddy 2002:

194) to achieve all the aforementioned biological characteristics. Then, the biological agent can be spread through a vector, which is a tool to transport the pathogen from the attacker to the target. The choice of vectors is influenced by technological developments and the nature of pathogen because - in order to process biological agents into a viable weapon - a producer must make them capable of surviving storage and dissemination. In fact, some agents like viruses have the advantage to be replicated and spread, making the possibility of contagion by air available. In this case, scholars have shown that specific technologies would not be needed, because it is enough to release the virus in areas of great concentration and passage of people, such as the subway or a mall. Besides a person-to-person contagion, biological agents can be dispersed in many ways. For example, it can be inserted inside a cavity of artillery shells, bombs, missiles or rockets and, at the moment of the shot, be released, acting like a chemical weapon. In addition, biological weapons can act through insects or animals and contaminate the water and crops, damaging the production chains of human food. In such dramatic cases, the presence of health checks on food chains and efficient sterilization mechanisms can prevent or neutralize the attack. The agent can also be sprinkled with airplanes or sprayers, but the person-to-person contagion in crowded places remains the most efficient mechanism. The targeting area depends also on weather condition, because bacteria and viruses can resist and diffuse only in optimal conditions, such as mild temperatures, little or no UV, low wind and no rain. These are the reason why, biological attacks are frequently released through foods, as in Oregon in 1984, or through the postal system, as in Washington in 2001[36].

The American Centres for Disease Control (CDC) have divided biological agents into three categories of dangerousness, based on the ease of dissemination and the severity of the effects they cause:

Category A (the most dangerous agents and toxins):

- They are easily transmitted from person to person;
- They are capable of producing a high incidence of mortality and have a great impact on health;
- They can cause panic in the population;
- Require special actions for the health system.

Category B:

- They are fairly easy to spread
- They give rise to diseases of medium intensity and low levels of mortality;
- Require specific improvements of the CDC laboratories and careful control of the disease.

Category C:

- Include the possibility of new pathogens created for a mass diffusion;

[36] See Felician (2010: 42)

- They are easily available;
- They are easily produced and disseminated;
- They have the potential of high morbidity and mortality incidence, and relevant health effects.

B category agents, despite a considerable complexity, are the virus and bacteria exploited by terrorist groups to sow chaos, actions which take the denomination of "Bioterrorism". The term "bioterrorism" refers to the threat of attacks with biological agents by terrorists. The American government defines a bioterrorist attack as "the deliberate release of viruses, bacteria or other germs (agents) used to causes illness or death in people, animals or plants". The biological terrorism has several implications that go beyond the pathological fact alone, in itself already serious. Without hypothesizing an apocalyptic scenario and relying only on the data of actual attacks, a biological strike sows panic and fear. Fear because the enemy is not known, not seen and there is the possibility of contagion. The risk of contagion leads to put under pressure pharmacies and health facilities, where hundreds of people ask for information or complain about real or presumed symptoms. Thus, the first consequence is the entire or partial collapse of the health system, namely filled hospitals, neglected hygiene rules to accommodate the whole of patients and lack of staff. It can be just the result of alarmism, but a significant delay in treatment can actually lead to death. Subsequently, deaths further increase fear and people move away the affected area, generating abnormal traffic volumes, slowing down the transport system, and may helping spread the agent. A great spread of the disease would paralyze economy, public and private services, provoking difficulties for the communities and significant economic costs. There would be an inevitable decline in tourism and difficulties of bringing basic necessities, that would become scarce in short time. In all this calculation should not be forgotten a progressive increase in deaths, due to lack of drugs, health facilities or an excessive time for the identification of the disease. In the meantime, more complicated and unpredictable events can still occur. In such a dramatic context, winners are those who perpetrated the attack, namely terrorist groups, which would see its purpose to spread chaos perfectly fulfilled. This is the reason why it is more realistic to imagine an attack with biological weapons perpetrated by terrorist organizations than by conventional military forces. Indeed, insidiousness and fear of contagion are excellent allies for those seeking to pursue destabilization projects rather than immediate tactical results[37].

From a legal perspective, treaties concerning biological weapons have not an international and bilateral formation as vast as those of other WMD. Indeed, biological weapons were initially assimilated to chemical weapons - although they had not been employed during the First World War - and included in the 1925 Geneva Protocol for banning the use of chemical substances in warfare. At the end of the 1960s, President Nixon decided to unilaterally destroy the important American biological arsenal, facilitating the international initiative to conclude a comprehensive agreement concerning biological weapons. This realization led to the

[37] See Felician (2010: 42-44)

conclusion of the Biological Weapons Convention in 1972. This convention is an international treaty whose full name is “Convention on the Prohibition of Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction”, also known as BWC or BTWC. It was signed in 1972 and entered into force in 1975[38].

The Convention consists of a preamble and fifteen articles. The preamble begins with a reference to the will to complete disarmament, with the conviction that this can be achieved through the prohibition of “development, production and stockpiling” of chemical and biological weapons, and through their elimination. The text as a whole and the preamble of the Convention do not cite the actual utilization of biological weapons[39]. The reason behind this apparent gap is given precisely by the setting that was attributed to the BTWC, which did not want to eliminate the provision of the 1925 Protocol or renew it with another guise, just integrate a series of further limits. The prohibition eliminated at least theoretically biological weapons from the military instruments. Actually, the analysis that the doctrine about BTWC reveals several points that weaken this Convention. For instance, the BTWC has not created any international control structure, as owned by the other categories of weapons of mass destruction. Indeed, nuclear energy has the IAEA and the Chemical Weapons Convention created the OPCW. Another weakness is the lack of control and verification systems, which means there is only the possibility of denouncing the defaulting state. Then, there is the delicate issue of a series of failed ratifications and failed signing of the treaty, since many of the states that have signed the treaty have not ratified it, and many others have not even signed the treaty[40].

In conclusion, the danger of bioterrorism persists nowadays, and the situation has been further aggravated by the devolution in the life sciences[41]. In addition, the problem of biological weapons is underestimated by the international community and it remains fragile if compared to other weapons of mass destruction’s perception. All of this makes the biological threats a perfect tool to employ in the hybrid conflicts.

2.3. Digital threats: a war without limits

In the previous section, biological agents are defined as global threats against humanity because can be exploited in hybrid conflicts and can affect the world as a whole.

As climate change, biological weapons act in the physical world, inducing damaging effects on people health. Nevertheless, beyond the Earth space exists a most dangerous zone called cyber-space. The cyber-space is born with the development of internet and it is currently hosting several new digital threats. The rise

[38] See Chambers (1999: 113)

[39] Find the text on http://www.opbw.org/

[40] See Felician (2010: 109-110)

[41] See Centre for Biological Threats and Special Pathogens (ZBS)

of new digital threats results from the transformation of the cyber space in a place of strategic competition. This strategic competition depends on the internet main features, namely the low-cost accessibility and its pervasiveness, which create an area of absolute chaos and permit to hide criminal networks. Thus, it is an ideal place for the proliferation of old and new weapons, with whom intelligence operators are currently obliged to deal with to maintain national security[42].

Despite the novelty of the cyber-phenomenon, technology has always been a tool for the consolidation of global geopolitical hierarchies. Throughout history, nation states have exploited technological development to sophisticate its armaments, gaining advantages upon the others. Today, modern technology - which is linked to a wide range of networks and present low acquisition and usage costs - is favouring geopolitical decentralization through the virtual universalization of the power. Basically, a revolution has been occurring since 1989, the year of the debut of Internet. In 1993, only fifty sites were registered on internet around the world, but there was already present the dangerousness of a potential cyber-war. The "cyber-war" was defined as an extension of the intelligence war during the Cold War, when numerous computer engineers were employed to gain sensitive data and information. These engineers maintained their expertise in the post-Cold War era, selling their skills and becoming mercenaries devoted to cyber war, especially in the former Soviet bloc. By the end of 90's, the international community became completely aware of this phenomenon and tried to rule these new threats. The first result was the Wassenaar Arrangement, signed in 1996, which is still in force and has been strengthened in 2014. This arrangement is focused on the dual use of technology, in both civilian and military sector, referring on nuclear and computer software, offensive or defensive tools, used for the state security.

In 1998, Russia was the first to present in the UN Assembly a project to disarm the cyber space by limiting infrastructures. This idea was based on the model of disarmament agreement between the USSR and the United States after the Cold War. Finally, the United States - scared by the possibility to lose their technological advantage - rejected the project. In 2004, a Group of Governmental Experts on Cybersecurity was set up by the UN, following the model of the climate, to define properly such cyber conflicts in the contemporary world and learn to rule it. Since 2004, the group has published several texts. In 2013, international law was also validated and applied in the cyber space and after two years, in 2015, the group of experts produced a code of good conduct in the cyber zone.[43]

As mentioned before, the Wassenaar Arrangement has been reinforced in 2014, advocating strict contracts and controls. For instance, it imposes an imperative ban on the export of dangerous software. Today, there are 42 signatory countries, such as the whole of Western Europe, Russia and the United States.

[42] See Ansalone (2012: 37)

[43] See IFRI Politique Etrangère (2018)

Nevertheless, China, Brazil and India - where came from the majority of engineers - refused[44].

Besides these attempts, the cyberspace is still an unknown and unverifiable place, because its own nature impedes a perfect regulation. Such a nature is based on a paradox: on one hand, a cyber war demands the technological mastery - currently owned by the United States - which is the cornerstone to dominate cyberspace; on the other hand, despite the technical supremacy, a basic cyber knowledge it is enough to allow individuals to trigger a cyber-attack. Hence, it is evident that such a huge revolution has its pro and cons. The cost resides in the proliferation of transnational criminal networks, hackers, terrorists and the manipulation of digital capability carried on by governments or companies against their competitors. Such a collision of interests could lead to a real war fought via internet. Indeed, countries like Russia, Israel, Iran or North Korea are already able to deploy "cyber armies" to perpetrate asymmetric attacks, sabotage communications networks and hit critical national infrastructures.

In brief, economists, analysts, security operators and governors will have to deal with a more and more virtual and obscure reality in the matter of politics and economy. Nevertheless, the cyber space is not completely unknown, and three considerations can be made[45].

Firstly, the cyber-space is living a constant evolution, because its pervasiveness runs hand in hand with the development of IT infrastructures and the expansion of political, commercial and economic relations between States.

Secondly, vulnerabilities are generated when interdependence is not governed. In this term - along with the regulation of the traditional domains of sky, sea, land and space - the cyber space can be ruled and used as a strategic tool, exploiting the cyber power in peace as in war, in offense as in defence.

Lastly, even though the cyberspace can be presented as the last evolution of the technological path - started with the printing press, the telegraph, the telephone until the wireless communication - it is not just a communication tool but an instrument to create, accumulate and manipulate information.

Taking everything into account, the cyber power is tactically and technically distinct from the other tools of military power and it broadens the spectrum of strategic actors and vulnerabilities[46].

The main actors involved in the cyber space are pointed out in the following table:

[44] See Wassenaar Agreement (2014)

[45] See Ansalone (2012: 39)

[46] Ibid.

States	**Digital giants**	**Cyber security start-up**	**“Hacktivists”**	**Groups linked to criminal networks**
Overall, 6 states are currently responsible for 90% of cyber-attacks. These states are the USA, Russia, China, Israel, Iran and North Korea.	The digital giants can play a double role in the cyber war: they are the main victims of computer attacks but, at the same time, they can rule this digital war. An emblematical case it is the use of Facebook by Russians to influence the election campaign and broadcast fake news.	These start-ups are all the companies that develop software and sell it to states or to other actors. Sometime, there is an obscure relationship between them and the public authorities.	The term “hacktivists” came from the hacking ability of certain individuals that act as activists, such as the famous group “Anonymous”.	These are cyber engineers employed by criminal group, which act for a matter of money.

[Source: IFRI Politique Etrangère 2018]

That large number of actors involved is the first vulnerabilities of the cyber space, which provokes problems in term of accountability. Indeed, in this crowded scenario is difficult to identify who is actually behind the attack, making the principle of self-defence and retaliation - the two paramount principles of war rules - very fragile and precarious.

The situation is aggravated by the relationship between cyber actors, especially state services and private agencies. Indeed, there are cases of collusion between the government and private group, which are employed by the state in itself to avoid international repercussions. For example, in September 2016 the World Anti-Doping Agency suffered from a Russian cyber-attack, perpetrated by a private group. The event occurred after the exclusion of some Russian athletes, which resulted positive to the anti-doping test. Thus, it was high probable a conspiracy between such a group and the Russian government. Moreover, the attack revealed that the agency had allowed the participation of American athletes, despite positive anti-doping tests. The Russian government denied any involvement or responsibility and no evidence was found, but the situation remains uncertain.

A more evident case of collusion linked the French government with cyber companies, start-ups like VPN - specialized in the discovery of computer flaws in the system of global giants - and the French company *Amesys*, which developed and sold to Gaddafi a program to infiltrate in the digital devices of Libyan citizens. In this last case, the International Federation of Human Rights accused France of complicity in crimes of torture and political repression. Despite the French authorities broke the bonds with *Amesys*, problem of image and judicial issue remained. Indeed, France has continued to use some programs of *Amesys*, arising problems of intellectual property and security[47].

These links highlight that the ambiguity of cyber actors can have severe repercussions in the moral, legal and security sector. In this sense, important summits have been established to deal with this new threat and its implications, like the Munich Security Conference in 2017. During this meeting, the states involved clarify the modus operandi and the ultimate goal of a cyber-attack, which is to weaken a country destabilizing the international scenario by creating uncertainty. Such an uncertainty can be produced thanks to the diversity of the cyber-threats. The diversity of these offensive threats depends on the weapons available, who can be divided in three main categories: Denial of Service attacks (DoS), cyber-espionage and attacks perpetrate through blackmail with Ransom System[48].

First of all, the term "Denial of Service attacks" is used to describe attacks against sensitive infrastructure, impeding them to work properly. It is a sort of remote sabotage, which can be done with different tactics, for instance through a blackout. Such a strategy is applied in classic interstate relations, perpetrated by a country against another using a wide range of tools. Usually, three sectors are hit by these attacks: energy infrastructure, such as in 2012 against the Arabic oil company *Arabecom* (to paralyze energy resources for three days and raise prices around the world); telecommunication, such as the blocking of *Tele5monde* in 2015 (to pass propaganda messages); and financial organization, such as the attack against the US bank Jimmy Morgan in 2014 (to stealing data).

Overall, the first-ever cyber-attack was a DoS attack, perpetrated in Estonia in 2007. In May 2007, the country's administration, banks and industrial apparatus were paralyzed by a Russian cyber-attack. Since Estonia had completely digitalized the main infrastructures, the success of this strike was predictable. The reason behind such a gesture was the rapprochement between Estonia and NATO and that is why, after this tragic event, Estonia called NATO to respond. Hence, despite the digital nature, the dynamic of the conflict does not differ to an actual invasion of the Russian army. This remains the major cyber-attack against state infrastructures. Nonetheless, there are other important examples, such as the case of Stuxnet in 2016 and the American aircraft in Iran in 2017.

[47] See *Rapport d'enquête de la Fédération internationale des droits de l'homme sur « l'Affaire Amesys ».*

[48] See IFRI Politique Etrangère (2018)

The Stuxnet was a virus employed to target uranium heating centres in Iran. The consequence was the disruption of operations and a degradation in uranium quality. The Iranian services did not immediately realize to be victims of a cyber-attack, thinking to deal with a technical problem. Finally, Iranian secret service found out that the true responsible was Israel, helped by American technological support. However, Americans denied having given support to Israel. Despite the usage of cyber-weapons, this controversy is framed by the nuclear battle between Israel and Iran.

The last practical example concerns not only the vulnerability of a state, but also the permanent effects of this type of cyber-attacks. In 2017, Iran's cyber defence services took control of an American aircraft that flew into the area. Thus, the aircraft landed in Iranian territory, allowing Iran to retrieve and explored American technology. The US denounced Iran, because it acted against the international law. As a result, sanctions have been imposed but American technology was already translated into technical plans and sold to Moscow and Beijing by the Iranians. Thus, the damage was irreversible.

In addition, another threat in the cyber space is “cyber-espionage”. This technic aims to steal sensitive data and, when it is convenient, publish them. The data access it is facilitated by the existence of digital companies and social networks, where it is possible to penetrate the systems and steal data in a discrete way. The first biggest company which was victim of cyber-espionage in 2013, is *Yahoo*. Facebook was another victim in 2017-2018, showing the vulnerability of private actors and their need to develop a cyber defence in compliance with the government, the ultimate guarantor of citizens’ privacy. Along with the spying classic framework, there are other strategic means like the interceptor mails and the publication of secrets. For instance, in 2016 the email of some American Democratic Party’s member was hacked to steal data and destabilize the presidential campaign. Beyond the classic interstates relations, cases of piracy and industrial espionage are frequent, such as the theft of *Renault* data by the Chinese.

Finally, the last kind of cyber-attacks employs ransom system, called “Ransomware”, to blackmail. This modus operandi can be easily set up by isolated individuals and have dramatic effects. For example, in May 2017 two large successive cyber-attacks occurred, contaminating 300 thousand computers in 150 Countries in just two days. The ransomware was called *WannaCry* and its origin is still unknown. The same year, in June the ransom *Notepya* affected administrations and multinationals worldwide. Despite the extension of the attacked area, a clear target was identified. That was Ukraine and the aim was to weaken the power of Kiev. This is the reason why Russia was targeted as potential responsible. Nevertheless, Ransomwares are usually employed by criminal groups, due to the amount of money involved and the opacity of these attacks.

To conclude the cyber space is multiplying potential hot spots, vulnerabilities and the targets of potential attacks. Paradoxically, nowadays data can be better protected in a paper archive than on a digital one, where they can become easily an instrument of conflict.

However, the keywords to contrast the cyber menace are coordination and clarity of the command and control lines. It needs a comprehensive approach which would involve different investment realities and agencies devoted to the protection of critical infrastructures. Moreover, it is also necessary to involve important economic operators, who are an essential part of the country-system, to define adequate security protection measures and equip them with resources and professionalism. These are the cornerstone of the cyber-defence strategy against potential attacks[49].

In the last few years companies, civil, governmental and military organizations around the world have been fighting cyber conflicts every day within the cyberspace. The dynamism and ambiguity of cyber-attacks require the adoption of new techniques, methodologies and skills aimed at fighting cyber threats. Thus, defensive and offensive tools are developed thanks to a continuous research and acquisition of online information concerning the opponents.

In this complex but advanced system, espionage and cyber-espionage can play a fundamental role in protecting, not only attacking the integrity of information assets. Indeed, if computer security tends to the optimization of the technological infrastructure to reduce the vulnerability of IT systems, cyber espionage and cyber counterintelligence activities can create an indispensable "wisdom" for the predictions of future scenarios, to understand the trends and objectives of the adversaries and to provide support in the decision-making processes. These are example of cyber intelligence activity, which includes also new tools for contrasting and manipulating information, such as online deception (cyber deception), defined by J.J. Yuill as “ a set of actions designed to mislead attackers and take specific actions to help cyber security defences”, and the adoption of psychological, cognitive and behavioural schemes (cyber behaviour) to grasp the thoughts and attitudes of hackers. The operational space in which these cyber intelligence activities are applied is not limited to national defence and include other sectors more directly related to population needs[50]. Indeed, in the current climate of mistrust, each agency as well as each country is setting up its own cyber security strategy.

[49] See Teti (2018: 183-204)
[50] Ibid.

Chapter 3. Case Studies:
National security strategies in the USA, Russia and China

Besides the specific topic of cyber-security, overall each country tends to set up its own security strategy. Indeed, the National Security Strategy (NSS) is an official document, drafted periodically by each state, defining the core issues that can affect national security and designing a strategic plan to face them.

In the previous chapter, some of the most dangerous global challenges have been qualified. According to the most recent Global Risks report, drafted by the World Economic Forum, a global threat owns five features: global scope, cross-industry relevance, uncertainty, economic or public impact and multi-stakeholder approach. The following table is going to explain these concepts:

Global scope: a risk should have the potential to affect - including both primary and secondary impact - at least three world regions to be considered global. Despite a regional or even local origin, the impact can potentially be felt globally.
Cross-industry relevance: The risk has to affect three or more industries, including both primary and secondary impact.
Uncertainty: There is uncertainty about risk's effects within ten years and uncertainty about the magnitude of its impact. This assessment must be done in terms of likelihood and severity.
Economic/Public impact: The risk has the potential to cause economic damage of 10 billion US$ or more and/or the potential to trigger considerable public pressure and global policy responses.
Multi-stakeholder approach: A certain complexity of the risk, both in terms of effects, drivers and inter-linkages with other risks. That require a multi-stakeholder approach for the risk mitigation.

[Source: World Economic Forum 2019]

These features can be applied to all the aforementioned threats, namely biological, environmental and cyber threats, but also to other ones. Global threats are the result of a change in the international relations (IR), which have become more fluid and less predictable with the end of Cold War. Indeed, although the scholar Martin White has assumed that the principal value of IR is the persistence of history, which allows to find a solution against future challenges, it is undeniable that the world is facing unprecedented threats[51]. Such a complex international environment requires to deal with these menaces alongside with the state, applying a

[51] See Fabio Rugge (2019)

comprehensive approach and making external and domestic policies meet[52]. Thus, each state or International Organization should include these global threats in their own NSS and be ready to face them, sometime going beyond its interests.

In the last few years states tend to have a more realist and nationalist approach, provoked by an evident shift in the governance and government of various important influential countries and the alleged decline of liberal democracy. The decline of liberal democracy started in 2006, when the global financial and economic crisis occurred. Today can be observed the survival of a few totalitarian states (e.g. North Korea/DPRK), a sizeable group of authoritarian and kleptocratic[53] governments (e.g. Syria, Eritrea) and a growing number of managed[54] democracies (following, more or less openly, Russian practices). On the backdrop one can also see a spectrum ranging from governments that have failed - due to civil war, the influence of organized crime, systemic poverty, etc. - to democracies that are functional, but are increasingly subjected to manipulation and political interference, both from within and without the system. In such untrustworthy scenario, national security strategies are turning into a tool to protect national interest, manipulating the perception of the potential threats to explain and justify state decisions [55].

This statement is going to be investigated through the analyses of three NSS, namely the American, Russian and Chinese strategy. This chapter is going to point out how there is not a common agreement about menaces and that states prefer deal with global challenges targeting the other countries rather than cooperating with them. Such an approach, currently adopted by the global leading countries, can activate in the medium term a process of de-globalization, which would create a more conflictual multipolar world where the odds that a major war will occur would be very high[56].

3.1. The USA: Trump’s NSS in 2017

The last American NSS was drafted in 2017, after the installation of Trump and the Republicans in the White House. Such an edition presents elements of continuity with the previous administration and elements of innovation. Indeed, the choice of certain strategies rather than others reflects Republicans’ priorities. Nevertheless, basic American values remain unquestionable. For instance, the US has maintained the EU-

[52] See Laura Mirakian (2019)

[53] A kleptocracy is a government with corrupt leaders (kleptocrats) that use their power to exploit the people and natural resources of their own territory in order to extend their personal wealth and political powers. Typically, this system involves embezzlement of funds at the expense of the wider population.

[54] A managed democracy, also called guided democracy, is formally a democratic government that functions as a de facto autocracy. Such governments are legitimized by elections that are free and fair, but do not change the state's policies, motives, and goals. Under managed democracy, the state's continuous use of propaganda techniques prevents the electorate from having a significant impact on policy.

[55] See Alessandro Politi (2019:11-12)

[56] Ibid.

NATO partnership as a cornerstone in its strategy, while several multilateral agreements, such as TPP, NAFTA and the Paris Agreement, are questioned preferring a more bilateral approach for future negotiations. President Donald Trump justifies his choice defining these agreements as an "unfair burden-sharing with our allies", incapable to actually defend the USA against hostile actors. Trump's motto "America First" is the base of the strategy, offering a narrow and focused view of American global position in line with realism's principles. In fact, Trump claims that the last NSS "is realist because it acknowledges the central role of power in international politics, affirms that sovereign states are the best hope for a peaceful world and clearly defines American national interests" (Donald Trump 2017: 55). Since the realist theory sees the international environment as a zero-sum game, applying this approach requires harder forms of power, such as an increase in defence expenditure and harsh measures against sneaky competitors. The realist analysis has been employed also in the selection of the current main threats, which are basically the other states. It is interesting to notice that the menace of WMD is defined as a problem only in relation with the development of nuclear weapons and missiles by certain rogue states in Middle East. Moreover, the so-called "US enemies", namely China, Russia and Iran, are blamed to encourage radical Islamist terror groups, criminal cartels work, unfair trade practices, porous borders and unenforced immigration laws to make the US vulnerable[57].

China is described as an ambitious and dangerous country, which is trying to affirm its dominance in the whole Indo-Pacific area. According to the American narrative, Chinese strategy consists in presenting its ambitions as mutually beneficial to limit American access in the region and militarize the South China Sea. In addition, Chinese investments and trade strategies in Europe, Latin America and Africa are only a mean to affirm a global dominance beyond its regional borders. These are the reasons which have justified the escalating trade war between the United States and China, culminated with the recent decisions by the US administration to impose a further ten percent tariff on $200 billion worth of Chinese imports and the sharp drop of the Chinese currency[58].

Among the US's enemies, Russian strategy differs from Chinese one, prioritizing intimidation. Russia's actions aim to provoke the credibility of the USA and the EU, questioning the sovereignty of certain strategical states, like Georgia and Ukraine, and openly threating the other countries through WMD and cyberattacks[59]. The USA has responded sanctioning Russia, provoking an impact on its economy to jeopardize its social peace. Nonetheless, after the imposition of Western sanctions for the annexation of Crimea and the open conflict in Ukraine, Russian international influence has expanded and gained relevance. As a matter of fact, the freezing of relations with the West and the impact of sanctions, especially those affecting the energy and financial sectors, have led Russia to look East, intensifying economic, political and military relations with

[57] See Donald Trump (2017: 1)
[58] See Elenoire Laudieri (2019: 39)
[59] See Donald Trump (2017: 46)

China, accelerated the process of integration within the Eurasian Economic Union (with Armenia, Belarus, Kazakhstan and Kyrgyzstan), intensified its involvement in the Shanghai Cooperation Organization and in the BRICS, and reached a historic agreement on the Caspian Sea with the other littoral countries. Such controversial relations between the US, China and Russia are described in the fifth part of the NSS, called "The Strategy in a Regional Context". The other pillars are shorter and include "Protect the American People, the Homeland and the American Way of Life", "Promote American Prosperity", "Preserve Peace through Strength" and "Advance American Influence". It is evident by the NSS's structure that the US prioritizes dangers associated with foreign states interests rather than fatal global threats. The particular attention devoted to cyber-security, drafted in the first pillar dedicated to "Protect the American People, the Homeland and the American Way of Life", is an exception justified by the tangible risk of foreign states' infiltration. In the cyber-security domain, the President Trump shows his awareness about adversaries' low-cost opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken Federal networks, and attack tools and devices used every day by Americans to communicate and conduct business. The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks mean that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication. Federal networks are also those which allow government agencies to carry out vital state functions and provide basic services to the American people. Thus, the risk associated with cyber-attack is high, especially when cyber capabilities become tools for projecting influence and protect and extend autocratic regimes. In the section of the NSS dedicated to cyber, the US administration recognizes the presence of malicious state which use cyberattacks for extortion, information warfare, disinformation and, above all, to undermine faith and confidence in American democratic institutions and in the global economic system. This is the reason why, the United States include in their NSS the need to deter, defend, and when necessary defeat these actors who use cyber capabilities against the USA[60]. The US strategy against cyber-attack is clear and effective and includes the priorities actions highlighted in the following table:

[60] See Donald Trump (2017: 4)

Improve attribution, accountability and response: It means to invest in capabilities to support and improve the US ability to attribute cyber- attacks and allow for rapid response. The importance of preventing the attacks before they affect U.S. critical infrastructure lies in the capability of response. Indeed, the United States could impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities.
Enhance cyber tools and expertise: It means to improve cyber tools across the spectrum of conflict, U.S. Government assets and U.S. critical infrastructure protection, as well as the integrity of data and information. First of all, it requires to properly identify and prioritize the risk assessing, especially where cyberattacks could have catastrophic or cascading consequences. In this sense, the American NSS have been identified six key areas, namely national security, energy and power, banking and finance, health and safety, communications, and transportation. Then, the latest commercial capabilities, shared services and best practices to modernize the Federal information technology are employed. The U.S. departments and agencies will recruit, train, and retain a workforce capable of operating across this spectrum of activity.
Improve integration and agility: Basically, it is an improvement in the integration of authorities and procedures across the U.S. Government, which allows to pursue cyber operations in the proper way. Thus, the aim is to create a comprehensive approach between the Congress - responsible for addressing the challenges that continue to hinder timely - and the intelligence to share information, plan the operations and the development of the necessary cyber tools. Moreover, in accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector to better detect and attribute attacks.

[Source: the US National Security Strategy 2017]

In sum, that is the American strategy to face cyber-attacks, which have hit several times the USA in the last few years. With regards to the other global threats that has been mentioned, namely climate change and biological threats, there are only few remarks.

The Trump's NSS dedicates no more than one section to the biological threat, referring to the deliberate 2001 anthrax attacks against the USA. Nonetheless, the impact of biological threats on national security has been grasped by the President Trump, especially its potential harm against lives, economy, and confidence in government institutions. Furthermore, the risk that state actors or malicious non-state actors develop more advanced bioweapons through advancements in life sciences is considering very high.

Along with this, three priorities actions are fixed:

Detect and contain biothreats at their source: it implies to work with other countries to mitigate and prevent the spread of disease and ensure that laboratories that handle dangerous pathogens have in place safety and security measures.
Support biomedical innovation: it is possible by strengthening the intellectual property system that is the foundation of the biomedical industry.
Improve emergency response: it is obtained strengthening the emergency response and unified coordination systems to rapidly characterize outbreaks.

[Source: the US National Security Strategy 2017]

On the contrary, climate change issues are not directly mentioned in Trump's NSS. There is not a section dedicated to global warming risks, only some lines concerning the importance of energy. The NSS 2017 claims that "the United States will continue to advance an approach that balances energy security, economic development, and environmental protection, remaining a global leader in reducing traditional pollution, as well as greenhouse gases, while expanding our economy" (Donald Trump 2017: 22). American "vibrant cross-border energy trade and investments" (Ibid.) are considered as vital for a robust and resilient U.S. economy and its energy market and - even though the US committed to supporting energy initiatives aims not only to attract investments but also to safeguard the environment - the economic gain is the main concern. In fact, the US withdrawal from the Paris Agreement demonstrates that Trump priorities are not about climate, but about economic growth. This approach differs from the previous administration and the NSS 2015 position, in which President Obama considered to ignore global problems such as climate change as a key danger. Conversely, in President Trump vision the danger resides in the dilution of the US national interests, caused by the over-committing to broad multilateral agreements that ignore how competitors, such as China, Russia or Iran, can take self-interested advantage of them[61].

3.2. China: Outline of the National Security Strategy, January 2015

In January 2015, the Politburo of the Communist Party of China (CPC) passed an "Outline of the National Security Strategy". The Chinese National Security Strategy was produced by the Central National Security Commission, established in January 2014, under the direct leadership of Xi Jinping as Commission's Chairman. Notwithstanding the full text is not accessible, the official state media has published a few

[61] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 18)

statements and comments about that, which have made possible to draw some conclusion about its premises and goals. During the first meeting of the Commission, held in April 2014, ten categories of security were listed, namely security of political rule, national territory, military affairs, economy, culture, society, information, ecology, natural resources and nuclear security. Xi has elaborated a comprehensive national security outlook by saying that "the security of the people is the objective, political security is the foundation, economic security is the basis, military, cultural, and societal forms of security are the guarantees, and international security is the support". Thus, the Chinese strategy poses the international security only as a support to sustain Chinese people security. Such an international security is threatened by American, Russian and European attitudes and policies against Chinese territory and maritime interests, referring to the Western promotion of democracy, cultural hegemonism, profligate dissemination of news and media on the internet and religious infiltration. This is considered as a peaceful evolution strategy aimed at undermining socialism and China's values. In particular, internet provides a channel for breaking China's ideological and national cohesion at the same level of a terrorist attack. As a result, the international environment provokes a grave concern in the Chinese government, which demands peace, cooperation and mutual benefits externally and development, reform, and stability internally.

In October 2017, Xi Jinping announced the beginning of a New Era of Socialism with Chinese Characteristics which would lead to the completion of a socialist modernization by 2035 and China's emergence as one of the leading nations in the world with a world-class military in the 2050s[62]. This vision of national development and revitalization is known as the "Chinese Dream", a dream which seeks to ensure economic prosperity, social stability, and an overall higher quality of life for Chinese citizens. It also seeks to restore national prestige and assure China's rise as a prosperous and powerful nation. The socialist system with Chinese characteristics has been the guiding ideology of the CPC since the Deng Xiaoping era (1977–1992), enshrined also in the 2015 Outline of the National Security Strategy. Indeed, the Chinese NSS addresses this need to perfect the Chinese socialist system and guarantee the *anbang-dingguo* (安邦定国, namely the internal peace and stability of governance. In practice, Beijing's security strategy revitalization has promoted at the regional level security-related organizations and institutions that do not include U.S. representation, such as the Conference on Interaction and Confidence Building Measures (CICA) and the Shanghai Cooperation Organization (SCO). Furthermore, the Chinese confidence about the leading role of China in the world has been seen when the government flaunted its Belt and Road Initiative and taken a hard line on territorial issues such as the South China Sea and Taiwan[63]. Besides shaping the international environment, China's security strategy aims to enhance protection for its core interests, including those of national security, territory, sovereignty, and economic development. Over time, China's defence policy has similarly moved beyond a

[62] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 31)
[63] See Elenoire Laudieri (2019: 40)

focus on homeland defence to also cover regional threats and security needs beyond China’s immediate periphery. However, it is becoming evident that such overly nationalistic stance has been the reason why the United States are trying to undermine China's economic growth. The escalating trade war between the United States and China is raising concerns over its impact on the Chinese economy. In fact, tariffs are likely to affect business confidence, investment and growth, making more difficult to achieve the political objective of an annual GDP growth of around 6,5 percent until at least 2020, a target declared by the President Xi in late 2015 during a meeting of the Chinese Communist Party. Achieving this growth rate, at all costs, for five consecutive years would generate sufficient combustible material in the shadow banks to make a financial crisis just a matter of time[64]. Therefore, China has already abandoned its role of economic giant in favour of massive investments in defence since 2017. In this domain, the People’s Liberation Army’s (PLA’s) is the primary guarantor for achieving China’s national security goals beyond Chinese internationally recognized borders and for supporting domestic security forces inside the country. The PLA’s tasks include shaping the international and regional security environment through military-to-military engagement and participation in peacekeeping and other non-war missions. It is also responsible for defending core interests by maintaining a strategic deterrent, defending territorial and maritime claims, defending land borders, and carrying out a variety of missions to protect more distant economic and other interests. China’s military strategy has evolved as well as its threat assessment and its place in the world. Two key military strategy concepts include “active defence” and local wars under “informatized” conditions. Active defence posits an operationally defensive posture for the PLA and states that the military will not strike first. The definition of what constitutes a “first strike” is ambiguous. Because Chinese strategists regard a defensive-oriented security policy as compatible with offensive military actions. Indeed, a defensive security policy limits the authorized use of military force to the protection of China’s core interests, hence any threat to a core interest, even if a latent or perceived threat, could justify military actions. The PLA is also working to develop greater cyber tools to degrade the war fighting capabilities of an adversary or hold critical infrastructure at risk during a conflict. These instruments comprise elements of command, control, communications, computers, intelligence, and surveillance (C4ISR) and counter-C4ISR information operations, but they also potentially provide unique offensive means against strategic targets such as power grids, transportation networks, and financial systems. The cyber capabilities employed in this category encompass the usage of computer network exploitation (CNE) and computer network attack (CNA) to glean information about an adversary and target an adversary’s networks or critical infrastructure. Critical infrastructure could include logistics hubs, reinforcement centres, command and control (C2) facilities, key missile, air, and naval bases[65]. These are all elements of war under “informatized” conditions. Such a war can be understood clarifing that the definition of cyber usually

[64] See Elenoire Laudieri (2019: 41)

[65] See Timothy R. Heath, Kristen Gunness, Cortez A. Cooper (2016: 37)

employed by Western experts and media, namely a domain enclosed in Internet and in the electronic world, is not the same applied by Chinese expert, media and government agencies. The Chinese consider the cyber domain as part of a broader framework, which includes the information space. This is the set of information of which citizens can access through internet, media and oral communication. Similarly, the term cyberwarfare is used in China only in reference to Western cyber operations. The Chinese prefer to deal with information warfare, a concept that includes all the cyber offensive operations carried on by the People's Liberation Army (PLA) and by the responsible government agencies. In China prevails a holistic approach on the cyber warfare, which explains the state management of media and web. In fact, the Politburo vision of uncontrolled information as a danger and not as an opportunity, justified the main role of the state in controlling cyberspace. In addition, the Chinese political culture prioritizes the maintenance of social order above citizens' privacy and freedom of thought.

However, the knowledge of Chinese cyber-strategy is complex because of the absence of a consolidated doctrine. In effect, only in the last few years - with the presidency of Xi Jinping - the Chinese government has started a process of institutionalization of the cyberwarfare by creating new civil and military structures and increasing investment in cyber research. One the earliest documents that outlined a Chinese cyber strategy is a book called "Unrestricted Warfare", written by Qiao Lang and Wang Xiangsui, two colonels of the Chinese army in the late 90's. The book explains how China could compare and overcome a technologically superior country through the employment of asymmetric instruments without resorting to traditional military force, such as through the sabotage of enemy networks. In fact, China has decided to invest in the cyber domain aware of not being able to compare with the United States military power. In recent decades, various bodies, such as the State Council of Information Office (SCIO) or special working groups formed by the Politburo, have drawn up programmatic documents for a cyber-strategy. For instance, it is the case of "Document 27", a national security strategy developed in 2003 by the State Network and Information Security Coordination Small Group, then chaired by Premier Li Keqiang. A first attempt to find a unitary strategy for both the cyber dimension and control of information came with the establishment, in February 2014, of the Small Leading Group for Internet Security and Informatization. The group was chaired by Xi Jinping and it was created for the precise purpose to combine information security and information control. Despite the initiatives pursued by Xi has partially solved the institutional fragmentation of Chinese cyber-governance, today there are still dozens of government agencies and army departments dealing with cyber domination in all its dimensions. As mentioned before, the President Xi has initiated an army reform to built logistics systems that offer support to fight and win modern wars, serve the modernization of the armed forces and lead them to informatization. Along with this, it has been created a new department, called Strategic Support Force (SSF). The SSF has the dual aim of presiding over operations in space and cyber space. In the near future, the SSF will likely be responsible for the majority of cyber operations. Currently, the units dedicated to cyberwarfare remain within the Third Department (3 / PLA), a sort of American National Security Strategy counterpart. This department is divided into twelve bureaux, each with a different function. Units 61398 and Unit 61486 are among the most lethal Chinese cyber actors. The first division was brought to light by a report of the cyber security company Mandiant. The investigations about the Unit 61398 carried on by experts and confirmed by intelligence sources, have traced back a long trail of cyber-attacks against US' institutions and critical infrastructure that began in 2006, to hit the Pentagon, the State Department and Coca-Cola. With regard to the unit 61486, the cyber-security company CrowdStrike demonstrated that it has conducted cyber-attacks against European and American companies operating in the defence and aerospace sector. Taking everything into account, it is evident an increase in the level of institutionalization acquired by the Chinese cyberwarfare over the years. Moreover, according to the political expert Edward Luttwak, the majority of the Chinese cyber-attacks are driven by state employees, functionaries and militaries rather than hacker collectives, because the ultimate goal of Chinese cyber-strategy is no longer "catch-up", which means the achievement of an equal military capabilities of the US, but the idea of Sha Shou Jian, namely "if you get the proper resources, you can defeat an enemy much bigger and stronger than you"[66].

These are the reasons behind the enhancement of Chinese cyber investments, the increasing role of Chinese cyber-espionage and the inclusion of cyber-security in the Chinese security deterrence strategy alongside nuclear threats.

Despite the importance of nuclear in the Chinese security strategy is undeniable and comparable with cyberwarfare, the other WMD are not mentioned in the Outline. Chemical and biological threats are not taken into account by the Politburo, which remains more focused on technological research rather than biological one.

Dealing with environment, the question is more complex. In effect, China's leaders added environmental-related policy objectives to its overall program at the 18th Party Congress in 2012, establishing one year later a four-tiered alert system for air quality. More recently, issues related to the health of China's environment have risen in prominence, so much to include them in the Security Outline under the heading "ecology" and "natural resources". Policies have been directed to clean the country's water, air, and soil - all of which heavily contaminated - and improve the quality and safety of food and products. In spite all the effort, in December 2015 China issued the first air pollution "red alert" in Beijing (the highest possible alert level) and the implementation of the policies remain problematic. Actually, the core issue is that climate change effects has been subordinated to Chinese economic interests, since the PRC government researchers state that cheaper and more abundant energy resources are essential to China's continued economic growth[67]. In

[66] See Paolo Messa (2018: 93-100)

[67] See Alessandro Politi (2019: 13)

conclusion, despite Xi initial statement about looking for human security and cooperation, global threats maintain a marginal position in the Chinese strategy if compared to state core interests.

3.3. Russia: Putin's National Security Strategy, December 2015

On December 31st , 2015, the Russian President Putin signed the Russian National Security Strategy. The decision to review the National Security Strategy, taken by the Security Council, was publicly announced in May 2015, when Nikolai Patrushev - then Secretary of the Security Council - wrote in the Russian armed forces newspaper, called *Krasnaya Zvezda*, argued that a revision of the previous strategy was needed due to the changing security environment. He referred explicitly to the "Arab Spring" in Syria and Iraq, as well as the continuing conflict in Ukraine. According to Patrushev, the major powers use indirect measures to further their interests, including the use of the protest potential of the masses, radical and extremist organizations, and private military companies to advance state interests. Later in July 3rd, 2015 - two days after the publication of the United States National Military Strategy - the Security Council held a meeting where the president Putin instructed the review of the national security strategy based on the analysis of the whole spectrum of potential challenges and risks.

The main structural elements, such as the division in six chapters, has been the same of the previous strategy, drafted in May 2010. In the 2015 edition, Chapter 4th is the longest one and it deals with the "protection of national security". It lays down a comprehensive security outlook for Russia, including such topics as national defence, state and public security, improving the quality of life of Russian citizens, economic growth, science, technology and education, public health, culture, ecology of living systems, rational use of natural resources, strategic stability and the equal strategic partnership. The new strategy sees the world through the prism of "strategic stability", whereby the military component of national security and the relevance of Russia's position in the world are emphasized. A dominant position can be achieved - according to the Kremlin - using the full spectrum of means in the competition for power and prestige, abandoning the previous idea of economic and technological transformation as a route to Russia's global economic competitiveness. At the root of this change is Putin's third presidential term, when the development of the defence industry was identified as the driver of Russia's modernization[68].The function of the Strategy is outlined in Article 4, where it is stated the intention to consolidate the policies and actions of different state agencies and civil society actors in an effort to create favourable internal and external conditions to realize the Russian Federation's national interests and strategic national priorities. This is a key paragraph, which expresses both the function of the strategy (as a guideline for policymaking) and the direction of the policy (the creation of favourable internal and external conditions). As main threats against national security are

[68] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 42)

identified the erosion of Russian values, the weakening of the historical unity of the peoples of Russia and the external cultural and information expansion. The references to the conflict with the West are implicitly voiced, although the direction of the critique is evident. For example, the strategy identifies as a risk the practice of overthrowing legitimate political regimes and provoking intrastate instability and conflicts, referring to the Ukrainian conflict. Along with this, Russia points out how territories affected by armed conflicts are becoming the basis for the spread of terrorism, interethnic strife, religious enmity, and other manifestations of extremism. Such terrorist and extremist organizations could carry out major attacks, including with nuclear, chemical or biological weapons[69]. Moreover, the strategy makes some puzzling assertion of the spread of U.S. military-biological labs nearby Russian borders. This most likely refers to a number of cooperative biological defence facilities set up with the governments of Georgia, Ukraine, and Kazakhstan, which some Russians have viewed as a means to continue the development of biological weaponry under cover of efforts to seek antidotes and defences[70].

In addition, the strategy identifies radical public associations, foreign and international nongovernmental organizations, financial and economic structures, and even individuals as aiming to destroy the unity and territorial integrity of the Russian Federation, destabilizing the domestic political situation[71]. In this threatening framework, it has been spread the idea that traditional military power, always important in intimidating weaker neighbours, is not sufficient for protecting Russian strategic interests. The changing security landscape requires an “asymmetric approach” whereby the strengths of Russia (the weaponization of information, technology and organizations) counterbalances its relative weakness in military-technological development. The main objective of this approach is expressed in Article 36, in which has been summarized Russia’s strategy of “active defence”, namely the activation of a set of non-military measures - i.e. informational, political, economic, organizational and cyber resources - to neutralize potential threats to Russian national interests[72]. Among these non-military measures, cyber-security deserves a special mention. In this field, Moscow has taken a different, more comprehensive and integrated approach to information security compared to Western capitals’ focus on more technical network-centric capabilities. It is interesting that rarely it is heard the word “cyberwarfare” in Moscow, preferring the term “information warfare” (*informatsionnaya voyna*) used by Russian propaganda to expose or condemn alleged interference of the West in its domestic affairs[73].

Such a Russian focus on the control of information dates back to the Soviet era, when the Bolsheviks sought to use mass media not to inform but to shape and mould the populace. In more recent times, the Russian

[69] See Vladimir Putin (2015)

[70] See Roger Roffey and Anna-Karin Tunemalm (2017)

[71] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 45-46)

[72] See Vladimir Putin (2015)

[73] See Paolo Messa (2018: 87)

government - as shown in official documents like the 2000 Information Security Doctrine - has linked information security to internal stability, arguing that the state should take a strong role in guarding against external interference. Over the years, events like the colour revolutions in Ukraine and Georgia, the Arab Spring, and the 2014 ouster of Ukrainian President Viktor Yanukovych have contributed to Russia's heightened sense of threat in the information domain and have provided justifications for extensive domestic Internet surveillance and control[74]. Thus, the cyber aspect is only a piece of a great strategy pursued by the Kremlin since the beginning of the Cold War. Disinformation, espionage and cyber operations are all manifestations of that *informatsionnaya voyna* to which explicitly refers the Gerasimov doctrine saying that "the information space opens up ample asymmetric possibilities to reduce the potential enemy". In the last few years - especially in the aftermath of the Russian invasion of Crimea - the Western media have begun to indicate such Russian war strategies with the name of "Hybrid War". The hybrid nature of the Russian war resides in the joint use of psychological warfare, trolls, economic warfare, sabotage of electoral systems alongside conventional military operations. As specified in the first chapter, the hybrid war is not an unprecedent phenomenon, but Russia has been the first state to employ cyber-technologies to widen the range of military operations. However, the British academic Keir Giles said: "despite the Russian doctrinal references to indirect or asymmetrical methods, hybridization does not define entirety the new Russian war strategy. The role of conventional and asymmetric capacities and means in Russian military doctrine must be placed in Moscow general perception of new strategic challenges, where nuclear and conventional conflicts are still protagonists". In this complex framework, the Kremlin has gradually institutionalized the cyberwarfare under the leadership of Putin, by inaugurating special military units[75]. For instance, Russian armed forces have recently embraced the cyber war, which once was the exclusive prerogative of agencies such as the Secret Service of the Russian Federation (FSB), the Main Information Directorate (GRU) or the International Intelligence Service (SYR). Officially, the Kremlin's approach to cybersecurity is still defined by the FSB generals at the Security Council and the foreign ministry's Department for New Challenges and Threats (headed by the Kremlin's special envoy on cybersecurity, Andrey Krutskikh). Intellectual support is provided by Moscow State University's Information Security Institute, a think tank founded and led by Vladislav Sherstyuk. Nonetheless, these state actors presented only the façade of the Kremlin's approach to cyber issues[76]. Indeed, in putting its military doctrines into practice, one of the tactics employed by Russia is to co-opt with criminal hackers. Former Soviet states have large populations of highly educated, technically skilled individuals who have few legitimate economic opportunities. Such a situation leads some of them to turn into hackers and work for criminal enterprises. There is a nexus between the state and criminal hackers,

[74] See Roberto D'Agostino (2019: 66)
[75] See Paolo Messa (2018: 88)
[76] See Andrei Soldatov and Irina Borogan (2018: 18)

founded on a tacit bargain under which hackers will not target people within the former Soviet states and Russia will tolerate their criminal activity. This tacit toleration can be more proactive when Russian security services require hacking talent[77]. The first experiment to test Russian cyber offensive capabilities occurred in Estonia in May 2007, followed by the cyber-attacks against the Georgian government in summer 2008. Several cyber-attacks were also perpetrated during the conflict with Crimea and, in December 2015, the cyberwarfare against Kiev evolved. In fact, in the afternoon of the 23rd, three of the country's main electricity companies suffered a blackout caused by cyber-attacks. More than 220,000 people has been left in the dark for six hours in the harsh Ukrainian winter. This strike opened the door to a new frontier of cyberwarfare, pointing out how targeting country's critical infrastructures undermine people's confidence in the institutions and in their ability to defend the citizens. The aforementioned attacks have been planned in detail and carried out by collectives of hackers with resources, expertise and an organization out of the reach of a private citizen. It is evident that these groups operate fully respecting the Russian political agenda, acting against countries considered Russian Federation's enemies to send a message against Ukrainian government. This kind of team can respond directly to the Russian government or to oligarchs who work on their own. The Kremlin has more than one valid excuse to rely on these units. First of all, their cost is relatively cheap. Secondly, the collective can be recruited and discharged quickly. Finally, hackers guarantee anonymity, managing easily to vanish without a trace[78].

To sum up, traditional military means, WMD, cyber tools and national interests remain the first concern for Russian government. With this perception, challenges like climate change are always subordinated to political interest and, apart from a few references to global warming in the Russian National Security Strategy 2015, it does not consider a hazard.

[77] See Tim Maurer and Garrett Hinck (2018)

[78] See Paolo Messa (2018: 92)

Chapter 4. Case Studies:
A multilateral perspective

In the first chapter, the difference between national security and human security has been defined. With the concept of “human security” the individual turns into the centre of the analysis and to protect people from economic, food, health, environmental, personal, community and political security becomes its ultimate purpose. It is important to focus on this idea, which brings together different and previous neglected human elements of development, security and rights, because global challenges affect first and foremost people as human beings, not as citizens of a certain country. Indeed, events like climate change effects, cyber threats and bioterrorism affect everyone without distinction, provoking a global insecurity which vary significantly across countries and communities. Both the causes and expressions of global challenges depend on a complex interaction of international, regional, national and local factors, making the one-way bilateral approach (described in the previous chapter) to achieve human security useless, less realistic and at times destructive. Since it accepts that human insecurities cannot be tackled in isolation through stand-alone responses, a comprehensive approach - which stresses the need for cooperative and multilateral responses - must be applied. In practise, such an approach is embodied in the 21st century proliferation of regional and international organizations, which become more multifunctional and devote themselves in whole or part to security goals. Old-style alliances with a defined opponent are now rare, and most groups address themselves to the reduction of conflict (internally or externally) and to transnational challenges such as terrorism. It is no coincidence that regions where these structures are absent or weak are also those with the greatest remaining problems of interstate tension or internal violence.

Taking everything into account, it is easier to face menaces which affect the world as a whole using a cooperative behaviour rather than apply the traditional national approach. This statement is going to be empirically demonstrated through the analysis of regional and international organizations’ security response, particularly that pursued by NATO, EU, SCO and UN.

4.1. NATO’s Strategic Concept

The North Atlantic Treaty Organization is a political and military alliance established in 1949 and currently composed by twenty-nine members.

The official document that outlines NATO’s enduring purpose and nature and its fundamental security tasks is the Strategic Concept. The last NATO’s Strategic Concept was drafted in 2010 and assess the value and importance of working with partners from across the globe and a review of NATO strategic posture. It also identifies the central features of the new security environment, specifies the elements of the Alliance's approach to security and provides guidelines for the adaptation of its military forces.

The 2010 Strategic Concept - after having described NATO as "a unique community of values committed to the principles of individual liberty, democracy, human rights and the rule of law" (NATO Strategic Concept 2010: 6) - presents NATO's three essential core tasks, namely collective defence, crisis management and cooperative security.

Collective defence: NATO members will always assist each other against attacks, in accordance with Article 5 of the Washington Treaty. That commitment remains firm and binding. NATO will deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole.

Crisis management: NATO has a unique and robust set of political and military capabilities to address the full spectrum of crises before, during and after conflicts. NATO will actively employ an appropriate mix of those political and military tools to perform the following function:

- help manage developing crises before they escalate into conflicts that have the potential to affect Alliance security;
- stop ongoing conflicts where they affect Alliance security;
- consolidate stability in post-conflict situations (where that contributes to Euro-Atlantic security).

Cooperative security: The Alliance is affected by, and can affect, political and security developments beyond its borders. The Alliance will engage actively to enhance international security at the lowest possible level of forces, through partnership with relevant countries and other international organisations. This engagement is embodied in an active contribution to arms control, non-proliferation and disarmament and in NATO's open-door policy towards all European democracies that meet their standards.

[Source: NATO Strategic Concept 2010]

Among them, "collective defence" remains the Alliance's greatest responsibility and "deterrence" the core element of NATO's overall strategy, based on an appropriate mix of nuclear and conventional capabilities. To crisis management, NATO is adopting a holistic approach, encouraging a greater number of actors to participate and coordinate their efforts and considering a broader range of tools to be more effective. This comprehensive, all-encompassing approach to crises, together with greater emphasis on training and developing local forces goes hand-in-hand with efforts to enhance civil-military planning and interaction. Thus, the Strategic Concept depicts an inclusive, flexible and open relationship with the Alliance's partners across the globe, especially stressing its desire to strengthen cooperation with the United Nations and the European Union. It also reiterates its commitment to developing relations with countries of the Mediterranean and the Gulf region[79].

Then, the document describes the current security environment and identifies the capabilities and policies to ensure that NATO's defence and deterrence, as well as crisis management abilities, are sufficiently well equipped to face today's threats. These threats include, for instance, the proliferation of ballistic missiles and nuclear weapons, terrorism, cyber-attacks and environmental problems. In view of these priorities, the strategy affirms that NATO will continue its reform and transformation process in order to maximise efficiency, improve working methods and spend its resources more wisely[80].

Nonetheless, the strategic landscape has not suffered just a transition in the last few years, but a real shock which has made the 2010 Strategic Concept's approach obsolete. For example, on June 9th, 2018 there has been held the 44th G7 Summit, in La Malbaie (Quebec) and the 18th Summit of the Shanghai Cooperation Organisation (SCO), in Qingdao (China). In addition, a few days later, the US President Donald Trump met with the North Korean Supreme Leader Kim Jong-un at the so-called Singapore Summit. These three events have been proofs of the main transformations that are occurring in the international environment, such as the fragmentation of the West, the consolidation and reinforcement of the East around the main role of China and the denuclearisation of the Korean peninsula (for the first time after seventy years)[81].One fundamental point that has been underestimated and it is not present in 2010 Strategy is the return of great States power politics and the rise of potential peer competitors, i.e. China and Russia. The rude awakening for the Alliance has been in 2014 Russia's illegal annexation of Crimea, which changed the rules of the game and led NATO to adapt to new threats. For instance, an area of adaptation includes unconventional threats, such as terrorism, enhanced by phenomena of instability in the neighbourhood. In the last few years, the defeating of ISIS has been very encouraging, nevertheless, this is not the end. Indeed, terrorism continues to be resilient and widespread. Its impact has become critical in Africa, is still significant in the Middle East and Central Asia, and is increasing in South-East Asia, where occur a progressive shift towards international jihadism on the part of pre-existing groups and the coming up of new well-organised and well-funded groups. The arise of international jihadism demands the reallocation of some Counter-Terrorism resources, from kinetic anti-terrorism programmes to terrorism-prevention programmes, but for a conventional defence organization like NATO it is not easy to meet such unconventional challenges. Notwithstanding some difficulties, such as a great technological gap in

[79] See NATO Strategic Concept (2010: 26)
[80] See NATO Strategic Concept (2010: 33-34)
[81] See Di Paola G. (June 2018: 39)

the international community, the Alliance is actually preparing to deal with new threats adopting a 360 degrees security approach, in particular to face cyber and hybrid threats. In effect, predictions about potential "cyber apocalypses" have led NATO to warn against (and focus on) potential cyber-attacks capable of compromising its member states' critical infrastructure, paralysing the government or affecting the operational effectiveness of the armed forces. Practically, NATO have adopted an enhanced policy and action plan to maintain robust cyber defences. This enhanced policy was endorsed by Allies at the Wales Summit in September 2014 and the action plan was updated in February 2017. The policy recognizes that cyber defence is part of the Alliance's core task of collective defence and that international law applies in cyberspace. Among cyber top priorities, there is the protection of the communications systems owned and operated by the Alliance. The policy also reflects Allied decisions on issues such as streamlined cyber defence governance, procedures for assistance to Allied countries, and the integration of cyber defence into operational planning (including civil emergency planning). In addition, the policy defines ways to take forward awareness and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations like the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). It also foresees boosting NATO's cooperation with industry, including on information-sharing and the exchange of best practices through the NATO Industry Cyber Partnership. Allies have also committed to enhance information-sharing and mutual assistance in preventing, mitigating and recovering from cyber-attacks. Such an engagement with partners is based on shared values and common approaches to cyber defence and the requests for cooperation with the Alliance are handled on a case-by-case basis founded on mutual interest. Moreover, NATO's cyber defence policy is complemented by the aforementioned action plan with concrete objectives and implementation timelines on a range of topics from capability development, education, training and exercises, and partnerships. Allies pledged at the Warsaw Summit in 2016 to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term adaptation, this will reinforce the cyber-defence and overall resilience of the Alliance[82].

Alongside such new complex challenges, NATO is also changing its approach towards traditional threats. For example, regarding the proliferation of weapons of mass destruction (WMD) and their means of delivery, NATO is taking seriously into account the possibility for terrorists to acquire WMD, especially biological ones. During the 2006 Riga Summit, was already noted in the Comprehensive Political Guidance that the spread of WMD and the possibility that terrorists will acquire them would be the principal threats to the Alliance over the next 10-15 years. Indeed, there were already indications that terrorists have intended to acquire Chemical, Biological, Radiological and Nuclear (CBRN) materials for malicious purposes and, nowadays, the rapid advances in biological science and technology continue to increase such a threat. To date,

[82] See NATO Official web site: https://www.nato.int/cps/en/natohq/topics_78170.htm (July 2018)

the Alliance has responded to this challenge by addressing WMD proliferation, CBRN defence and consequence management, respectively, within relevant NATO bodies. Policies have focused primarily on developing military capabilities and measures to protect NATO deployed forces, territory and populations against the use of WMD as well as preventing proliferation. Therefore, the Alliance still seeks to prevent their proliferation through an active political agenda of arms control, disarmament and non-proliferation as well as by developing and harmonising defence capabilities. Moreover, regular consultations, information and intelligence sharing among Alliance members, partners, international organisations and national authorities, where appropriate, help foster a common understanding of potential WMD proliferation threats by States and non-State actors, emphasising the importance of the implementation and compliance with the Nuclear Non-Proliferation Treaty (NPT), Chemical Weapons Convention (CWC) and Biological and Toxin Weapons Convention (BWC), as well as relevant United Nations Security Council Resolutions such as UNSCR 1540[83]. Beyond the matter of prevention, a balanced mix of forces, response capabilities and strengthened defences is also needed in order to deter and defend against the use of WMD. Deterrence is conveyed through maintaining a credible overall deterrence posture as well as declaratory statements that, *inter alia*, demonstrate NATO cohesion. Robust passive defence and mitigation measures must be in place because of the potentially devastating consequences of WMD. Such measures enable NATO forces to continue effective military operations in a CBRN environment and allow appropriate civilian agencies to assist Allies and partners when WMD are used against them. Furthermore, Allies need to continue working to develop a proven ability to identify State responsibility through intelligence and forensic attribution in order to discourage any State from transferring nuclear weapons or technology to non-state actors. In practise, NATO and its Allies have significantly improved and are further improving the Alliance's CBRN defence posture with the establishment of the Weapons of Mass Destruction Centre (WMDC), the Combined Joint CBRN Defence Task Force (CJ-CBRND-TF), the Joint CBRN Defence Centre of Excellence (JCBRN Defence COE), the Defence Against Terrorism COE, and other COEs and agencies that support NATO's response to the WMD threat. The Allies have invested significant resources in warning and reporting, individual protection and CBRN hazard management capabilities. Despite all, capability shortfalls remain and are due, to some extent, to the limits of existing technologies and national capabilities among Alliance members. In this sense, the Alliance should seek to enhance capabilities that are critical to a robust CBRN defence, such as bio-detection and disease surveillance, by investing more national resources - when possible - to accelerate NATO's efforts within CBRN defence and by entering into partnerships for further research and development of innovative

[83] In resolution 1540 (2004), the Security Council decided that all States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes. The resolution requires all States to adopt and enforce appropriate laws to this effect as well as other effective measures to prevent the proliferation of these weapons and their means of delivery to non-State actors, in particular for terrorist purposes.

technologies and strategies. NATO should also continue assisting Allies with this development through training, advice, experimentation and concept development, and by considering ways to resolve funding issues. Finally, when efforts to prevent or defend against a WMD attack do not succeed, NATO must be fully prepared to recover from the consequences of WMD use against its members' populations, territory and forces and similarly to assist its partners, although the primary sovereign responsibility to prepare for and mitigate the consequences of CBRN event is of the allied governments. They are the first responders, and this is the reason why nations-state should have the full range of protective, medical, and remediation tools to identify, assess, and respond rapidly to such an event on home territory[84].

In the past, NATO managed to overcome great political shocks thanks to the political will of its member states. Currently, the Alliance's cohesion is challenged by Brexit, mass migration, financial fragility and trade wars. Some countries have an increasingly diverging approach to the political values and practices of the Alliance and the wave of neo-national thinking together with the rise of new anti-establishment parties in different democracies put into question the usefulness and the sense of international organisations[85]. This instability within and outside the Alliance is aggravated by ignored new phenomena, such as climate change. In fact, NATO does not directly address the matter of climate change, notwithstanding it is a factor that threaten security. In effect, as specified in chapter two, climate change could undermine livelihoods, increase migration, create political instability and weaken the resilience and capabilities of states to face threats appropriately. Thus, it has the potential to increase the need for humanitarian assistance and disaster response, to create tension over shared resources, to renew and enhance geo-political interest in the Arctic, and to deepen concern with respect to the Middle East and North Africa (MENA). As a result of this new political and environmental reality, NATO must consider how to adapt properly to meet new demands, also preparing itself to manage unforeseen consequences. If NATO would develop options to augment standing procedures and grapple with climate security risk, future crises could be met with *ad hoc* responses[86].

4.2. EU's Global Strategy

The EU is not a state and it cannot be defined as a major power in the traditional sense, especially due to its very limited ability to project military force. Since the beginning, the EU's foreign policy performance has been constrained by the lack of political unity, strategic thinking, common strategic culture and - despite the numerous European's efforts to move towards a post-Westphalian or post-sovereign conception of external affairs - member states still hold onto their sovereignty in this field.

[84] NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear (CBRN) Threats (2009)
[85] See Berti B. (June 2018: 41-43)
[86] See Lippert, Tyler H. (2016: 1-2)

Nonetheless, the EU has generated what can be called a "collective security strategy", complementary to the strategies of its individual member states. This European Global Strategy (EGS) was adopted in June 2016, at a moment when the Union's unity and even existence was being questioned more than ever before in its history. Such a strategy drew on a Strategic Review adopted in June 2015 and replaced the European Security Strategy of 2003. Its explicit purpose was to build a stronger union based on a "unity of purpose" (Mogherini F. 2016: 5), which is possible only increasing the legitimacy of the Union in front of its member states and citizens. The EGS reflects the perceived need for Europe, both inside the Union and outside among partners, to become a more capable foreign and security policy actor after decades of focusing on economic integration. It is clear that during the Cold War the US safeguarded security in Western Europe, whereas early efforts by the EU's predecessors to develop a common European security policy were thwarted. The previous European Security Strategy (ESS) was not a proper global strategy, but an *ad hoc* solution against the US war on terror launched after 9/11, which divided the Europe between countries that joined the US-led coalition for the invasion of Iraq (including the UK, Spain and Central and Eastern European countries), and a group opposing the Iraq war (led by Germany and France). Instead, the EGS is the response to the radical worsening of the EU's security environment. In this strategy, the common recognized five key threats, namely regional conflicts, state failure, organized crime, terrorism and WMD proliferation, were complemented by new ones, including military aggression by Russia against Ukraine, turmoil in North Africa and the Middle East, the concomitant migration crisis, global challenges like climate change and the so-called hybrid threats, including cyber-attacks, disinformation and election-meddling. Increased vulnerability and insecurity created a strong push for member states to seek unity in spite of their different national foreign and security policy priorities. Thus, the EGS explicitly rejects a realist worldview by stressing the EU's commitment to a win-win approach and stresses its openness to partnering with a wide range of actors, including states but also civil society actors and the private sector. As a result, today the EU is probably the most strongly rules-based entity that goes beyond the nation-state, challenging the state-centric view of international relations. Nonetheless, while the EGS expresses strong continuity in terms of the EU's understanding of a (preferred) global order, it also indicates a clear shift when it comes to the assessment of the regional security situation and subsequent European response. Indeed, the strategy expresses a heightened sense of insecurity, which necessitates a new focus on self-protection[87]. The main concerns become external threats coming from the neighbourhood, the East and South, including terrorism, hybrid threats, economic volatility and energy insecurity that "endanger our people and territory" (European Global Strategy 2016: 9). In response, the strategy identifies three core tasks for the EU in the field of security[88]:

[87] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 54)

[88] See European Global Strategy (2016: 9-11)

1. responding to external conflicts and crises;
2. building the capacities of partners;
3. protecting the Union and its citizens.

Thus, the EU's attention has shifted from projecting stability beyond the Union's borders to defending oneself against external instability. In comparison to the earlier strongly value-based agenda aimed at transforming the neighbourhood and beyond, the EU has become less idealist and more inward-looking. This is the result of the intensified global contestation over values and the emergence of new security threats, which has led to a debate about the continued relevance of an idealist, liberal value-oriented approach. Thus, the promotion of values such as democracy, the rule of law and human rights have lost its central place, acquired a more defensive dimension. Therefore, the EGS tries to find a new balance between idealist goals and what appears to be an increasingly realist world. The increased instability in the neighbourhood is one of the main factors that have led to a reconsideration of the EU's approach. This new approach focuses on improving the resilience of neighbours and helping them build up their own capabilities for improving security. At the same time, the increased concern about defending the EU's own territory and citizens has necessitated the rise of military aspects of security on the EU agenda. The importance of strengthening European defence, including military capability, is underlined in the strategy and has been a key priority in the implementation process. This marks a clear shift from the 2003 strategy where military capability played a marginal role and the EU aspired to develop non-military aspects of security, such as addressing the root causes of conflicts and promoting dialogue, a less state-centric approach, socio-economic development, respect for human rights and sustainable climate policies[89].

Regarding climate policies, the EU continues to address its main causes and it is currently strengthening the European response in the framework of the Paris Agreement. The commitment of the EU and its Member States to swiftly and fully implement the Paris Agreement has been reaffirmed in June 2017 by the European Council and then, in March 2018, the European Commission was invited by the Council to present a proposal for a long-term EU strategy to address greenhouse gas emissions reduction, taking into account its members' national plans. The Strategy opens a thorough debate involving European decision-makers and citizens about the 2050 horizon and the potential submission of the European long-term Strategy to the UN Framework Convention on Climate Change by 2020. The proposed Strategy does not intend to launch new policies, nor does the European Commission intend to revise 2030 targets[90], which are:

[89] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 56-59)

[90] See European Council (October 2014).

- At least 40 percent cuts in greenhouse gas emissions (from 1990 levels);
- At least 32 percent share for renewable energy
- At least 32.5 percent improvement in energy efficiency

The EU, responsible for 10 percent of global greenhouse gas emissions, remains a global leader in the transition towards a net-zero-greenhouse gas emissions economy. The EU have already set its objective in 2009 to reduce emissions of 80-95 percent by 2050. Europeans have managed to successfully decouple greenhouse gas emissions from economic growth in Europe for the past decades and this clean energy transition has spurred the modernization of the European economy, driven sustainable economic growth and brought strong societal and environmental benefits for European citizens. Unfortunately, this is not enough to achieve the Paris Agreement's temperature goals worldwide. Indeed, in the second chapter, it has been pointed out that the world needs to limit climate change to 1.5°C to reduce the likelihood of extreme weather events. It has also emphasized that emissions need to be reduced with far more urgency than previously anticipated. In order to limit temperature increase to 1.5°C, net-zero CO2 emissions at global level needs to be achieved around 2050, together with neutrality for all other greenhouse gases. Therefore, the Strategy outlines a vision of economic and societal transformations, engaging all sectors of the economy and society for such a purpose. It seeks to ensure that this transition will be socially fair - not leaving any EU citizens or regions behind - and will enhance the competitiveness of EU economy and industry on global markets, securing high quality jobs and sustainable growth in Europe while providing synergies with other environmental challenges, such as air quality or biodiversity loss. The road to a net-zero greenhouse gas economy could be based on joint action along a set of seven main strategic building blocks[91]:

1. Maximise the benefits from Energy Efficiency including zero emission buildings;
2. Maximise the deployment of renewables and the use of electricity to fully decarbonize Europe’s energy supply;
3. Embrace clean, safe and connected mobility;
4. A competitive EU industry and the circular economy as a key enabler to reduce greenhouse gas emissions;
5. Develop an adequate smart network infrastructure and inter-connections;
6. Reap the full benefits of bio-economy and create essential carbon sinks;
7. Tackle remaining CO2 emissions with carbon capture and storage.

[91] See COM/2018/773 final.

Reaching this objective requires deep societal and economic transformations within a generation touching every sector of the economy. Some example of required actions is drafted in the following table:

Accelerate the clean energy transition, ramping up renewable energy production, high energy-efficiency and improved security of supply - with increased focus on reducing cyber security threats - while ensuring competitive energy prices, all of which power the modernization of our economy.
Recognize and strengthen the central role of citizens and consumers in the energy transition, foster and support consumer choices reducing climate impact and reap collateral societal benefits improving their quality of life.
Roll out carbon-free, connected and automated road-transport mobility; promote multi-modality and shifts towards low-carbon modes such as rail and waterborne transport; restructure transport charges and taxes to reflect infrastructure and external costs; tackle aviation and shipping emissions using advanced technologies and fuels; invest in modern mobility infrastructure and recognize the role of better urban planning.
Increase the EU's industrial competitiveness through research and innovation towards a digitalized and circular economy that limits the rise of new material dependencies; start testing at scale breakthrough technologies; monitor the implications on the EU's terms of trade, in particular for the energy intensive industries and suppliers of low carbon solutions, ensure competitive markets that attracts low carbon industries, and in line with international obligations alleviate competitive pressures that could lead to carbon leakage and unwanted industrial relocation.
Promote a sustainable bioeconomy, diversify agriculture, animal farming, aquaculture and forestry production, further increasing productivity while also adapting to climate change itself, preserve and restore ecosystems, and ensure sustainable use and management of natural land and aquatic and marine resources.
Strengthen infrastructure and make it climate proof. Adapt through smart digital and cyber-secure solutions to the future needs of electricity, gas, heating and other grids allowing for sectoral integration starting at local level and with the main industrial/energy clusters.
Accelerate near-term research, innovation and entrepreneurship in a wide portfolio of zero-carbon solutions, reinforcing the EU's global leadership.
Mobilize and orient sustainable finance, invest in green infrastructure and minimize stranded assets as well as fully exploit the potential of the Single Market.

Invest in human capital in the next decade and beyond, equip current and future generations with the best education and training in the necessary skills (including on green and digital technologies) with training systems that quickly react to changing job requirements.
Align important growth-enhancing and supporting policies, such as competition, labour market, skills, cohesion policy, taxation and other structural policies, with climate action and energy policy.
Ensure that the transition is socially fair. Coordinate policies at EU level with those of Member States, regional and local governments allowing for a well-managed and just transition that leaves no region, no community and no worker and citizen behind.
Continue the EU's international efforts to bring all other major and emerging economies on board and continue creating a positive momentum to enhance global climate ambition; share knowledge and experience in developing long-term strategies and implementing efficient policies so that collectively the objectives of the Paris Agreement are accomplished. Anticipate and prepare for geopolitical shifts, including migratory pressure, and strengthen bilateral and multilateral partnerships, for instance by providing support to third countries in defining low-carbon resilient development through climate mainstreaming and investments.

[Source: COM/2018/773 final.]

Member states have had to submit by the end of 2018 to the European Commission their draft National Climate and Energy Plans, which are central for the achievement of the 2030 climate and energy targets and which should be forward-looking and taken into account in the EU long term strategy. In addition, an increasing number of regions, municipalities and business associations are drawing up their own vision for 2050, which will enrich the debate and contribute to defining Europe's answer to the global challenge of climate change. Thus, the matter of climate change is one of the few exceptions requiring the EU's soft power in its new security approach. In effect, the other threats demand progress in the field of defence cooperation, especially in the case of cybersecurity[92]. To date, attacks perpetrated by means of ransomware have tripled since 2015, the economic impact of cyber-crime has increased fivefold between 2013 and 2017 and 87 percent of European citizens consider cyber-attacks as one of the great challenges for the EU internal security[93]. These challenges extend beyond national borders and have an impact not only on security and stability but also on the economy and the safeguarding of the democratic order. Security incidents, such as technical failures and viruses that can affect information and communication systems, are becoming more frequent and difficult to manage, undermining businesses and public services functionalities alongside consumer confidence. The first

[92] See EGS (June 2018: 14)

[93] See European Commission Data (2017)

EU-wide cyber-security rules was adopted by the Council in May 2016 and by the European Parliament in July 2016, coming into force a month later. This European directive, called NIS (Network and Information Security), aims to increase cooperation between Member States on vital cybersecurity question and define security obligations for operators of essential services (in critical sectors such as energy, transport, health and finance) and digital service providers (i.e. online markets, search engines and cloud services). In addition, according to such a system, each EU country should have appointed one or more national authorities and a proper cyber-strategy. Today, a further increase in cyber-attacks has led the EU to raise awareness and response among its Member States and European institutions. Thus, the Council have adopted a new cybersecurity regulation on April 9th, 2019 to introduce a set of certification systems at EU level, which is a series of rules, technical requirements and procedures capable of reducing market fragmentation, eliminating regulatory obstacles and establishing a climate of trust, and a new EU cybersecurity agency, that updates and replaces the current European Union Network and Information Security Agency (ENISA). The set of certification systems would be applied in all Member States, facilitating cross-border business exchanges and the new cybersecurity agency would have a permanent status and a more incisive role in the cyber sector[94].

Moreover, as part of the cybersecurity reform, the EU institutions is promoting a legislation that would create the Industrial, Technological and Research Centre on cyber security - supported by a network of national coordination centres - to secure the digital single market and increase EU autonomy in the sector. In the meanwhile, the EU is working on cross-cutting measures that address cyber threats in different sectors. For example:

- the fight against organized cyber-crime, which is going to be one of the top ten priorities for the 2018-2021 period;
- achieving the objectives of the common foreign and security policy discouraging cyber- attacks;
- updating the EU cyber defence framework.

In the field of cyber-defence, the Commission had already presented a comprehensive cybersecurity package in September 2017 to improve resilience, detection and response to threats. It includes also a “cyber diplomacy toolbox”, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations, and the European support in several cyber exercises such as PACE17, Cyber-Europe as well as the CYBRID exercise. The EU has further strengthened its cyber dialogues with the US, Japan, India, South Korea, Brazil and China and works closely with other international organizations, such as NATO, the ASEAN Regional Forum, the OSCE, and the Council of Europe[95].

[94] See European Parliament No 526/2013 (April 2019)

[95] See EGS (June 2018: 15)

Beyond the specific topic of cyber, a more credible European defence is considered essential for internal and external security. New mechanisms were created to allow Member States and the EU to face new threats and challenges. For instance, on December 14th, 2017 the Permanent Structured Cooperation on defence (PESCO) was launched. This is an opportunity provided for in the Lisbon Treaty ten years ago but never used until now. Twenty-five Member States have committed to join forces on common projects, to provide troops and assets for common missions and operations. They also committed to speed-up their national decision-making and share information among them to improve the ability to counter threats by stepping up maritime surveillance, cyber information sharing and military disaster relief. Seventeen concrete projects have already been launched and this form of cooperation should guarantee more effectiveness on the ground and less monetary expenses. Along with this, on June 12th, 2018, the Commission has proposed a much more ambitious European Defence Fund (EDF). In other words, for the first time the European budget contains a specific line for defence, and it is implemented by a specific Fund to complement Member States' investment in the field. The EDF is endowed with 13 billion euro to enhance collaborative research projects and co-fund capability development. This is a true European instrument to enhance EU strategic autonomy[96].

Overall, the EU is taking little steps to maintain and enhance security in the region, fighting global challenges that can provoke instability. Even in the field of biological threat the EU adopted in January 2019 a new Council Decision to support the Biological and Toxin Weapons Convention (BTWC). Indeed, during the launch of such a decision in March 2019, the Ambassador Walter Stevens, Head of the EU Delegation to the UN, stated that "the threat of proliferation of biological and toxin weapons remains real in light of rapid advancements in life sciences. Thus, the European Union will remain vigilant and will ensure good governance structures, namely legislation, administration, judicial systems and law enforcement, to minimize the risk of malicious use of pathogens or toxins and respond quickly to them"[97]. In this field, the EU supports the Biological and Toxin Weapons Convention since 2006, in order to promote the adherence of its member states. Today, with the new EGS focused on defence, it is easier for the EU not only to organise regional workshops, but also provide expert assistance in strengthening national legislation to improve biosecurity in laboratories and plan emergency response to possible biothreats.

To sum up, the increased global insecurity and instability has provoked a certain anxiety both in the Union and in its member states, which has been reflected in the new EGS. Despite the EU's vision of the world order can still be characterized as liberal idealist, stressing the importance of multilateralism and rules-based cooperation, the rising global contestation between major powers as well as violent conflicts in nearby regions

[96] See EGS (June 2018:15-16)

[97] See Council Decision (CFSP) 2019/97 (January 2019)

to the EU's east and south have pushed the Union towards a more realist and defensive approach to the outside world[98].

4.3. SCO: the Shanghai convention on fight against terrorism, separatism and extremism

The forms taken by multilateralism in the area of the former Soviet Union have been particularly little studied. There is a widespread assumption in the West that, because they involve imperfectly democratic states and often reject externally defined norms of governance, such groups are bound to be illegitimate or ineffective or both. One of the world's least-known and least-analysed multilateral groups is the Shanghai Cooperation Organization (SCO), which has been established in 2001 by China, the Russian Federation, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. The SCO Charter, adopted in June 2002, lists several basic principles of international law as the foundations of the organization, including the sovereign equality of states and the rejection of hegemony and coercion in international affairs. Such SCO's norms - referred to as the 'Shanghai spirit'- differ from the United Nations Charter in term of respect for human rights and the self-determination of peoples[99]. Moreover, the SCO was designed essentially as an intergovernmental network led by annual summits and by regular meetings of the heads of government, foreign ministers and other high officials of the member states. Security-relevant areas are the most frequent subjects of working-level meetings, which include experts on information security, secretaries of national security councils and heads of supreme courts. Indeed, its deeper goals include managing potential Sino-Russian tensions or competition, handling economic and infrastructure cooperation and, above all, transnational threats.

To understand SCO's approach against traditional and new threats it is necessary to retrace its institutional development, in which this entity matured from an *ad hoc* arms control grouping via emphasis on internal security to an international organization with a variety of cooperation and activities. It can be divided into three phases[100]:

1. Confidence and security building measures (1996-2001)
2. Regional security against the three evils (2001-2004)
3. Comprehensive international organization (2004-present)

In November 1992, China, Russia, Kazakhstan, Kyrgyzstan and Tajikistan started security negotiations, based on the basic need of diminishing possible tensions at the borders after the end of Cold War.

[98] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 59)

[99] See Bailes, A. J. K., Dunay, P., Guang P. and Troitskiy, M. (May 2007: 5-6)

[100] See De Haas M. and Van der Putter F. (November 2007: 7-10)

In 1996 and 1997, the heads of states, at their meetings in Shanghai and Moscow respectively, signed an "Agreement on deepening military trust in border regions" and an "Agreement on reduction of military forces in border regions", which became an important historical stage and resulted in launching the "Shanghai Five mechanism". This resulted in annual meetings, held alternately in each of the five countries, to strengthen good-neighbour relations of mutual trust, friendship and cooperation among the five countries.

Next, the members of the Shanghai Five together with Uzbekistan decided to lift such a mechanism to a higher level, in order to make it a stronger base for developing cooperation among the six states under new conditions. On June 15th, 2001 in Shanghai the Heads of these six states signed the "Declaration on Establishment of the Shanghai Cooperation Organization", creating a new organization of regional cooperation. During this meeting "The Shanghai convention on fight against terrorism, separatism and extremism" was also signed. After diminishing military tensions and by creating mutual trust, friendship and cooperation, this convention against the so-called "three evils" (i.e. terrorism, separatism and extremism), marked the next phase in development of the SCO. It established a common understanding between the parties on what these terms mean and commits them to reciprocally extradite persons committing such crimes. Moreover, the members cooperated through the exchange of information and intelligence, by meeting requests for help in operational search actions, in developing and implementing measures to prevent, identify and suppress offending actions and in collaborating to stop the flow of finance and equipment for the guilty parties. Then, the year 2004 saw the completion of the institutional phase with the establishment of two permanent organs, namely a Secretariat in Beijing and a Regional Anti-Terrorist Structure (RATS) in Tashkent, Uzbekistan. Furthermore, Mongolia joined as the first SCO observer.

Thus, until 2004 the SCO mainly dealt with regional security. Gradually, the SCO changed from a purely regional outlook into an organization seeking international recognition and cooperation. In 2004 the SCO received an observer status at the UN and the next year its Secretary-General was allowed to make a speech to the UN General Assembly. Additionally, the SCO has signed Memoranda of Understanding with the Association of Southeast Asian Nations (ASEAN) and with the Commonwealth of Independent States (CIS). At the Summit of July 2005 in Astana, Kazakhstan, the SCO seemed to proclaim a radical change of course. Indeed, in the previous years, the governments of the Central Asian member states (especially Uzbekistan) - facing the Western backed regime changes in Georgia (2003) and Ukraine (2004) and another change of government in Kyrgyzstan (2005) - saw their existence threatened by the Western countries. This situation forced them to diminish their (economically favourable) relationship with the West. This led to a final statement of the SCO members, in which (US) unipolar and dominating policies, as well as foreign military deployment in Central Asia, were condemned and the withdrawal of Western military troops encouraged. In addition to Mongolia, in July 2005 Iran, Pakistan and India joined the SCO as observers. The joining of the "rogue state" Iran as observer as well as the offensive orientated "Peace Mission 2005" military exercises of August 2005, made some Western media described SCO as an anti-Western security organization, a sort of "NATO of the East".

Nonetheless, as a proper security organization, the SCO still lacks a considerable number of essential features, such as an integrated military-political structure with permanent operational headquarters, a rapid reaction force and continuous political deliberations. This is one of the reasons why, the SCO has never characterized itself as a traditional military alliance comparable to NATO and it has not even tried to claim a role in mounting active multilateral peace operations in its own region or outside. Indeed, it would be impossible to imagine Russia guaranteeing China's entire territory against attack and vice versa, let Chinese and Russian forces - and potentially their nuclear weapons - be brought under a single command with joint force goals[101].

In addition, the condition *sine qua non* to guarantee an effective regional security cooperation is to serve at least some common interest, not handicapping it in the pursuit of individual ones. In SCO, differences in strategic position and influence are most obvious between, on the one hand, the two large and potentially global powers - China and Russia - and the four Central Asian members on the other. The latter are not only far smaller but are also landlocked and have few fields of action beyond the regional. Within the group of four, Kazakhstan's and Uzbekistan's oil and gas and their size place them in a different category from Kyrgyzstan and Tajikistan. China and Russia, for their part, are linked by their status as nuclear weapon states, permanent membership of the UN Security Council and long experience of Communist rule. Possible divergent objectives are found between Kazakhstan and Uzbekistan, rivals for regional primacy, between observers India and Pakistan, after a long-time antagonist relation, and in Iran's support of extreme Islamists, which may result in a threat to the national security of one or more Central Asian states. Moreover, it is undeniable that the two leading countries, namely Russia and China, pursue different interests[102].

The core Chinese national interest is the survival of its current regime and, as main precondition to regime survival, the maintaining of its domestic political legitimacy. The government intends to maintain its political legitimacy performing a number of basic tasks, among which protecting China's economic development, territorial integrity, and national sovereignty are the most important. China's grand strategy combines these various interests, as it aims at achieving international prominence and gaining international support through various kinds of partnerships with other countries, while avoiding direct confrontations with any great power. This strategy maximizes access to the global economy, while minimizing the risk of foreign military threats, and thus provides the best guarantee for the Communist regime's political survival[103].

[101] See De Haas M. and Van der Putter F. (November 2007: 13-14)

[102] See Bailes, A. J. K., Dunay, P., Guang P. and Troitskiy, M. (May 2007: 8)

[103] See Bailes, A. J. K., Dunay, P., Guang P. and Troitskiy, M. (May 2007: 13-14)

In "the priority tasks of the development of the Armed Forces of the Russian Federation", a security policy document published by the Kremlin in October 2003, the SCO for the first time was described as an important organization for regional stability in Central Asia and the Far East, especially in countering military threats. For Russia, the SCO apparently acts as a means to bring together different policy objectives. Not only China, but India and Iran as well have a special (economic) relationship with Russia. All three states are important actors in Russia's arms export. In addition to this, China and India are gaining a closer relationship with Russia in the field of joint, bilateral military exercises. Therefore, the fact that India and Iran have joined China in its cooperation with Russia within the SCO, could prove that the SCO serves as a platform for Russia's security policy. Another example of the SCO being used towards this end is the fact that it was Russian President Putin who instigated the foundation of an energy club within the SCO. This fits in Russia's policy of using energy as a power tool. Moreover, Russia will use this organization to reduce Western (US) influence in its backyard of Central Asia, which was accomplished in the aftermath of 9/11. In such a way, supported by China's rising power status, the SCO serves Russia as a vital instrument to achieve geopolitical objectives[104].

Besides the national interests of SCO's leading countries, the SCO has developed itself towards a truly international entity. The aforementioned evolution indicates a closer cooperation in the field of security and the enhancement of a SCO military cooperation. The dimension where the SCO has worked hardest to establish its profile and expand its activities is that of combating first and foremost terrorism, separatism and extremism, but also dealing with universal problems such as drug trafficking, cyber-sabotage and aspects of weapons of mass destruction (WMD) proliferation.

Recently, one of the main SCO's concerns in this field is the "information security". In line with Chinese and Russian security visions, the SCO proposes information security as an equivalent to what Westerners call "cybersecurity" and drafted the Agreement on the Information Security Area in 2009, following the repercussion of cyber-attacks in Estonia (2007) and during the conflict in Georgia (2008). Such an agreement identifies the following threats:

- The development and use of weapons of information and preparation to undertake information warfare;
- information terrorism;
- information crime;
- use of dominant position in cyberspace to the detriment of interests and security of other states;
- dissemination of information harmful to political systems;

[104] See Bailes, A. J. K., Dunay, P., Guang P. and Troitskiy, M. (May 2007: 10-12)

- natural and/or human threats to safe and stable operations of the global and national information infrastructure (SCO 2009: 203).

The SCO's principles of respect to sovereignty, non-interference in the internal affairs of states, equality and mutual respect in the fulfilment of international norms and the fight against the three evils to the cyber realm, are embodied in this Agreement. In addition to the ideas of the SCO embedded in these perceptions, a criticism is made against the Internet governance pattern centred in the United States. Consequently, four members of the SCO (i.e., China, Russia, Tajikistan, and Uzbekistan) presented a draft International Code of Conduct for Information Security to the United Nations General Assembly (i.e. A66/359) on September 12th, 2011, but it was rejected. Four years later six SCO members presented a new draft of the code to the UN General Assembly (i.e., A69/723), which was rejected again. This rejection was given based on a perception of an excessive state control for cyberspace in SCO members view. Indeed, information security is a proposal that seems to rebound the Soviet collective memory of the need for a strong and centralized power since it is up to the State to secure the content of cyberspace. Therefore, even if in the eyes of the East this would be the best way to balance the cyberspace, this fact could lead to a possible breach of international rights in relation to freedom of expression and privacy.

It is interesting to note that there is a clash of Sino-Russian influences on the Asian region reaching the cyber arena, but in a complementary way. In fact, information security remains a priority for both of them because of its implications in the energy and transport infrastructures that interconnect the region. Thus, SCO has demonstrated its flexibility and adaptiveness to the cyber rapid growth, creating new mechanisms and being on the forefront to manage the Internet's impact on governments, specifically to counter its use for what it calls information terrorism[105].

Nevertheless, the SCO agenda remains tightly focused on conflict avoidance and peaceful dialogue among its members[106]. Indeed, the Shanghai Cooperation Organization address threats only if affecting directly the stability between its member states, such as in the case of cyber-threats and WMD (only in the field of nuclear proliferation), ignoring relevant global menaces like global warming. Furthermore, the SCO has frequently been criticized for the lack of political will and internal cohesion, for the institutional weaknesses resulting in the gap between initiatives announced and their actual implementation and its slim record of achievements. For example, in 2012, SCO leaders approved a new non-military collective response mechanism for responding to situations that put peace, security and stability in the region at risk which theoretically allows SCO members to intervene politically and diplomatically in other SCO members in case of internal conflicts. This new mechanism has not yet been tested. This discrepancy between SCO objectives

[105] See Toso de Alcântara B. (October 2018: 552-553)

[106] See De Haas M. and Van der Putter F. (November 2007: 57-59)

and principles on the one hand, and SCO members' action on the other, severely undermines the SCO's credibility and image. An emblematic example is the condemnation of Russian invasion of Georgia in 2008 by SCO’s members but their silence about Russia's 2014 annexation of Crimea

Taking everything into account, analysts argue that the SCO's traditional and non-traditional security cooperation must be improved[107].

4.4. UN: 2018 Report of the Secretary-General on the work of the Organization

In the 2018 Report of the Secretary-General of United Nations (UN) Antonio Guterres, it is expressed the awareness about the difficulties of the global current situation, due to an increase in conflict with grave violations of human rights and humanitarian law, the risen inequality, intolerance and discrimination against women and the impact of climate change.

The primary responsible for the maintenance of international peace and security within UN’s structure is the Security Council (UNSC). Composed by has fifteen members, of which five permanents, the Security Council takes the lead in determining the existence of a threat to the peace or act of aggression, calls upon the parties to a dispute to settle it by peaceful means and recommends methods of adjustment. In some cases, the Security Council can resort to imposing sanctions or even authorize the use of force to maintain or restore international peace and security. Its decisions are binding on UN members but, the lack of an actual binding, legal oversight mechanism makes Security Council’s efforts problematic. Another limitation of such organ is the power of veto. The power of veto is held by the five permanent members of the UN Security Council, i.e. China, France, Russia, United Kingdom and United States, and gives them the ability to block any “substantive” resolution (at the same time, the five permanent members decide which issues deserve this title). This rule not only prevents much needed international action from taking place, but it also undermines the entire basis of the UN, which is international cooperation. International cooperation can be obtained only through unity and solidarity between countries, going beyond national interests to address global issues. This is the proper way to adopt a wide range of reforms which can set the world on track towards a better future.

To date, UN have made progress in some area, but elsewhere complex crises continue to elude solutions. Among the threats which require a global response, the 2018 UN Report recognize the following[108]:

- The expansion of new technological frontiers, namely artificial intelligence, genetic engineering and advances in cyberspace.
- The impacts of climate change.

[107] See European Parliament Briefing (June 2015: 9)
[108] See Guterres A. (2018: 3-4)

- The threat of the use of weapons of mass destruction, especially the rise of chemical and biological weapons.
- Terrorism, which is becoming a worldwide scourge and thus requires a globally coordinated response.

Global strategies against them include building partnerships among Member States, regional and international organizations, and civil society to share ideas and actions and promote burden-sharing. As high priority, the UN recognize prevention, which requires not only an understanding of the dynamics that lead to crises, but the will to act early even in the face of uncertainty[109]. "Prevention" is first and foremost about supporting efforts by national governments and populations to make full use of the gamut of United Nations tools and programs. At the High-level meeting on Peacebuilding and Sustaining Peace, held in April 2018, Member States reiterated their support for precisely an holistic and coordinated approach across the United Nations which, through the creation of an integrated regional structure and a more effective positioning of the Peacebuilding Support Office, aim to achieve coordination across the three pillars of peace and security, sustainable development and human rights in support of prevention. Besides the prevention, missions on the ground remain critical tools in preventing conflict and sustaining peace. Indeed, peacekeeping missions are increasingly operating in deteriorating security environments encompassing asymmetric threats, transnational organized crime and regionalized conflicts, without clear trajectories for political progress. Thus, UN are strengthening its internal arrangements to ensure the proper response to such security threats, taking into account the need to implement their tasks in the absence of viable political processes and maintain the protection of civilians as a priority. As a result, United Nations peacekeeping missions have developed new tools, such as a new framework on accountability to lay out clearer responsibilities for both civilian and uniformed personnel. In addition, steps to improve performance have been taken, such as receiving new military and police pledges, enhancing triangular partnerships between Member States with expertise, troop and police and critical skills of UN operations in engineering, signals and command and control. Moreover, personnel have been better trained and equipped to face high-risk environments, including to improvise explosive device risk mitigation against asymmetric threats. Thanks to these advances, UN can better fit units to operating environments and identify opportunities to fill training and capability gaps[110].

Another key aspect of UN security strategy to preserve human security is "disarmament". The disarmament agenda, announced on May 24th, 2018, sets out concrete actions especially against the proliferation of WMD. While nuclear tensions may have lessened between the USA and the Democratic People's Republic of Korea, the continuing existence of nuclear weapons remains a concern, as well as the use of chemical weapons in the Syrian Arab Republic and the risk of biological weapons proliferation (plus

[109] See Guterres A. (2018: 7)

[110] See Guterres A. (2018: 28)

the potential arise of bio-terrorism). The UN disarmament agenda aims at saving lives and ensuring a safer world for future generations. As main instruments have been identified: arms control, non-proliferation, prohibitions, restrictions, confidence-building measures and even elimination when called for. The Treaty on the Non-Proliferation of Nuclear Weapons is the cornerstone of the nuclear disarmament and non-proliferation regime and, since nuclear disarmament is vital for national, regional and international security, UN works to facilitate dialogue and ensure the Treaty's continuing health and vitality, especially in the lead-up to the 2020 Review Conference, the 50th anniversary of its entry into force. Beyond nuclear proliferation, also the continuing use of chemical weapons is becoming problematic. The repeated breach of this taboo is exacerbated by the environment of impunity, following the termination of the Organization for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism in November 2017. The UN have repeatedly advocated for the establishment of an independent, impartial and professional attribution mechanism. This is even more troubling in the field of biological weapons. In fact, it is undeniable that developments in science and technology bring benefits, but there are also collateral effects. In particular, such knowledge would be dangerous if acquired by malicious actors, like terrorist groups. The UN Secretary General has pointed out the need to report current developments in science and technology and their potential impact on international security, to increase awareness and response capability[111]. Then a spectrum of responses and multi-stakeholder coalitions will be required to meet all the new potential challenges. This is true especially dealing with cyber threats and climate change effects.

Regarding cybersecurity, the challenge is to reap the benefits of these rapidly developing technologies while protecting against unintended consequences and the dark side of technological advances. In the UN framework, considerable progress has been made on the issue by several groups of governmental experts with respect to the application of international law, cyber norms, rules and principles of responsible State behaviour, and confidence-building and capacity-building measures. To enhance understanding of frontier technology issues, the Office for Disarmament Affairs has developed an online training course for diplomats and all interested stakeholders, released in October 2018. The last year, the International Telecommunication Union, which is a specialized UN agency since 1947, released a document called "National Cyber-security strategy" with the aim to guide national leaders and policymakers in the development of a National Cybersecurity Strategy and in thinking strategically about cybersecurity, cyber-preparedness and resilience. This guide is one of the most comprehensive overviews of what constitute successful cybersecurity strategies and it is the result of a unique, collaborative and equitable multi-stakeholder effort, which taps into the knowledge, experience and expertise of many organizations in the field. Specifically, this Guide has been produced by twelve partners from public and private sectors, as well as academia and civil society. Among them, there are the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), RAND Europe, The World

[111] See Guterres A. (2018: 64-65)

Bank, the United Nations Conference on Trade and Development (UNCTAD) and the contribution of the European Union Agency for Network and Information Security (ENISA). Such a Guide is based on the ITU Global Cybersecurity Agenda (GCA), launched by the former ITU Secretary-General, Dr. Hamadoun I. Touré (2007 -2014) in 2007. This Agenda is a framework for international cooperation aimed at enhancing confidence and security in the information society, designed to guarantee cooperation and efficiency and avoid duplicating efforts through the collaboration with and between all relevant partners. The GCA is built upon five strategic pillars, also known as work areas, which are Legal Measures, Technical & Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. These areas have been also the basis of the Global Cyber-Security Index (GCI)[112], established by ITU in November 2018, because they shape the inherent building blocks of a national cybersecurity culture[113].

With respect to climate change, UN Report highlights that global warming is being felt throughout the world and today represent a true existential threat. Indeed, scientists have confirmed the strong human influence on the climate ecosystem, and a worsening of its effects worldwide. Among these effects, the UN Secretary General recognizes the rising sea levels, which threaten coastal cities, low-lying island nations and vulnerable deltas, and a potential ice-free summer in the Artic, with devastating repercussions for indigenous peoples and sea life. Thus, the UN claims the need to increase ambition to bend the emission curve by 2020. The Paris Agreement on climate change is already an important expression of collective commitment to limit the rise in global temperature to well below 2 degrees Celsius and as close as possible to 1.5 degrees. However, efforts at lower level are still necessary. For instance, the countries need to turn pledges into national climate action and cities, regions, territories and private entities must contribute by setting their own ambitious targets[114]. With the aim to bring climate action to the top of the international agenda, a Climate Action Summit will be held in September 2019 by the UN Secretary-General. This Summit will focus on the heart of the problem - the sectors that create the most emissions and the areas where building resilience could make the biggest difference - and it will provide the opportunity for leaders and partners to demonstrate real climate action and showcase their ambition[115].

Taking everything into account, UN has initiated a broad set of reforms to strengthen the effectiveness of the Organization and ensure cross-pillar communication. Such reforms of the peace and security architecture are aimed at ensuring a stronger prevention, agility in mediation, and effectiveness (also cost-effectiveness) in UN operations, joining up topics and approaches that have often been isolated silos. As a

[112] The GCI is an innovative and useful tool to monitor and compare the level of the cybersecurity commitment of countries.

[113] International Telecommunication Union (2018: 5-8)

[114] See Guterres A. (2018: 3-4)

[115] See UN official web site: https://www.un.org/sustainabledevelopment/climate-change/

result, UN security system is becoming much more effective, well-coordinated transparent and accountable, ready to better assist countries in implementing their capabilities to face new threats.

In conclusion, the United Nations - aware of the structural difficulty in achieving its goal - need to continue to innovate and adapt to changing challenges, enhancing in the meanwhile internal cohesion. In the spirit of the its Charter' principles, UN should make the prevention of crises, vulnerabilities and conflicts its highest priority to save succeeding generations from the scourge of war[116].

[116] See Guterres A. (2018: 72)

Chapter 5. The Italian security response

In 2018, Italy has faced a volatile security environment characterized by instability and weaknesses. Such instability and weakness have led to a long series of controversies, culminated with the favorable vote of both the Chamber of Deputies and the Senate of the so-called "Security Decree". The Security Decree, which has been already approved and published on the Official Gazette, is a package of measures wanted by the Italian Minister of the Interior, Matteo Salvini about some delicate issues such as terrorism, the fight against mafias and public security. It includes also a part entirely focused on immigration. This last part is the most troubling, because it makes difficult for asylum seekers to stay in Italy and limits the work of the NGOs operating in the rescue of migrants. Regarding the public order, the Decree provides a substantial increase in the power of the mayor, the prefect, the quaestor and the law enforcement, introducing also harsher measures, like the use of tasers by the police. This is the outcome of the Italians' perception of "threat", a view aggravated by an international environment where a competitive approach prevails on the cooperative one. The final result is the closure within the borders of the nation-state and a strict focus on domestic security rather than global one[117].

Despite this new nationalistic approach, it is undeniable that Italy remains an important actor in multilateral organizations, such as in the EU and UN. Hence, international documents have still an impact on Italian legislation, representing a solid framework for actions. This is evident in the work of Italian intelligence, expressed in the annual report "*Relazione sulla politica dell'informazione per la sicurezza*".

5.1. Relazione sulla politica dell'informazione per la sicurezza 2018

In the last year, the action of the Italian intelligence measured against multiple factors of instability and threat, which contributed to affect negatively national interests and safety. The Italian security report recognized a certain global instability and national individualisms that are affecting current international relations. This is the result, as emphasized in the preamble, of an unfair economic development and its political impact, namely pronounced imbalances, situation of marginality and, thus, incubator of profound resentments. These tensions are felt in emerging and less developed countries, which are fuelled by a narrative that continues to ascribe injustices and inequalities to an incurable conflict between the North and South of the world. Then, this resentment is exacerbated by the gradual reduction of the transatlantic community, embodied for example in the most assertive and unilateral posture pursued by the US administration. The affirmation of national individualisms strengthens the role of nation-states, whose governments however have much more

[117] See D.L. 113/2018 - A.C. 1346

limited means and margins of action than in the past. In this framework, it is difficult to find a unitary voice and position on delicate dossiers of common interest, such as cyber-threats, WMD proliferation and climate change effects. In this framework, the international role of organizations like the EU is perceived as weaker and subordinated to national interests, uncapable to enhance global trust to face new threats. The aforementioned weaknesses of the European front and the propensity of the USA to redesign the ambits and the scope of its own intervention assume particular importance in comparison with the proactivity shown by both Beijing and Moscow, determined to acquire, or to regain, a role of absolute centrality through the protection of their interests and their ability to seize opportunities for growth and development[118].

In this critical international scenario, the action of the Italian security and information systems remained, as in the past year, focused on the neighbourhood, i.e. Mediterranean and the Near East area, which is still marked by internal crises. The main Italian priority is Libya and its difficult stabilization process. Nonetheless, the control of the whole area that goes from Egypt to the Maghreb - which include the sub-Saharan regions of the Sahel, the Gulf of Guinea and the Horn of Africa - as well as the control of Syria and Iraq, is important to counter threats such as terrorism, organised crime, illegal immigration and narcotics. Moreover, the Italian intelligence monitors all the territories affected by jihadist threat, such as Afghanistan and Pakistan, and by illegal immigration, focusing on criminals that manage the traffic and the possible linkage between illegal migratory movements and terrorism[119].

Regarding jihadist threat, it is assuming an international façade, especially due to DAESH propaganda. DAESH is making its propaganda through a series of official and non-official dedicated sites, repeatedly praising the commitment on the ground and transmitting operational suggestions online, aimed to attract autonomous and extemporaneous soldiers. In particular, since 2018 such a propaganda instigates to experiment new weapons, such as drones and chemical and biological substances, to conduct terrorist attacks in the West. The issue of using chemical and biological agents to hit the West has been emphasized in an ad hoc editorial, called “Silent terror. Kill them silently”, inaugurated at the beginning of August 2018 by the pro-DAESH channel “at the Saqri Institute of War Sciences”. This editorial explains the passages necessary for the retrieval, production and use of biological and chemical agents, including hydrogen phosphate, cyanide and botulinum toxin. In addition, the series is accompanied by real motivational steps aimed at persuading the potential mujahidin of the legitimacy of the use of these operating methods[120]. Despite it recognizes the risk of bioterrorism, Italian security strategies have not recently addressed the topic of WMD, at least not in a direct way.

[118] See Relazione sulla politica dell’informazione per la sicurezza (2018: 7-16)

[119] See Ibid (20-21)

[120] See Relazione sulla politica dell’informazione per la sicurezza (2018: 83)

Then, after having described all the potentially dangerous scenarios in the neighbourhood, the Italian Report focused on economic stability. Indeed, Italy still suffers for the problems accumulated during the economic crisis and needs a strong commitment to safeguard the country's financial stability and its credit system. In this field, latent menaces like the energy procurement and the growing role of new technologies is provoking further concerns for Italians, so much to deserve intelligence's attention. Taking into account the energy procurement, Italy's priority is to maintain a certain continuity in the supply system, at least to assure economic sustainability. In this context, climate change effects bring to light the need to replace fossil fuels with renewable sources. Besides the importance to limit global warming impact on the environment, a low-carbon emissions policy - with a central role of renewable sources - would reduce the Italian energy dependence, diminishing the demand for fossil fuel imports and mitigating the negative effects of geopolitical instability in the countries of production and transit. This is the reason why in the past decade, hydroelectric, photovoltaic and other renewable energies have gained increasing importance in the Italian energy basket, reaching to cover one fifth of the needs. Nevertheless - despite the investments to adapt the electricity system and contain the criticalities connected to the discontinuous nature of wind and photovoltaics - technical solutions to allow a complete and economically sustainable decarbonization are still uncertain and problematic. In this context, intelligence arises to guarantee energy supply, in defence of companies and research centres to protect technological and scientific heritage and, last but not least, to contrast hostile manoeuvres aimed at marginalizing the country system in the competition for energy sector innovation[121]. Such hostile manoeuvres can be carried on through the usage of new technologies, especially in the cyber domain.

During the last year, a significant propensity of various actors - including the state or those supported by states - to resort to sophisticated cyber-attacks was registered. This led to a renewed determination to develop instruments of early detection, cyber-contrast and reaction. The most significant effort put in place by the Italian cyber-expertise concerns the contrasting of digital espionage campaigns and hybrid threat, whose operational translations have been amplified thanks to the digitization of social life. For instance, in early 2018 Italy established an ad hoc exercise aimed at gathering – within the so-called "Cyber National Perimeter"[122] - possible indications of use, interference or conditioning of the electoral process on March 4th, 2018. This exercise was also reactivated in view of the European Parliament's elections.

Along with the most significant initiatives for the development of the cyber national architecture, the operational start of the Cybernetic Security Team must be noted. It acts to prevent, prepare and response against cyber crisis, with the ultimate aim of strengthening the country's cyber defence capabilities. These capabilities have received a renewed impetus with the implementation of the "National Strategic Framework

[121] See Ibid (67)

[122] The Cyber National Perimeter has been built to increase the resilience of digital infrastructures.

for cyber space security", established by the Cyber Technical Table (TTC) on April 3rd, 2013, and the subsequent "National Plan", which operates in the Security Information Department (DIS). Because of its centrality in the national "cyber ecosystem", the DIS has promoted various initiatives aimed at increasing the country's overall response capacity, actively contributing - in conjunction with other competent institutional actors - to ensure the timely transposition of the EU Directive 2016/1148 on the security of networks and information systems (NIS Directive) in Italy. This effort would be more concrete if associated with a parallel growth of cyber security culture which, apart from public and private subjects, interests every single citizen. In this sense, DIS has developed the first national digital training campaign "Be Aware Be Digital", creating interactive tools, also for students, in order to raise knowledge and skills in the matter of conscious web and new technologies use. Together with national efforts, the incessant and tumultuous evolution of the sector requires not only readiness, competence and adaptability, but also the ability to ensure constant and timely connections between the various national components, namely governments, universities, research centres and the business world, with allied countries[123]. This approach is actually imposed to deal with the entire range of global threats, which should be faced accompanying the projection on the ground with a continuous and careful process of updating methods and practices between allied states. All of this in the perspective to put at the service of national security the best resources, aware of the complexity of the current challenges.

5.2. Cybersecurity: Documento di Sicurezza Nazionale

At the end of the Italian Security Report, there is a special attachment about cybersecurity. Such a document, called "Documento di Sicurezza Nazionale", was introduced with the law 124/2007 (according to the article 38, co.1 bis.) and points out the current status of cyber-threats, the main actors involved and the Italian cyber capabilities.

The preamble describes the current international scenario, characterized by a harsh confrontation between actors, where cyber has been confirmed as one of the main tools to pursue strategic objectives. On the basis of the information elements acquired by AISE (*Agenzia Informazioni e Sicurezza Esterna*) and AISI (*Agenzia Informazioni e Sicurezza Interna*), it emerges an overall number of hostile actions more than quintupled compared to 2017, mainly to the detriment of central and local public administration IT systems. In particular, the hackers aim to steal information about the main international security dossiers and damage the computer systems of operators. In this sense, national computer systems active in Oil & Gas, as well as those of Italian academics, are the main targets[124].

[123] See Relazione sulla politica dell'informazione per la sicurezza (2018: 14-16)

[124] See Documento di Sicurezza Nazionale (2018: 5-6)

The most significant initiative carried on enhancing the Italian cyber architecture is the creation of the "*Nucleo per la Sicurezza Cibernetica*" (NSC), under the chairmanship of a General Vice-Director of the DIS. The NSC, convened on a monthly basis, acts in the key of prevention, preparation, response and recovery against cyber crisis situations with the aim of strengthening country's cyber defence capabilities. In the performance of its functions, the NSC has[125]:

- verified the state of implementation of inter-ministerial coordination measures for purposes of preparation and management of cybernetic crises;
- collected and analysed data about security violations and compromises networks in administrations' critical functions;
- promoted and coordinated the national participation in cyber exercises, for example the "Cyber Europe 2018" - aimed at increasing the reaction and intervention capacity of the EU States - and the "European Union Hybrid Exercise-Multi Layer 2018 Parallel and Coordinated Exercise" (EU HEX-ML 18 PACE), addressed to EU Institutions, EU states and NATO countries, to verify their capacity to manage hybrid attacks against critical infrastructures.

On an extraordinary basis, the NSC has managed significant events which led to the development of coordination activities of response and recovery. A renewed impetus was then given to the implementation of the strategic guidelines envisaged by the "National Strategic Framework for cyber space security" and the operational ones included in the subsequent "National Plan". These documents provide:

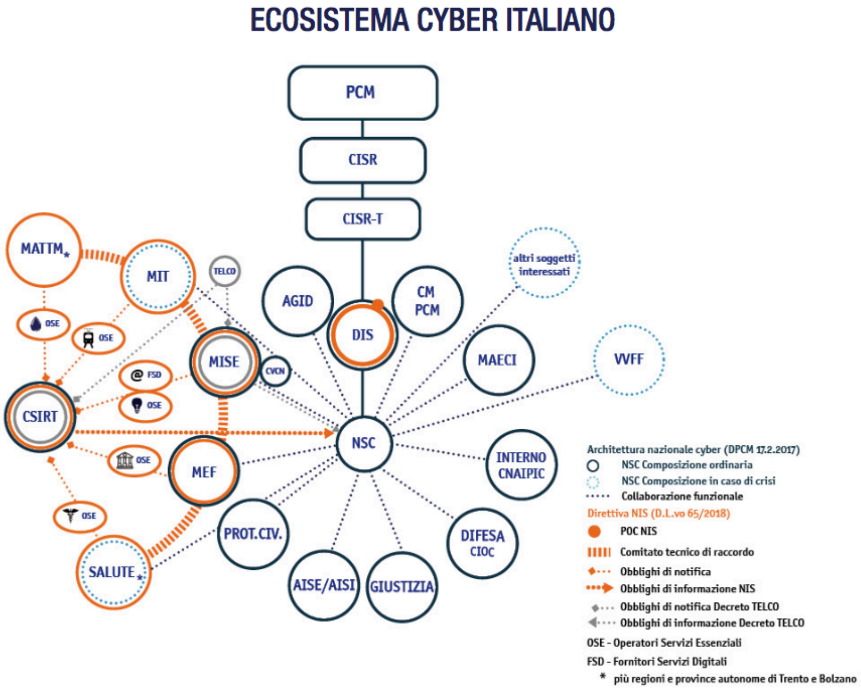
- an enlarged working group, alongside the CISR (*Comitato Interministeriale per la Sicurezza della Repubblica*), to implement the aforementioned "cyber-national security perimeter", aimed at raising the security levels of the country's vital assets;
- the establishment of a further work group, aimed at identifying guidelines for a safe procurement of ICT (Information and Communications Technology) products and services for the Public Administration, coordinated by the Agency for Digital Italy (AgID);
- a close collaboration with the *Ministero dello Sviluppo Economico* (MiSE) for the creation - in compliance with Italian and European regulations - of the National Evaluation and Certification Center (CVCN) for the verification of the safety conditions of ICT solutions, used for the functioning of networks and critical infrastructure services;

[125] See Ibid (11)

- the development of synergies - through the stipulation of a protocol between DIS, AgID and *Confindustria* - aimed at ensuring the interaction between highly specialized centers, established by the MiSE under the national *Impresa 4.0* Plan, and the Digital Innovation Hubs (DIH) promoted by *Confindustria*, to facilitate companies in assessing their level of digital and technological maturity;
- the launch of an initiative, in agreement with the Guarantor for the Protection of Personal Data, aimed at facilitating the harmonious implementation of the regulations concerning computer security with the interested private actors, taking into account the Regulation (EU) 2016/679 "General Data Protection Regulation" (GDPR), the Decree implementing the NIS Directive and the Minimum ICT Security Measures issued by AgID.

Moreover, as previously mentioned, the DIS has actively contributed to the drafting of the Legislative Decree implementing the NIS Directive (Legislative Decree No. 65 of May 18th, 2018), participating in the activities of the working group set up at the Department of European Policies of the Presidency of the Council of Ministers. This legislation assigned to the DIS the role of single NIS Contact Point (PoC NIS) with the task of ensuring, at the national level, the coordination between security of networks and information systems and, at European level, the necessary connection between the Italian NIS Authorities and a series of actors: Member States, NIS Cooperation Group (NIS CG) of the Commission and Network of Computer Security Incident Response Team (CSIRT). In its capacity, the DIS has organized a series of meetings with the competent NIS Authorities and the Italian CSIRT (Computer Security Incident Response Team) in order to coordinate the implementation of Legislative Decree 65/2018 favouring the process of identifying the OSE (*Operatori dei Servizi Essenziali*) for each sector envisaged by the EU Directive[126].

[126] See Documento di Sicurezza Nazionale (2018: 12-15)


ECOSISTEMA CYBER ITALIANO
PCM
CISR
CISR-T
MATTM*
MIT
TELCO
AGID
DIS
CM PCM
altri soggetti interessati
OSE
OSE
MISE
CVCN
MAECI
VVFF
FSD
OSE
CSIRT
NSC
OSE
MEF
INTERNO CNAIPIC
OSE
PROT.CIV.
DIFESA CIOC
SALUTE*
AISE/AISI
GIUSTIZIA
Architettura nazionale cyber (DPCM 17.2.2017)
○ NSC Composizione ordinaria
NSC Composizione in caso di crisi
Collaborazione funzionale
Direttiva NIS (D.L.vo 65/2018)
● POC NIS
Comitato tecnico di raccordo
Obblighi di notifica
Obblighi di informazione NIS
Obblighi di notifica Decreto TELCO
Obblighi di informazione Decreto TELCO
OSE - Operatori Servizi Essenziali
FSD - Fornitori Servizi Digitali
* più regioni e province autonome di Trento e Bolzano

The Italian cyber eco-system, shown in the previous picture, at the end of 2018 has been the result of the Legislative Decree 65/2018 and the "Telco" Decree of the MiSE (on December 12th, 2018) adoption, which oblige private operators to apply cyber-security measures and notify significant incidents. In addition, particular focus was placed on increasing protection and resilience to cyber-attacks, especially in the academic and research field, and an overall awareness about cyber. In this sense, to further development "Be Aware Be Digital" national campaign, it was realized the first video-game settle in cyberspace, called "Cybercity Chronicles", downloadable on smartphones and tablets and addressed at secondary school students. It also contains a cyberbook to facilitate familiarization with the words of the cyber domain, exploiting the information and lessons learned during the game[127].

To sum up, it is evident that the Italian cyber position has been defined in relation to the main international fora (EU, NATO and OSCE) policy documents (described in the previous chapter), maintaining a multilateral approach in the field to draft a unified cyber-security position.

5.3. Italy in the BTWC framework

The spread of weapons of mass destruction still represents a threat to international peace and security which requires, as in the case of cyber, a multilateral response. Indeed, the 2001 attacks brought to light the

[127] See Documento di Sicurezza Nazionale (2018: 16)

actual possibility that terrorist groups acquire WMD. Since that moment, the fight against proliferation, even in the face of the disappearance of the traditional criteria of deterrence, has become a growing international priority, even in Italy. Nowadays, the risk of WMD escalation is higher than before because of the rise competition between states in international relation. In effect, the base to assure a non-proliferation system is to live in a situation of stability and mutual trust, which is not present right now.

The commitment to disarmament and non-proliferation has been a qualifying element of Italian foreign policy, based on a broad support from Parliament and civil society. Traditionally, it is a field that sees Italy active on several fronts, such as in the United Nations, the European Union, the G-8, in the review processes of the major international Conventions - first of all the Nuclear Non-Proliferation Treaty (NPT) and the Conventions against Chemical and Biological weapons -and on a bilateral level with its main partners. Regarding the Italian role within the European Union, Italy took several actions about WMD during its six-month Presidency, in the second half of 2003. For instance, it adopted the European Strategy of non-proliferation as the foundations of a coherent European policy. The European Strategy was inspired by the strengthening of the international non-proliferation system, the promotion of the universality of international agreements, the guarantee of application and compliance with international rules and the need to consolidate and develop collaboration with the United States and other major partners. These diplomatic and political preventive measures and the involvement of international organizations has represented the first line of defence against proliferation. Such an approach is guided by the conviction that multilateralism represents the most suitable instrument to achieve the set objectives and that international cooperation remains the obligatory reference framework.

In the European perspective, the system created by multilateral treaties is the foundation of all efforts in the area of non-proliferation. However, in order to maintain credible this system, it is necessary to make it truly operational. In other words, it is fundamental the full compliance of the Member-States towards Treaties obligations, through the existing verification mechanisms and the creation of new tools. In this context, the role of the United Nations Security Council, considering its limitations, should be strengthened and a more direct collaboration between the UN and other international organizations put in place[128].

In practice, the Union is still working to define its strategic objectives and translate them into operational terms through the appropriate tools. In the past, an EU Common Position in the matter was adopted, promoting:

- the implementation of Security Council Resolution 1540/2004, which obliges national governments, *inter alia*, to adopt security measures and controls to prevent the danger of weapons of mass destruction - including biological ones – and their usage by terrorist groups;

[128] See Terzi G. (2006: 326-327)

- the development of the aforementioned G-8 Global partnership, with reference to the control and security of sensitive materials, systems and professionalism;

- the further study of the relevant issues, which includes the national measures to implement the obligations of the various Conventions.

Such a traditional European response, which addressed the causes of instability and insecurity to face WMD proliferation, has been overcome in the new EGS (previous chapter) in favour of a more defensive approach. This approach has been necessary because of a less stable environment at regional and international level. Notwithstanding this change, the non-proliferation strategy remains the same and Italy has always maintained a policy in line with EU, for example when they both implemented the Proliferation Security Initiative (PSI), launched by the United States with the aim of identifying and prohibiting illicit trafficking. Along with this, the non-proliferation is still a terrain of agreement between Italy and the United States, even with Trump's administration, and Europe essentially shares this perception of the nuclear, biological and chemical threat. This is an obligatory area of cooperation, which is able to strengthen the transatlantic dialogue.

Since the adoption of the common approach, Italian Permanent Representatives and Embassies carried out daily activities and bilateral consultations with some of the main partners to advance its WMD non-proliferation program. For instance, demanding a more incisive role of the European Union, a progressive and extended adherence to the additional International Atomic Energy Agency (IAEA) protocols and the implementation of the G-8 Global partnership for the elimination of weapons of mass destruction. The consultations have confirmed the constructive role of Italy in the matter, which, through its balanced approach, has represented a privileged interlocutor, both for nuclear countries and for the most active countries supporting nuclear disarmament[129].

To sum up, Italy commitment and initiatives with the various partners have contributed to make the debate in the European Union more dynamic and inclusive, to the advantage of the common policy. Moreover, Italy's action in non-proliferation was not only focused on nuclear, but also in the biological and chemical sector, recognizing the destructive potential of biological weapons, especially in the frame of terrorist organizations.

However, Italians had performed Biological Weapons (BW) activities since 1934 - although on a small scale and mainly for defence purposes. Italian BW experiments with Bacillus prodigious spray were described after the war by Lt. Col. Dr. Giuseppe Morselli from the Laboratory of Microbiology of the Italian Ministry of War. This facility was located on the area of a military hospital and was quite large with working space not only in two floors but also the basement. At the Eighteen-Nation Disarmament Committee meeting in 1969, the United Kingdom, supported by the United States, called for the elimination of BW. The United States agreed to ban the development, production, and stockpiling of BW and announced its intent to ratify the

[129] See Terzi G. (2006: 336-337)

Convention. The Convention opened for signature on April 10th, 1972, after the United States and the Soviet Union reached agreement on the text of the Convention. Since the entry into force of the Convention on the ban on bacteriological weapons (BTWC), and after the 2003 European Strategy adoption, Italy dedicated a strong commitment to fight BW proliferation. The full respect of BTWC obligations required the identification, an effective verification mechanism and a valid national implementing legislation, especially with respect to transparency measures and the safety and control in the management of pathogenic micro-organisms and toxins. The case-by-case investigation of suspected use of biological weapons and subsequent monitoring, identification and fight against infectious diseases, demanded also for periodic review conferences of the Convention, in the context of which it is possible to propose amendments and update about scientific developments in that sector[130].

At the 6th BTWC Review Conference, held in Geneva in November 2006, Italy played a steering role through the presentation of an Action Plan for universal application of the convention. Nonetheless, such a review did not reach agreement on that, because of disagreements between developed and developing countries about how to reconcile BWC obligations against proliferation with provisions which facilitate exchange of information, materials, and technology for peaceful purposes. The States Parties also did not address the contentious issues of verifying compliance and increasing transparency of national biodefense activities. In spite of all, the President of the Sixth Review Conference praised the outcome, arguing that it produced historic results[131]. On the contrary, non-governmental experts considered the result "very modest" (Pearson A. 2006) and Tucker argued that the dysfunctionality of the biological arms control process was demonstrated by the fact that the modest accomplishments of the Sixth Review Conference were hailed as a success[132].

Such a dysfunctionality is still felt, as also the 8th and last Review Conference's outcome, held in Geneva in November 2011, emphasizes. The conference was attended by over 900 participants from 124 member states parties (MSP) - among them Italy - four signatory states, two states neither parties nor signatories to the Convention, four UN organisations, nine international organisations and thirty-three NGOs and research institutes. This was a record participation with a twenty percent increase in attendance by States Parties compared to the Seventh Review Conference in 2011. Additionally, Guinea, Liberia and Nepal all joined the BWC just beforehand and were welcomed by the Conference as new States Parties, thereby increasing the BWC's membership to 178 States Parties. During the Conference, States parties submitted a total of eighty-three Working Papers, covered a wide range of proposals which included:

[130] See Nuti L. (September 2007)
[131] See Ambassador Masood Khan (December 2008).
[132] See Tucker J. B. (January 2007)

- a mechanism to review developments in science and technology,
- the establishment of a database under Article VII of the UN Charter, concerned assistance to States exposed to danger resulting from a violation of the treaty,
- guidelines for the submission of a request for assistance under Article VII,
- voluntary codes of conduct for biological scientists,
- the Geneva Protocol, which an instrument predating the BWC that prohibits use of biological weapons,
- a legally-binding instrument including a verification and an export control mechanism
- consultation and clarification procedures,
- enhance the decision-making authority of the Meeting of States Parties.

The general feeling at the end of the Conference was of disappointment and frustration because, despite the large number of working papers, ideas and work programs, the Final Document contained "minimal" provisions. The causes have been the different visions by some key players between pursuing a comprehensive, legally- binding verification protocol versus the strengthening of the BWC and the issue of enhanced decision- making authority of the MSP. These divisions are still present, and they must be overcome to realize the common goal of strengthening the BWC thereby upholding the established norm against biological weapons. Otherwise, States Parties might feel inclined to focus on other less comprehensive and universal initiatives, leading BWC to a fragmentation and lose its relevance in the international regime against weapons of mass destruction[133].

5.4. Italian National Strategy for Adaptation to Climate Change (SNAC)

The multilateral approach enshrined with the BTWC, which has involved Italy, is controversial and present a wide range of limits. On the contrary, the approach inaugurated by the EU about climate change is more successful and it has been efficiently transposed in Italy.

Indeed, on April 16th, 2013, the adoption of the European Climate Adaptation Strategy gave the impetus to European countries like Italy, lacking a coordinated national vision on climate change adaptation, to begin the elaboration of a national strategy.

Thus, the Italian National Strategy for adaptation to climate change (SNAC) was created, founding on the technical-scientific report "State of scientific knowledge on impacts, vulnerability and adaptation to climate change", the technical and legal report "Analysis of the legislation for adaptation to climate change: Community framework and national framework" and "Elements for a National Strategy for adaptation to

[133] See Maylis D., Konovalova E., and Bertherat C. (2017: 2-5)

climate change". The first document, the technical-scientific report, confirms what has been already indicated in the documents prepared by the International Panel on Climate Change (IPCC) and by the European Environmental Agency (EEA) on the vulnerability of Italy in the context of the Mediterranean area. The Report also considers the estimation of climate change's cost, providing an in-depth study of vulnerable environmental systems such as the Alpine and Apennine area and the Po river basin district. Instead, the technical-legal report presents an analysis of the European situation and the EU legislation on climate change adaptation. Climate change costs have been determined also examining the "European Adaptation Strategy" of the European Commission, the existing tools for integrating adaptation into the various sectoral Community policies and the set of rights, legal obligations and political objectives of the Member States within the Union, with reference to impacts, vulnerability and adaptation to climate change. Finally, the document "Elements for a strategy of adaptation to climate change" defines the national measures capable of giving future answers to the impacts of climate change in multiple socio-economic sectors and natural systems, based on an assessment of sectoral vulnerabilities[134].

As a result, SNAC develops a national vision about the common paths to follow in dealing with climate change, countering and mitigating its impacts. In this sense, SNAC identifies actions and guidelines to minimize the risks deriving from climate change, protect health, well-being of the population, preserve the natural heritage, maintain or improve the resilience and adaptability of natural, social and economic systems , as well as take advantage of any opportunities that may arise with the new climatic conditions.

To achieve these objectives, this document defines five strategic actions[135]:

- improve current knowledge on and climate change impacts;
- describe the vulnerability of territory, the adaptation options for every natural system and the relevant socio-economic sectors with their associated opportunities;
- promote participation and increase the awareness of stakeholders in the definition of sectoral strategies and adaptation plans through a wide communication and dialogue process;
- support awareness-raising and information on adaptation through the spread of communication activity about the possible dangers, risks and opportunities arising from climate change;
- specify the tools employed to identify the best options for adaptation actions, also highlighting co-benefits.

The set of actions and guidelines identified in this document has been selected with reference to the sectors of socio-economic and environmental importance that are most vulnerable to climate change, since

[134] See Ministero dell'Ambiente e della Tutela del territorio e del mare (2014: 8)
[135] See Ibid (10).

that understanding of the nature and consequences of climate change is at the basis of any serious mitigation or adaptation policy. As "mitigation", it means curbing climate change, whereas "adaptation" reduces the costs of climate change. In both cases, it is important to assess what would be the costs of inaction, that is, the economic impact of climate change in a baseline scenario, in which no policies are implemented.

The main scientific publications about the evaluation of impacts and vulnerability to climate change, at international and European level (IPCC, 20132; IPCC, 20143; EEA, 20104) as well as at national one (APAT / ISPRA, 20075; ENEA, 20076; FEEM, 20087; CMCC , 20098), agree that the impacts of climate change in the European Mediterranean region will be particularly negative in the coming decades. These impacts - together with the effects of anthropic pressures on natural resources - characterize this area as one of the most vulnerable in Europe[136].

In Italy the most significant expected effects will be the result of the exceptional rise in temperatures (especially in summer), the increase in extreme weather events' frequency (heat waves, droughts, episodes of intense precipitation) and the reduction in the annual precipitation average and annual river flows[137].

The worst scenario described - according to the fifth annual report of the Intergovernmental Panel on Climate Change - foresees the complete melting of European glaciers by 2050 (already the twenty percent of Europe's Alpine glaciers melted between 1980 and 2000). A case in point would be Europe's most southerly glacier, the Calderone*,* which sits on the Gran Sasso massif in Abruzzo. Nowadays, experts say it will be gone by 2020. In the meanwhile, the water generated by Italy's Alpine glaciers would melt contributes to the sea levels rising and to the global temperatures increase, since that the large tracts of white ice are no longer present to reflect the sun's rays back out to space. In addition, the Alpine environments are particularly susceptible to climate change and it warms at three times the rate of coastal areas. Thus, the global warming would strongly impact in this area, threatening Italy's ski industry and, subsequently, tourism. Indeed, figures from Italy's Ministry for Environment, Land and Sea show that the rise of temperature, would eliminate nearly all the snow cover under 2000 meters in the Alps and that snow at higher altitudes would arrive later and melt sooner. That would be bad news for Italy's 286 ski resorts, whose half-pipes, ski lifts and chalets may soon be nothing more than abandoned structures. As Italy's glaciers wilt in the sun, the coastal waters around the country would rise, putting low-lying cultural treasures at risk, such as UNESCO World Heritage sites like Pompei and Herculaneum, or cities like Venice. Furthermore, despite it might not seem dangerous, higher global temperatures cause higher rates of evaporation, change the way air moves and affect the amount of water vapor the air can hold. On a global scale, such a situation would disrupt weather systems and cause violent and unpredictable events such as storms and droughts. This is already happening in Italy in these last years and will only get worse if climate change is not tackled. Along with this, a 2013 study by Conservation

[136] See Report of the European Environment Agency (2010)

[137] See Ministero dell'Ambiente e della Tutela del territorio e del mare (2014: 18)

International warned that if the climate trends continue at the current rate, Italy's famed wines could soon disappear, because grapes are one of the most weather-sensitive crops. Thus, the study predicts that a majority of suitable wine-growing areas would be lost by 2050 and wine production would start taking place in central and northern European countries. As a result, Italy's wines would become more expensive because of higher production costs spend on special measures such as irrigation[138].

Taking into account such assumptions and the whole SNAC document, Italian vulnerabilities are the following[139]:

- possible worsening of the already existing conditions of strong pressure on water resources, with consequent reduction in the quality and availability of water, especially in summer in southern regions and in small islands where the ratio between alluvial aquifers and mountain areas is low;
- possible alterations of the hydro-geological regime that could increase the risk of landslides, mud flows and debris, rock collapses and flash floods. The areas most exposed to hydro-geological risk include the Po river valley (with an increased risk of flooding) and the Alpine and Apennine areas (with the risk of flash floods);
- possible soil degradation and higher risk of soil erosion and desertification, with a significant part of southern Italy classified as being at risk of desertification and several regions of the North and the Center showing worrying conditions;
- greater risk of forest fires and droughts for Italian forests, with the Alpine area and the island regions (Sicily and Sardinia) showing the greatest criticalities;
- greater risk of loss of biodiversity and natural ecosystems, especially in the alpine areas and mountain ecosystems;
- greater risk of flooding and erosion of coastal areas, due to one greater incidence of extreme meteorological events and sea level rise;
- potential reduction in agricultural productivity especially for wheat crops, but also for fruit and vegetables; the cultivation of olives, citrus fruits, vines and durum wheat could become possible in northern Italy, while in the South and in the Center the cultivation of maize could worsen and be even more affected by the availability of irrigation water;
- repercussions on human health are possible, especially for the most vulnerable groups of the population, due to a possible increase in heat-related diseases and mortality, cardio-respiratory diseases

[138] See IPCC (2014) 5th Assessment Report.

[139] See Ministero dell'Ambiente e della Tutela del territorio e del mare (2014: 18-21)

from air pollution, injuries, deaths and diseases caused by floods and fires, allergic disorders and changes in the appearance and spread of diseases of infectious water and food origin;

- potential damage to the Italian economy as a whole.

Regarding this last point, a study developed by the World Bank have found out that climate change would reduce the Italian GDP in 2050 by -0.31 percent and the main driver of negative effects on GDP would be the decline in tourism. To deal with these problematic, the EU adaptation strategy have proposed some solutions, such as reducing water consumption, adapting building regulations, building flood defence systems and developing crops more resistant in drought conditions[140]. The Italian efforts about climate change fit with such EU climate action's framework and follow - besides the climate adaptation strategy – the 2020 and 2030 climate goals, the 2050 long term strategy and specific regulations on the matter. Moreover, Italian climate actions pursue the objectives agreed in 1992 during the United Nations Framework Convention on Climate Change (UNFCCC) and – more recently – those fixed by the upgrade of the Kyoto Protocol and the Paris Agreement.

Taking everything into account, Italy maintains its role as multilateral player in the international chessboard. Nonetheless, it cannot be underestimated the rising geopolitical and geo-economic competition, marked by the 2018 annual macro-data used in the last "*Relazione sulla politica dell'informazione per la sicurezza*". Indeed, even the relations between allied countries are showing multiple fault lines and a pronounced push towards unilateralism, which threaten the aforementioned multilateral assets. Thus, based on this assumption, the Italians perceive more domestic threats rather than global challenges, focusing on the decrease in welfare levels and the socio-economic impact of illegal migration and terrorism, as enshrined in the recent Italian Security Decree. In the meanwhile, the scale and nature of the current global threats demonstrate that they are far from a solution and their negative effects are accelerating and degrading.

[140] See EU Adaptation Strategy (2013)

Chapter 6. Conclusive Analysis

In a globalised world, emerging threats are interconnected and affect indistinctly people in every country. In effect, new tools of scientific and technological progress, like nuclear physics and cyber-technology, allow hybrid threats to overcome state limits, demanding a comprehensive security approach to be solved. Moreover, in the last few years global challenges are becoming more and more dangerous. For instance, now the effects of climate change are evident, the rising state competition is exacerbating cyber-attacks, and the proliferation of WMD is assuming new shapes. Thus, their effects tend to go beyond traditional security approaches - which explores how states maintain the integrity of their borders and protect their communities from external threats of violence - targeting potentially every single person in the world. This brings to light the importance of individuals as human beings and their security regardless national borders.

At the same time, a sort of "strategic confrontation" is re-emerging between great powers, enshrining a sort of rebirth of the realist paradigm in current IR. Thus, the international arena is interpreted as a zero-sum game, national interest prevails over common good and power represents state main tool and concern.

It is evident how such interpretation can be dangerous if applied in the current international scenario. In fact, negative relations between states can nourish global instability, already aggravated by the aforementioned emerging threats. In turn, such global instability enhances mistrust between states and their selfishness, creating a vicious cycle. Moreover, the current global threats, which can spread worldwide very quickly, cannot be faced by a state alone, making mutual trust and multilateral assets essential to maintain global security.

In this analysis such a reasoning has been demonstrated considering three of the current most dangerous global threats, namely the effect of climate change, biological threats/bioterrorism and cyber-threats. That is not a random choice. Climate change effects have been picked up because they are constantly underestimated and worsened by the reckless behaviour of people and global leader inertia. This is the worse emerging threats, because imply several other issues and, as ultimate effect, the permanent and drastic destruction of human beings. Such extremely serious outcomes are higher than is generally understood, aggravated by the impossibility to learn from mistakes and rely on the institutions, moral norms, or social attitudes developed from experience. Moreover, this issue can be solved only through a global engagement, because if some state continues to ignore measures against global warming the efforts of the others will be useless.

Dealing with biological threats, this is inscribed in the current debate about WMD proliferation. However, such a debate focuses more on nuclear or chemical weapons, leaving aside the matter of biological warfare. This a terrible mistake, because bio-threats are more dangerous than chemical ones and cheaper than nuclear. Indeed, they differs from chemical agents, which are not able to expand beyond the attacked area without losing their lethality, because they can spread easily maintaining their mortal effect. Moreover, biological agents do not require particular vectors as bombs, artillery shells, missiles, like nuclear weapons, but it is enough for them to contaminate water, crops, animal or air in crowded areas, such as the subway or a mall. Thus, not only it harms people, but it generates chaos and fear. This is the reason why it is more realistic to imagine an attack with biological weapons perpetrated by terrorist organizations (the so-called "bio-terrorism") than by a state. In addition, the biological research cannot be stopped because it is essential to eradicate diseases. Nowadays, this threat is more dangerous than ever because of modern scientific techniques, that can enhance existing biological agents and their lethality, and the global mistrust that can give an excuse to develop them.

To sum up, climate change and biological agents are defined as dangerous global threats against humanity because of their global effect, which affect the world as a whole outside the traditional battlefield, and because such an effect can be aggravated by the current strategic confrontation between states. Another threat which presents these features is the cyber-threat, which differs from the other menaces because it acts outside the physical world, in the cyber-space, and it is not underestimated by global leaders. The reason why the cyber domain has assumed a prominent role in the current security debate is that it is a powerful tool in the strategic confrontation between state. In fact, its low-cost accessibility and its pervasiveness are creating an area of absolute chaos which permits to hide criminal networks, hackers, terrorists and allows the manipulation of digital capability by governments or companies against their competitors. Despite all the new regulations and cyber-security capabilities, the cyberspace remains an unknown and unverifiable place, provoking still serious concerns in term of accountability. In practice, the large number of actors involved makes difficult to identify who is actually behind the attack, making the principle of self-defence and retaliation - the two paramount principles of defence rules - very fragile and precarious. Along with this, since new technologies are growing increasingly cheap and available, there is also a rise in terms of mass involvement and, subsequently, more channels of vulnerability.

Taking everything into account, the distinction between war and peace is fading away because of the exploitation of these threats in hybrid conflicts that, in the worsen case, can degenerate in an actual war.

This is the reason why it is important to increase both people and state awareness about the current security scenario and the new threats. The problems arise when each state presents a different interpretation of that, adopting a subjective and convenient narrative of the current IR. This means that each state drafts its own security strategy pointing out priorities related to national interest rather than shared views. In this thesis, the security strategies' analysis has indicated such a situation, showing notable discrepancies in the interpretation of threats. There are also differences about how each power sees its own place in the global order. Such divergent positions are more or less evident, thus in this chapter they are going to be analysed, starting with Italy.

Despite the Italian security report has highlighted a certain instability and weakness in the global security environment, Italy remains focalized on threats which come from the neighborhood. Such a perception has been influenced by the fears of the population, scared to suffer a terrorist attack and suspicious towards migrants. This general mistrust has been fomented and exploited by certain political parties to gain consensus and has led to a more closed approach within the borders of the nation-state and a strict focus on domestic security, rather than global one. However, the rising unilateralism and a weaker role of organizations like the EU has not undermined the Italian engagement in multilateral agreements, especially those enshrined in the framework of EU and UN. For instance, Italy is still part of the Paris Agreement and follows the EU climate change approach to fight the global warming. Moreover, the EU Directive 2016/1148 (NIS Directive) about cyber-security has been immediately transposed in the Italian legislation and Italians remains active members of the BTWC about biological weapons. Thus, global challenges are theoretically addressed by Italian government, even though they do not represent at the moment among government priorities. This gap between theoretical and practical actions is the main problem and - taking into account the 2018 annual macro-data used in the last "*Relazione sulla politica dell'informazione per la sicurezza*" – in this context also the rising geopolitical and geo-economic competition cannot be underestimated. These tensions make relations between allied countries more complicated, threatening the aforementioned multilateral assets and impeding to find a common ground in dealing with global challenges. These are the reasons why nowadays the Italian focus on national interests is subordinating global challenges to domestic issues such as the decrease in welfare levels, the socio-economic impact of illegal migration and terrorist propaganda. The practical example of that has been the adoption of the Italian Security Decree. However, the recent government crisis can scramble into play cards.

Considering the linkage between Europe and the US, the Italian closure has also been the result of the change in the American administration, which has redefined the rules of the game. In fact, since 2016 the US strategy has shifted from the Obama era - focused on global structural problems and cooperative ways of solving them - to prioritize competition between great powers. This is the base of Trump strategy, namely a narrow and focalized view of American global position in line with realism's principles. This zero-sum game vision has led to adopt harder forms of power to maintain national security, such as an increase in defence expenditure and harsh measures against sneaky competitors. Russia and China are identified in the US strategy as adversaries whose increasing influence has to be contained. For instance, according to the US' President, China wants to limit US access in the region and militarize the South China Sea, while Russian actions aim to provoke the credibility of the USA and the EU, questioning the sovereignty of certain strategical states, like Georgia and Ukraine, and openly threating the other countries through WMD and cyberattacks. In this framework, the American narrative address global challenges only in relation to the activities of these malicious actors, prioritizing dangers associated with foreign states rather than fatal global threats. In this sense, it is emblematic that the US security strategy takes into account cyber-security and WMD proliferation in depth, ignoring completely the matter of climate change. Dealing with cyber and WMD, President Trump recognizes the importance of global commitments and responsibilities, but the systems of alliance are downgraded in comparison to previous strategies. As a matter of fact, agreements like the TPP, NAFTA and the Paris Agreement are questioned, preferring a bilateral approach for negotiations. According to Trump interpretation, the reason behind this choice is the danger associates with the dilution of US national interests, caused by an over-committing to broad multilateral agreements that ignore how competitors, such as China, Russia or Iran, can take self-interested advantage of them. In turn, the strategies of both Russia and China aim at building a counterweight to the US power, sharing a competitive view of the international arena. However, there are significant differences between the Chinese and Russian approaches.

China is concerned about stability, which is needed for a long-term building up of the Chinese position and resources. The ultimate goal, to reach gradually, is an equal position for China among major powers in a multipolar order. Thus, the Chinese strategy highlights formally interdependence, mutual benefit and win-win results. Russia is seen as the main partner, but this cooperation is secondary to the wish of maintaining a stable relationship with the US. In the "Outline of the National Security Strategy" is enshrined this vision and the ultimate goal of protecting Chinese socialism and values. Thus, the actual enemy is not properly the US, but the promotion of democracy, cultural hegemonism and profligate dissemination of news and media on the internet by Western countries. In particular, according to the Politburo, internet provides a channel for breaking China's ideological and national cohesion at the same level of a terrorist attack. This vision of uncontrolled information as a danger and not as an opportunity, justified the priority role of the Chinese state in controlling cyberspace. Indeed, aware of not being able to compare with the United States military power, China has decided to invest in the cyber domain. The ultimate goal of Chinese cyber-strategy is no longer "catch-up", which means the achievement of equal military capabilities of the US, but the idea of *Sha Shou Jian*, namely "if you get the proper resources, you can defeat an enemy much bigger and stronger than you". Nonetheless, the current war trade with the US, is changing Chinese strategy and China has already abandoned its role of economic giant in favour of massive investments in defence. In this framework, there is no place for climate change and environmental issues, subordinated to Chinese core interests, especially economic ones. In fact, cheaper and more abundant energy resources, like fossil fuels, are essential to China's continued economic growth. Thus, global threats maintain a marginal position in the Chinese strategy because other dynamics are threating directly the Chinese international position.

On the contrary, Russia takes a distinctly more aggressive approach to achieve the goal of "strategic stability" in a polycentric world and it is explicitly hostile towards the US, the West and the EU. The Russian strategy is more explicit on how competition between major powers plays out in a variety of fields, ranging from access to markets and resources to social models and values. The Russian view on stability also appears quite different from the Chinese one, indeed strategic stability is a goal to be achieved through Russia's increasingly assertive role. Hence, the Russian and US strategies share a rather negative view on interdependence, seeing it as a constraint to national interests. Such interpretation of Russia's global position is described in the 2015 Russian National Security Strategy. The new strategy interpreter the current IR situation through a realist view, emphasizing the military component of national security. A dominant position can be achieved using the full spectrum of means in the competition for power and prestige, abandoning the previous idea of economic and technological transformation as a route to assert Russia role worldwide. The base of Russian strategy is the "asymmetric approach", whereby the strengths of Russia (the weaponization of information, technology and organizations) are coupled with its relative weakness in military-technological development, and the "active defence", namely the activation of a set of non-military measures to neutralize all the potential threats against Russian national interests. Among the non-military measures, cyber-security is the most important. In this field, Moscow focus on the control of information to shape and mould the populace, using disinformation, espionage and cyber operations to reduce the potential of the enemies. In putting its military doctrines into practice, one of the tactics employed by Russia is to co-opt with criminal hackers, founded on a tacit bargain under which hackers will not target people within the former Soviet states and the Russian state will tolerate their criminal activities. This strike opened the door to a new frontier of cyberwarfare. All of this is used to face the main threats which – according to the Kremlin - are those against Russian values, i.e. Western countries and culture. With this perception, challenges like climate change are not perceived like a hazard and traditional military means remain the first concern for Russian government.

This is seeming to leave multilateral organizations as the sole liberal idealist in the world of fierce great-power competition. In particular, the EU and UN strategies are the unique among all the analysed cases which reject clearly a worldview centred around zero-sum rivalry among major states. There is some similarity, however, between them and the Chinese outlook on interdependencies as a factor that favours cooperation and stability.

Dealing with European security policies, the European Global Strategy (EGS) has been the response to the radical worsening of the EU's security environment, threaten by common threats like terrorism and WMD proliferation as well as new global challenges like climate change and cyber-attacks. As said before, the EGS explicitly rejects a realist worldview by stressing the EU's commitment to a win-win approach but, at the same time, expresses a heightened sense of insecurity which necessitates a new focus on self-protection. As a result, the EU's attention shifts from projecting stability beyond the Union's borders to defending oneself against external instability and the promotion of values such as democracy, the rule of law and human rights loses its central place, acquired a more defensive dimension. The main European concerns are external threats coming from the neighbourhood, the East and South, but also international terrorism, hybrid threats, economic volatility, climate change and energy insecurity are taken into account. Regarding climate change, the EU continues to address its root causes in the framework of the Paris Agreement, fixing also independent European climate goals. In the field of cyber-security, the EU has adopted the NIS Directive, which will be updated soon. Moreover, the Union supports the Biological and Toxin Weapons Convention, especially promoting the adherence of its member states to the convention. To sum up, despite the increased global insecurity and instability has provoked a certain anxiety both in the Union and in its member states, pushed towards a more defensive approach to the outside world, the EU's global vision still stresses the importance of multilateralism and rules-based cooperation. The same has occurred in the UN strategy.

Indeed, in the 2018 Report of the Secretary-General of United Nations (UN) Antonio Guterres, it is expressed the awareness about a general increase of conflicts with grave violations of human rights and humanitarian law, the risen inequality, intolerance and discrimination against women, the impact of climate change and the need for defensive reforms. Theoretically speaking, the primary responsible for the maintenance of international peace and security within UN's structure should be the Security Council (UNSC), but it has relevant limits. In practise, the UNSC suffers the lack of a binding, legal oversight mechanism to make its decisions actually apply and the power of veto of its five permanent members (i.e. China, France, Russia, United Kingdom and United States) have the ability to block arbitrarily any resolution. These provisions undermine the entire basis of the UN, which is international cooperation. International cooperation can be obtained only through unity and solidarity between countries, which is further threaten by the new competitive environment and the overall distrust. Besides all the difficulties, UN is adopting a wide range of reforms to address properly global issues, which includes prevention and disarmament, building partnerships among Member States, regional and international organizations and civil society to share ideas and promote burden-sharing. United Nations peacekeeping missions have also developed new tools for the mitigation of new asymmetric threats. Overall, the UN Secretary General has pointed out the need to combinate lower and higher-level efforts and report current developments in science and technology and their potential impact on international security. These measures aim to increase awareness and response capability, especially in the biological, environmental and cyber field. Thus, despite its evident limits, the UN is trying at least to ensure a transparent cross-pillar communication between countries to help them in facing new threats and recovering a climate of cooperation.

Besides the well-addressed efforts of the UN and EU, other international organisations are trying to adapt to the new global order, but with more difficulties. This is the case of NATO and SCO.

The last NATO official security document was drafted in 2010, hence it is quite obsolete and demand important upgrades. One fundamental point that has been underestimated in the 2010 Strategy is the return of great states power politics and the rise of potential peer competitors (i.e. the USA, China and Russia) which, has said before, changes completely the rules of the game. Moreover, NATO has been obliged in the last few years to adapt unconventional threats, like terrorism, instability and cyber-threats. However, for a conventional defence organization like NATO it is not easy to meet such new challenges. Until now, the Alliance has taken step forward in the cyber domain, recognising cyber defence as part of the Alliance's collective defence and applying the international law to cyberspace. Allies have also committed to enhance information-sharing and mutual assistance in preventing, mitigating and recovering from cyber-attacks. Alongside such new complex challenges, NATO is also changing its approach towards traditional threats, such as the weapons mass destruction (WMD), taking seriously into account new potential manifestations like bio-terrorism. Indeed, the Allies have invested significant resources in warning and reporting, individual protection and CBRN hazard management capabilities. Despite all these efforts, NATO internal cohesion is currently challenged by Brexit, mass migration, financial fragility, trade wars and the new strategic confrontation. This instability within and outside the Alliance impedes to broaden NATO agenda, including for instance climate change.

The case of SCO is pretty different, because it still lacks a considerable number of essential features to be a proper security organization, like to have at least some common interests. "The Shanghai convention on fight against terrorism, separatism and extremism" is still the base of Shanghai Cooperation Organization (SCO) security approach, based on the "Shanghai spirit", which differs from Western core values in term of respect for human rights and the self-determination of peoples. This convention has been established against the so-called "three evils" (i.e. terrorism, separatism and extremism), which have to be fought by creating mutual trust, friendship and cooperation. Nonetheless, SCO members continue to follow their own national interests, especially leading countries like China and Russia. China, aiming to maintain its domestic political legitimacy for the survival of the regime, uses SCO to maintain various kinds of partnerships with other countries, avoiding directly confrontations with any great power. This strategy maximizes access to the global economy, while minimizing the risk of foreign military threats and led China to gain international support. For Russia, the SCO apparently acts as a means to bring together different policy objectives, using this partnership to export arms and energy and obtain a closer relationship in the military field. In addition, Russia exploits this organization to reduce Western influence in its backyard of Central Asia. In the last years, China, Russia and the other member states agreed to extend SCO agenda including, alongside the three evils, universal problems like drug trafficking, cyber-sabotage and aspects of weapons of mass destruction (WMD) proliferation, always with the ultimate goal of protecting core national interests. In line with Chinese and Russian security visions, the SCO proposes a cybersecurity strategy which embodied SCO principles such as the respect of state sovereignty, non-interference in the internal affairs of states, equality and mutual respect in the fulfilment of international norms and the fight against the three evils also in the cyber-space. This cyber-strategy differs completely to the Western one, because it implies an excessive state control in cyberspace, affecting the freedom of expression and privacy of citizens. Moreover, the SCO agenda remains tightly focused on conflict avoidance and peaceful dialogue among its members, because of the lack of political will and internal cohesion. This is the reason why it addresses threats only if affecting directly the stability between its member states, such as cyber-threats and WMD (only in the field of nuclear proliferation), ignoring global issue like climate change.

All in all, every strategy reflects the complex nature and multiplicity of threats in a subjective way, pointing out a broad and divergent range of responses. Only terrorism, economic security and vulnerabilities in the spheres of cyber and energy remains shared concerns. It is evident in each strategy the increased emphasis on military power, even in the EU frame, even if it lacks any serious capability in this field. The states which are weaker in the military field but aspire to gain a prominent international position, namely Russia and China, have complemented the military power with various other instruments, using an "asymmetric approach". At the same time, also great military power like the US stresses the need to be prepared to operate across multiple domains at once, in conflict scenarios involving political, military, economic and cyber spheres. Another point that enhances competition and divergent approach is the contestation over values. Indeed, advancing values such as freedom, democracy and human rights, once a declared cornerstone of the US, UN, European and Italian foreign policies (in different variations), even if still present in their strategies, are less central and more defensive in comparison to their earlier rhetoric. In the meanwhile, both China and Russia, also in SCO framework, stress their own particular values and the need to defend these against external influences. In spite of the differences, all the strategies tackle the rapid change of global structures and instruments of power and try to identify ways to shape these dynamics and adapt. A major common theme in the strategy documents is the rise competition among major powers and the need for a cyber-strategy, used to defeat the enemies in the military, political and economic fields as well as at the level of values.

The following table sums up the approach of each state towards the emerging threats analysed in this thesis, namely climate change, bio-weapons and cyber-threats:

	Cyber-threat	Bio-threat	Climate threat
USA	✓	✓	✗
CHINA	✓	✗	✗
RUSSIA	✓	✓	✗
NATO	✓	✓	✗
EU	✓	✓	✓
SCO	✓	✗	✗
UN	✓	✓	✓
ITALY	✓	✓	✓

After having analysed and retraced the national security strategies and their core points, the first part of the research question "if and why states and international organizations have different perspectives of emerging threats" has finally found a response. Now, it is time to give an answer to the research question as a whole, specifying the reasons behind the choice of national priorities. Intuitively, such a choice depends on the environment in which each state operates. In fact, this environment is affected by external inputs, like threats and international interests, to which the state must respond. However, because of the complexity of the international system, threats can be understood easier over short distances, and this is the reason why states prefer to worry within a regional area than a global one. The regional area does not refer to properly geographical borders, but to a zone defined by security relationships between the existing units. These relations identify a "red zone" of national interests in which the state works to defend itself against threats and promote its interests. This red zone is generated by the interaction between inputs from the international system (threats and opportunities) and the state's ability to respond to these inputs. In other words, the red zone depends on the power of influence of each state in the surrounding system. In this context, "power" should be interpreted as smart power, namely a combination of coercive and co-opting force. Power functions like a magnet, whose magnetic field represents the area in which the state is able to project its interests and attract threats. As a result, different areas of interest are created by the power of each state, defining the red zone of national interests. Both the shape and the extent of the red zone depend on the state's ability to respond to external challenges. For example, the red zone of a superpower coincides with the world in its entirety. Not surprisingly, the United States has global interests and equally global threats. Otherwise, the red zone of a great power includes inter-regional interests and threats and that of a medium power is usually regional. Finally, the red zone of a small power is substantially extended to its neighbourhood. Following that reasoning, the current focus of states on domestic environment and nearly neighbourhood is the result of a weaker ability to deal with global challenges. The reason behind such increasing weakness can be understood giving an internal look, essential to understand state capabilities and vulnerabilities. In this regard, it is useful to consider the state strength, namely its internal cohesion and ability to perform efficiently institutional tasks. In term of efficiently, a "minimal" state is able to ensure only basic services such as internal and external security and basic public infrastructures. In the opposite case, a "maximal" state is able to provide more complex services, such as the development of advanced infrastructures, a wide range of public services and capacities for social, economic and cultural development. Considering cohesion, a state can be "united" or "divided" depending on the degree of legitimacy that institutions receive among public opinion. Consequently, strong states are generally united in cohesion and maxims in purpose, while weak states are divided and minimal. A different combination of these factors can produce intermediate stages, namely strong states that are weakening or weak states that are strengthening. Weak states are more likely to generate internal threats, are less able to turn resources into power and generate strategic plans to address global threats. Thus, fragile states are more interested in domestic than international policy issues, because internal problems absorb most of the resources, and focus more on short term rather than medium / long term issues. This is because the ruling elite is concerned only by its own political survival. Taking everything into account, currently states are more fragile than before because of less efficient in term of public services, less legitimize and less cohesively. Such a situation can be the result of the economic crisis and the loss of values. Indeed, values are the last variable capable of influencing security policies, affected the strategic culture of a nation-state. Strategic culture is a way of thinking and acting, with reference to foreign policies, security and defence, interpreting the surrounding reality through the filter of people cultural values. This is the reason why, a national security strategy cannot be completely objective, but it is the result of values and historical experiences. In this sense, the strategic culture intervenes on the behaviour of the states influencing the perception or misperception of the other, the morale of the troops in war and the politics of alignment and alliances. This determines a state's sensitivity to threats. For example, the presence of tragedies suffered throughout history by a nation (aggressions, conquests, natural catastrophes) increases the level of sensitivity towards that type of threat. Moreover, strategic culture can influence the choice of the military doctrine, because culturally homogeneous and strongly cohesive populations are willing to bear greater costs in a conflict, compared to culturally heterogeneous and poorly cohesive states. Finally, political culture or ideology influences the choices of the alignment and cooperation, since States with similar cultural characteristics are more likely to cooperate[141].

[141] See Camilli E. (2014: 8-12)

Hence, the response to the research question “if and why states and international organizations have different perspectives of emerging threats” is that states and international organizations have different perspectives of emerging threats because there are values and historical experiences that affects state decisions and shapes their strategic culture. In addition, despite the majority of threats are global and demand a comprehensive approach to be solved, it is easier for states to focus on a narrow spectrum of threats, which are closer and more immediate. This limited state capacity depends on the rising global instability and the subsequent loss of nation-states’ centrality.

Nonetheless, state should avoid enhancing discrepancies and weakening multilateral assets, because these are the only to find a common ground and overcoming ancient grudges to deal with new global threats. In fact, these menaces demand an unified and equal efforts among the whole international community to be faced.

In conclusion, the concept of national security remains an ambiguous topic that needs a constant re-definition due to the continuous change of the international scenario. In the current world, the concept of national security is returning to its origins with a strict focus on national interest and a competitive approach among the international relations. After a decade of war on terrorism, the consequent wars in Afghanistan and Iraq, the international economic crisis, the difficult situation in Middle East and the rise of the cyber-threats, the sense of insecurity is too high to face global threats with mutual trust and strong multilateral relations. Such a situation undermines the popularity of organizations like NATO, the European Union and the effective power of UN which, on the contrary, should have been enhanced in such a difficult moment.

Bibliography

Introduction

- Baglione, L. A. (2016) *Writing a Research Paper in Political Science. A Practical Guide to Inquiry, Struture, and Methods*. Thousand Oaks, CA: CQ.
- Harman, S. and Williams, D. (2013) *Governing the world?*, London-New York Routledge.

Chapter 1

- Conferenza organizzata da NATO Defense College Foundation in partnership con the Balkan Trust for Democracy (2018, June 15th) *NATO versus the new global threats*. NATO Defense College Foundation.
- Felician, S. (2010) *Le armi di distruzione di massa*. Centro militare di studi strategici.
- Foradori, P. and Giacomello, G. (2014) *Le nuove minacce globali alla sicurezza*. Il Mulino.
- Harman S. and Williams D. (2013) *Governing the World? Cases in Global Governance*. London - New York: Routledge.
- Marcuzzi, S. (2018) *Hybrid Warfare in Historical Perspectives,* NATO Defense College Foundation.
- Minuto Rizzo, A. (2017) *Radicalismo, migrazioni e minacce ibride*. Pacini Giuridica
- Mockaitis, T. R. (2017) *Conventional and Unconventional War: A History of Conflict in the Modern World*. ABC-CLIO.
- Nagao, Y. (2011) Unconventional Warfare: A Historical Perspective. Report

Chapter 2

- Ansalone, G. (2012) *Minacce alla sicurezz*a: *Cyberspazio e nuove sfide*. Gnosis
- Chambers, J. (1999) *Chemical and Biological weapons and warfare*. NY: Oxford University Press
- Croddy, E. (2002) *Chimical and biological warfare*. NY: Springer-Verlag
- Fédération internationale des droits de l'homme (2016) Rapport d'enquête sur l'Affaire Amesys .
- Felician, S. (2010) *Le armi di distruzione di massa*. Centro militare di studi strategici
- Global Challenges Foundation (2017) Global Catastrophic Risks Report
- Hutchinson, R. (2003) *Le armi di distruzione di massa*. Roma: Newton Compton
- IFRI (2018) Cybersécurité: extension du domaine de la lutte. *Politique Etrangère* 83
- Kelle, A. (2007) *Controlling biological weapons*. New York: Palgrave

- Spratt, D. and Dunlop, I. (2019, May) Existential climate- related security risk: a scenario approach. BT Report
- Spratt, D. and Dunlop, I. (2018, August) National Centre for Climate Restoration. *What lies beneath? The understatement of existential climate risk*. Melbourne: Breakthrough.
- Teti, A. (2018) *Cyber Espionage e Cyber Counterintelligence: Spionaggio e controspionaggio cibernetico*. Rubbettino
- Xu, Y., and Ramanathan, V. (2017) Well below 2 °C: Mitigation strategies for avoiding dangerous to catastrophic climate changes. Proceedings of the National Academy of Sciences.

Chapter 3

- Finnish Institute of International Affairs. (2018, June) The security strategies of the USA, China, Russia and the EU. Report.
- Heath, T. R., Gunness, K. and Cooper, C. A. (2016) *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities.* Santa Monica: RAND
- Maurer, T. and Hinck, G. (2018, December) *Russia's Cybersecurity Strategy*. ISPI
- Messa, P. (2018, October) *L'era dello sharp power. La guerra (cyber) al potere.* Milano: EGEA Università Bocconi Editore.
- NATO Defence College Foundation (2019) *Shaping Security Horizons: Strategic trends 2012-2019*. Roma: AGRA
- Roffey, R. and Tunemalm, A. (2017, October) Biological Weapons Allegations: A Russian Propaganda Tool to Negatively Implicate the United States*. The Journal of Slavic Military Studies 30*
- Soldatov, A. and Borogan, I. (2018, October) *Hacks, leaks and disruptions Russian cyber strategies*. European Union Institute for Security Studies.
- The Kremlin (2018, December) Russian National Security Strategy. Report.
- The Politburo of the Communist Party of China (2015, January) Outline of the National Security Strategy. Report.
- The White House (2017, December). National security strategy of the United States of America. Report.
- World Economic Forum (2019) Global Risks Report.

Chapter 4

- Bailes, A. J. K., Dunay, P., Guang, P. and Troitskiy, M. (2007, May) The Shanghai Cooperation Organization, *Stockholm International Peace Research Institute* (SIPRI) Policy Paper 17.
- COM/2018/773 final. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank. A Clean Planet for all A European strategic long-term vision for a prosperous, modern, competitive and climate neutral economy.
- Conferenza organizzata da NATO Defense College Foundation in partnership con the Balkan Trust for Democracy (2018, June 15th) *NATO versus the new global threats*. NATO Defense College Foundation.
- Council Decision (CFSP) 2019/97 (2019, January). Council Decision in support of the Biological and Toxin Weapons Convention in the framework of the EU Strategy against Proliferation of Weapons of Mass Destruction.
- De Haas, M. and Van der Putter, F. (2007, November) Netherlands Institute of International Relations Clingendael, *The Shanghai Cooperation Organization; Towards a full-grown security alliance?,* The Hague: Marcel de Haas.
- European Council (2014, October) 2030 Framework for climate and energy. Report.
- European Parliament (2019, April) Regulation of the European Parliament and of the Council on ENISA and on information and communications technology cybersecurity certification and repealing regulation (EU) No 526/2013 (Cybersecurity Act).
- European Parliament Briefing (2015, June) The Shanghai Cooperation Organization.
- European Union Global Strategy (2016)
- EGS (2018, June) From Shared Vision to Common Action: A Global Strategy for the European Union’s Foreign and Security Policy. Implementation Report Year 2
- Finnish Institute of International Affairs (2018, June). The security strategies of the USA, China, Russia and the EU: Report.
- Guterres, A. (2018). Report of the Secretary-General of United Nations on the work of the Organization.
- International Telecommunication Union (2018). Guide to Developing a National Cybersecurity Strategy.
- Lippert, T. H. (2016) NATO, Climate Change, and International Security: A Risk Governance Approach. Report.

- NATO (2009) NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear (CBRN) Threats.
- NATO Strategic Concept (2010).
- Keohane, R.O. (1990). Multilateralism: An Agenda for Research. *International. Journal* 45 (4)

Chapter 5

- Ambassador Masood Khan (2008, December) 6th Review Conference of the Biological Weapons Convention. Closing Remarks.
- Documento di Sicurezza Nazionale (2018) Report.
- EU Strategy for Adaptation to Climate Change (2013) Report.
- IPCC (2014). Climate Change 2014: Impacts, Adaptation, and Vulnerability. Working Group II Contribution to the IPCC 5th Assessment Report.
- Maylis, D., Konovalova, E., and Bertherat, C. (2017) Political Affairs Interns, BWC Implementation Support Unit, UNODA Geneva Branch. *Biological Weapons Convention 8th Review Conference outcome: below expectations.*
- Ministero dell'Ambiente e della Tutela del territorio e del mare (2014) Strategia Nazionale di Adattamento al Cambiamento Climatico (SNAC).
- Nuti, L. (2007, September). *La sfida nucleare. La politica estera italiana e le armi atomiche 1945-1991*. Il Mulino
- Relazione sulla politica dell'informazione per la sicurezza (2018)
- Report of the European Environment Agency (2010) Climate change impacts and vulnerability in Europe 2012. Report No 12/2012.
- Terzi, G. (2006) L'Italia e la non proliferazione delle armi di distruzione di massa. *Affari Esteri* 150
- Tucker, J. B. (2007, January) *The 6th Review Conference of the Biological Weapons Convention: Success or Failure*? Centre for Non-proliferation Studies.

Chapter 6

- Camilli, E. (2014, March) *Sicurezza Nazionale tra concetto e strategia*. Sistema d'informazione per la sicurezza della Repubblica.
- Finnish Institute of International Affairs. (2018, June) The security strategies of the USA, China, Russia and the EU: Report.

Abstract

The research question (RQ) behind this thesis is "if and why states and international organizations have different perspectives of emerging threats, although the majority of threats are global and demand a comprehensive approach to be solved?". Such a question can easier find a response if divided in two part. The first part concerns an in-depth analysis about emerging threats (chapter 2), while the second one a pragmatical focus on states and international organisations' security approach (chapters 3,4,5). Nonetheless, it is important to clarify since the beginning (1 chapter) the term "security" and the evolution of the concept of "threat", which are going to frame the entire text. The matter of security has traditionally occupied a priority position in the hierarchy of public goods supplied by states, not only because it is linked to the exercise of the "monopoly of force" - which is the main feature of a state - as theorized by Max Weber, but also because it is not possible to provide other services, such as welfare, education and health, in an unstable or insecure environment. Thus, security is the basic condition of social living. On an academic level, security studies arose in the 1980s as an evolution of "strategic studies" and with the publication of *People, States and Fear* by Barry Buzan (1983), security starts being considered as a subjective and individual condition, influenced by emotions and people's perception of the menace. A further evolution occurred with the raise of new security actors, alongside the state, and the passage from its international dimension to the "global" one (Foradori and Giacomello 2014: 292). The term global security refers to the extent and the interconnected nature of threats emerged in the era of globalization. For example, the current fragility in Libya or Syria is stirring up terrorism and insurrections and such disorders are exploited by criminal networks to increase income, selling arms and drug. This instability can be also projected in the so-called "democratic countries" through migratory flows and crisis in energy supplies. Consequently, instability is the root of every new threat and should be addressed to face them. Nevertheless, such an instability is progressively enhancing in the last few years, aggravated also by tools of scientific and technological progress - like nuclear physics and cyber-technology. As a result, global threats are more complex than ever, and states cannot to deal with them alone. The employment of a comprehensive approach differs from the traditional security strategies, which followed a realist disposition. At the base of the realism is the assumption that there is a sense of threat in the international system in itself and each State should deal with that through the use of force (Waltz 1959: 160) and protecting its borders against external threats. Thus, according to realism, "no state will never sacrifice its interests to serve the larger community" (Frankel 1996: 15). In 1994, this paradigm was questioned by the UN Human Development Report, which introduces the "human security". This term was defined as safety from chronic threats, such as hunger, disease and repression, and protection from sudden and hurtful disruptions in the patterns of daily life. This interpretation is interesting because - taking into account the current security environment and the raise of new unconventional threats - it is undeniable that under the security umbrella are issues beyond territorial

conflicts and inter-state aggression. According to the Head of the Italian Delegation to the NATO Parliamentary Assembly, Andrea Manciulli, is true that at the macro-level it is re-emerging a sort of strategic confrontation between great powers, but in the meanwhile, at a very micro-level, new tensions such as cyber or hybrid threats are changing the nature of conflicts[142]. Indeed, today smaller actors are able to threaten much bigger and stronger adversaries exploiting the asymmetry of the threat and the use of high-tech tools. Thus, the most common and ancient threat, namely war, was ceasing to be the most serious global threat to human life (Stephen Walt 1991: 212) and inter-state wars decline (Miall *et al* 2005: p. 28) giving way to asymmetrical conflicts. The reason why traditional war has evolved towards such an asymmetrical nature reside in the increasing role of people in armed conflicts, which led firstly to create unconventional wars and then hybrid one[143]. The concept of hybrid war emerged just in the last few years, since the 9/11 terrorist attack. This type of confrontation embraces every aspect of modern conflicts, including terrorism, economic warfare, mass migration and organized crime[144]. Since new technologies are growing increasingly cheap and available, the mass involvement is increasing, enhancing the number of channels of vulnerability and hence the dangerousness of hybrid confrontations. For instance, in the cyberspace it is possible not only to amplify the conflict both in time and space, but also to inflict a harm escaping the "attribution of responsibility". Consider the absence of any laws prohibiting cybercrime in some countries or the complete lack of control over other dangerous instruments, such as biological or chemical agents, the modern notion of the state as the custodian of the monopoly of legitimate violence has been eroded[145]. One solution against that is "resiliency". Basically, it consists in a reinforcement of the internal structure of a state, not only in term of physic and material resources but concerning the psychological and political aspect of populations. In an environment of instability and scientific and technological development, resilience can be effective only if applied in a cooperative and collaborative environment between states[146].

Before analysing states and IOs responses, it is important to circumscribe the broad spectrum of the current global challenges, including those more ignored and potentially dangerous. Among these it is evident the role of the cyberspace which, although it is evident and prominent in the security debates, it is living a continuous expansion. Other relevant and less popular "weapons" that can be employed in these new hybrid contexts, are virus and bacteria, potentially used by malicious actors to sow chaos or weaken a population. Nowadays, it cannot be also ignored that climate change's effects, which more evident than ever. It is enough to open a newspaper or turn on the TV to understand that it is a serious challenge, heavily debated by activists, like Greta Thunberg, and international organisations. According to the Emeritus Director of the Potsdam

[142] See Manciulli (2018: 15-16)
[143] See Nagao (2011: 1)
[144] See Minuto Rizzo (2017: 117)
[145] See Marcuzzi (2018: 6)
[146] See Minuto Rizzo (2017: 119)

Institute, Prof. Hans Joachim Schellnhuber, “climate change is now reaching the end-game, where very soon humanity must choose between taking unprecedented action or accepting that it has been left too late and bear the consequences”. (Schellnhuber 2018: 3). Nonetheless, it is difficult to assess the actual risk of climate change because it is impossible to learn from mistakes or rely on institutions, moral norms, or social attitudes developed from experience. Moreover, predict climate change impacts is particularly complex because of the various ecosystems' responses and the heterogeneity in impacts and adaptive capacity (Kreigler *et al*. 2012). In this sense, many developed countries have refocused their priorities, trying to reduce greenhouse emissions or investing in adaptation strategies to reduce adverse consequences. Given that these strategies require significant financial investment, it follows that developing nations - who have extremely limited finances and therefore a limited capacity to adapt - will be impacted more severely by climate change effects (NCCARF and WHO 2013). In addition, in many parts of the world there are very limited funding dedicated to face global warming because of a certain scepticism regarding the scope and magnitude of the predicted outcomes. Beyond these limits, the real enemy of climate change prevention remains the massive inertia of global leaders. Thus, a clear focus on the extremely serious outcomes - that are higher than is generally understood - by state government is required to carry on a prudent risk-management. Moreover, a policy integrated across national, regional and global boundaries, and which recognizes that issues such as climate, energy, the ecological crisis and resources overuse are inextricable, is essential[147]. Such a policy should act as the driver of a massive global mobilization of resources to build a zero-emissions industrial system, with the final aim to restore a safe climate. Besides the physical harm that can be inflicted to the population and its resources by the effects of climate change, the action of certain viruses or microorganisms can imperceptibly have the same effects. This is defined as biological threat, a collateral effect of the biological research carried on eradicating diseases. Such researches led soon to discover how the presence of pathogenic viruses and microorganism can reduce people possibilities of working in short or long term and, in certain cases, lead directly to death. This finding has been exploited for centuries to deliberately infect or attack people with these viruses or micro-organisms, creating a sneaky and advanced tool of warfare. Indeed, biological agents can be dispersed in the environment in many ways, not only with a person-to-person contagion, but also being inserted inside a cavity of artillery shells, bombs, missiles or rockets and, at the moment of the shot, be released. In addition, biological weapons can act through insects or animals and contaminate water and crops, damaging the production chains of human food[148]. The capacity to spread quickly through cheap ways is the reason why such a weapon can be exploited by terrorist groups to sow chaos. This phenomenon is called “bioterrorism”. The bioterrorism has several implications that go beyond the physical attack alone. Without hypothesizing an apocalyptic scenario and relying only on actual cases, a biological strike sows panic and fear in the population because the enemy is

[147] See Spratt and Dunlop (2019: 7)

[148] See Felician (2010: 42)

not known, not seen and there is always the possibility of contagion. Moreover, it affects the security and functionality of state main services, like the health and transportation systems[149]. This is important because a state cannot work and maintain the security of citizens without effective critical infrastructures. Critical infrastructures are at the same time the cornerstone and the main weakness of a state. In the last few years, these has been threatening several times by cyber-attacks, which in this way can block the entire state system. The reason why cyber-attacks are so dangerous and effective depends on the nature of cyber-space. The cyber-space is born with the development of internet and it has soon become an area of absolute chaos because of internet low-cost accessibility and its pervasiveness. Indeed, the cyber space is based on a paradox: if on one hand the technological mastery is necessary to dominate cyberspace in a potential cyber-war, on the other side a basic cyber knowledge it is enough to allow individuals to trigger a cyber-attack[150]. This last feature permits the access of a large number of actors, to hide criminal networks and malicious actors and makes difficult to identify the guilty. Such an uncertainty makes the principle of self-defence and retaliation - the two paramount principles that ruling warfare - very fragile and precarious. The situation is aggravated by the relationship between cyber actors, namely state services and private agencies. Indeed, there are cases of collusion between the government and private group, which are employed by the state in itself to avoid international repercussions. As a result, the cyber space in currently a place of strategic competition. The keywords to contrast the cyber menace are coordination and clarity of the command and control lines, thus a comprehensive approach which would involve different investment realities and agencies devoted to the protection of critical infrastructures[151].

This descriptive part has been useful to circumscribe the global threats to take into account, namely climate change effects, biological threat / bioterrorism and cyber menaces. Now, the thesis proceeds with the case studies section, essential to draft the final analysis and give an answer to the RQ. Indeed, through the analysis of states and international organisations' security strategy emerged that in the last few years there is a trend towards a more realist and nationalist approach, provoked by an evident shift in the governance and government of various important influential countries and the alleged decline of liberal democracy[152]. All of this influences the main bodies which appear more untrustworthy and manipulate citizens' security perception to protect their own personal interest. This is evident especially in the last American National Security Strategy (USNSS) and in that of China and Russia. The last USNSS was drafted in 2017, after the installation of Trump in the White House. Such an edition presents few elements of continuity with the previous administration and several points in contrast. Indeed, it is based on Republicans' priorities, even though basic American values remain unquestionable. For instance, the US has maintained the EU-NATO partnership as a cornerstone in its

[149] See Felician (2010: 42-44)
[150] See Ansalone (2012: 37)
[151] See Teti (2018)
[152] See Alessandro Politi (2019:11-12)

strategy, while several multilateral agreements, such as TPP, NAFTA and the Paris Agreement, are questioned in favour of a more bilateral approach for future negotiations[153]. This occurs because the new US narrative prioritizes dangers associated with foreign states rather than the fight against global threats. The only exception is the particular attention devoted to cyber-security, drafted in the first pillar dedicated to "Protect the American People, the Homeland and the American Way of Life". In this section, the President shows his awareness about adversaries' low cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business[154]. With regards to the other global threats that has been mentioned, namely climate change and biological threats, there are only few remarks. The biological threat is considered referring to the 2001 anthrax attacks against the USA and recognizing the potential harm against lives, economy, and confidence in government institutions that it can inflict[155]. Regarding climate change issues, they are not directly mentioned and there is only some line concerning the importance of energy. Nonetheless, it is evident - despite the formal US commitment to support energy initiatives with the aim to safeguard the environment - that Trump priorities are not about climate, but about economic growth. This assumption is demonstrated by the US withdrawal from the Paris Agreement, which has marked a rupture with the previous administration. In fact, Obama considered dangerous to ignore global problems such as climate change, while in President Trump vision the danger resides in the dilution of US national interests, caused by the over-committing to broad multilateral agreements that ignore how competitors, such as China, Russia or Iran, can take self-interested advantage of them[156]. Such a negative perception of international relations is shared by Russia, which assumed in its last security strategy (2015, December 31st) that the world should be interpreted through the prism of "strategic stability". This led to prioritize the military component of national security to assure a dominant position for Russia in the world. Such a military component includes the full spectrum of means in the competition for power and prestige, abandoning the previous idea of economic and technological transformation as a route to Russia's global economic competitiveness. At the root of this change is Putin's third presidential term, when the development of the defence industry was identified as the driver of Russia's modernization[157]. Indeed, President Putin recognises the erosion of Russian values, the weakening of the "historical unity of the peoples of Russia" (Vladimir Putin 2015) as main threats, alongside the external cultural and information expansion, with tacit references to the conflict with the West. Dealing with the current intrastate instability and the consequent spread of terrorism, interethnic strife, religious enmity, and other manifestations of extremism, means for

[153] See Donald Trump (2017: 1)
[154] See Donald Trump (2017: 4)
[155] See Donald Trump (2017: 9)
[156] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 18)
[157] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 42)

Russia to apply an "asymmetric approach". The asymmetric approach exploits the strengths of Russia, namely the weaponization of information, technology and organizations, to compensate its relative weakness in military-technological development. The main objective of this approach is expressed in Article 36, in which is summarized Russia's strategy of "active defence", namely the activation of a set of non-military measures - i.e. informational, political, economic, organizational and cyber resources - to neutralize a potential threat to Russian national interests. Among the non-military measures, cyber-security has a prominent role. It is interesting that rarely it is heard the word "cyberwarfare" in Moscow. Russians prefer to employ the term "information warfare" (*informatsionnaya voyna*), a name used by Russian propaganda to expose or condemn alleged interference of the West in its domestic affairs[158]. In putting its cyber-defence doctrines into practice, one of the tactics employed by Russia is to co-opt with criminal hackers. In fact, former Soviet states have large populations of highly educated, technically skilled individuals who have few legitimate economic opportunities. Such a situation leads some of them to turn into hackers and work for criminal enterprises. The nexus between the state and criminal hackers is founded on a tacit bargain under which hackers will not target people within the former Soviet states and the Russian state will tolerate their criminal activity[159]. Hence, Russian government is focusing its security strategy on combining traditional military means, such as WMD, with cyber tools to protect Russian interests against the world. With this perception, global challenges like climate change are always subordinated to political interest and often ignored as a potential danger. The same approach is followed by China with few differences. In October 2017, Xi Jinping announced the beginning of a New Era of Socialism with Chinese characteristics which would lead to the completion of the "socialist modernization" by 2035 and China's emergence as one of the leading nations in the world with a world-class military in the 2050s[160]. This vision of national development and revitalization is known as the "Chinese Dream", a dream which seeks to ensure economic prosperity, social stability, and an overall higher quality of life for Chinese citizens. Beijing's security strategy revitalization has promoted at the regional level security-related organizations and institutions that do not include U.S. representation, such as the Conference on Interaction and Confidence Building Measures (CICA) and the Shanghai Cooperation Organization (SCO). Furthermore, the Chinese confidence about the leading role of China in the world was seen when the government flaunted its Belt and Road Initiative and took a hard line on territorial issues such as the South China Sea and Taiwan[161]. Besides shaping the international environment, China's security strategy aims to enhance protection for its core interests, including those of national security, territory, sovereignty, and economic development. In the "Outline of the National Security Strategy", passed by the Politburo in January 2015, this idea was already presented. Over time, China's defence policy has similarly moved beyond a focus

[158] See Paolo Messa (2018: 87)
[159] See Tim Maurer and Garrett Hinck (2018)
[160] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 31)
[161] See Elenoire Laudieri (2019: 40)

on homeland defence to also cover regional threats and security needs beyond China's immediate periphery. This has been cause and consequence of the escalating trade war between China and the US, worried about the raising impact of Chinese power in the world. Thus, such economic issues led China to abandon its role of economic giant in favour of massive investments in defence, of which the primary guarantor is the People's Liberation Army's (PLA's). The PLA guarantees China's national security and supports armed forces inside the country, using two key military strategy called "active defence", as Russia, and "informatized" war. The PLA is also working to develop greater cyber capabilities to degrade the adversary ones and hold critical infrastructure at risk during a conflict. It is important to clarify that the definition of cyber usually employed by Western experts and media, namely a domain enclosed in Internet and in the electronic world, is not the same applied by Chinese expert, media and government agencies. The Chinese consider the cyber domain as part of a broader framework, which includes the information space, namely a set of information of which citizens can access through internet, media and oral communication. Moreover, the term cyberwarfare is used in China only in reference to Western cyber operations, as in the Russian interpretation, and its ultimate goal is the idea of *Sha Shou Jian*, namely "if you get the proper resources, you can defeat an enemy much bigger and stronger than you"[162]. The Politburo and the Kremlin shared also the vision of uncontrolled information as a danger rather than an opportunity, which justifies the priority role of the state in controlling cyberspace, media and the web. This is the result of political cultures which prioritize the maintenance of social order above citizens' privacy and freedom of thought. Thus, while cyber assumes an important role for all of those states, the US, China and Russia, climate change issues remain completely ignored. In the case of China, the question is quite different because China includes environmental-related policy objectives to its overall program, but their implementation has remained subordinated to Chinese core economic interests. This occurs because, as the PRC government researchers state, cheaper, pollutants and more abundant energy resources are essential to China's continued economic growth[163].

Taking everything into account, global issues find little ground in state security strategy, but they should be better address in multilateral assets. This is not always true, especially in the case of NATO and SCO, two organisations strongly influenced by their leading countries, namely the US, Russia and China. The last NATO's Strategic Concept was drafted in 2010 and assess the value and importance of working with partners from across the globe. This official document outlines NATO's enduring purpose and nature and its fundamental security tasks, but it is becoming quite obsolete for the current international situation. The fundamental points that have been underestimated in 2010 Strategy are the rising instability, the return of great States power politics, the rise of potential peer competitors for NATO and new unconventional threats. The rude awakening for the Alliance has been in 2014 Russia's illegal annexation of Crimea, which changed the

[162] See Paolo Messa (2018: 93-100)
[163] See Alessandro Politi (2019: 13)

rules of the game and led NATO to review its strategies. Although it is not easy for a conventional defence organization like NATO to face such new issues, the Alliance is actually preparing to deal with new threats adopting a 360 degrees security approach, in particular to face cyber and hybrid threats. Practically, NATO have adopted an enhanced policy and action plan to maintain robust cyber defences. The policy also reflects Allied decisions on issues such as streamlined cyber defence governance, procedures for assistance to Allied countries, and the integration of cyber defence into operational planning (including civil emergency planning). In addition, the policy defines ways to take forward awareness and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations like the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). It also foresees boosting NATO's cooperation with industry, including on information-sharing and the exchange of best practices through the NATO Industry Cyber Partnership[164]. NATO is also changing its approach towards traditional threats. For example, regarding the proliferation of weapons of mass destruction (WMD) and their means of delivery, NATO is taking seriously into account every possibility. For example, during the 2006 Riga Summit, was already noted in the Comprehensive Political Guidance that the spread of WMD and the possibility that terrorists will acquire them, especially biological ones, would be the principal threats to the Alliance over the next 10-15 years. Therefore, the Alliance still seeks to prevent their proliferation through an active political agenda of arms control, disarmament and non-proliferation as well as by developing and harmonising defence capabilities. Moreover, regular consultations, information and intelligence sharing among Alliance members, partners, international organisations and national authorities, where appropriate, help foster a common understanding of potential WMD proliferation threats by States and non-State actors. Thus, NATO appears an effective and flexible security organisation, despite its traditional structure. However, if in the past NATO capabilities were assured by the political will of its member states, currently the Alliance's cohesion is challenged by Brexit, mass migration, financial fragility and trade wars. Some countries have an increasingly diverging approach to the political values and practices of the Alliance and the wave of neo-national thinking together with the rise of new anti-establishment parties in different democracies is putting into question its usefulness[165]. This instability within and outside the Alliance is aggravated by a strong US leadership and ignored phenomena like climate change, which is threatening security worldwide. This lack of cohesion is even more evident in the case of SCO. Formally, the members of the SCO, i.e. China, the Russian Federation, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, has signed "The Shanghai convention on fight against terrorism, separatism and extremism" which should have created mutual trust, friendship and cooperation between its members. This convention is against the so-called "three evils" (i.e. terrorism, separatism and extremism) and established a common understanding between the parties

[164] See NATO Official web site: https://www.nato.int/cps/en/natohq/topics_78170.htm (July 2018)

[165] See Berti B. (June 2018: 41-43)

on what these terms mean and commits them to reciprocally extradite persons committing such crimes. Thus, member states should cooperate through the exchange of information and intelligence, by meeting requests for help in operational search actions, in developing and implementing measures to prevent, identify and suppress offending actions and in collaborating to stop the flow of finance and equipment to the guilty parties. Over the year, SCO has worked hard to establish its profile and expand its activities including also the fight against universal problems such as drug trafficking, cyber-sabotage and aspects of weapons of mass destruction (WMD) proliferation. Recently, one of the main SCO's concerns is the "information security", an equivalent to what Westerners call "cybersecurity", which led to draft the Agreement on the Information Security Area in 2009[166]. Nonetheless, the SCO still lacks in practice a considerable number of essential features to be a proper security organization. Indeed, it has not an integrated military-political structure with permanent operational headquarters, a rapid reaction force and continuous political deliberations and a real internal cohesion. The lack of a common political will is the reason why the SCO agenda remains tightly focus on conflict avoidance and peaceful dialogue among its members, addressing threats only if affecting directly the stability between its member states, such as in the case of cyber-threats and WMD (only in the field of nuclear proliferation)[167]. Consequently, global menaces like the effect of climate change are ignored. These two cases show how is becoming difficult to address global threats and cooperate even in a multilateral framework. However, there are also examples of efficient international organisations, which are able to grasp current global issues and deal with them. This is the case of the EU and the UN. The EU adopted in June 2016 its collective security strategy, called the European Global Strategy (EGS), which is complementary to the strategies of its individual member states. The EGS reflects the perceived need for Europe, both inside the Union and outside among partners, to become a more capable foreign and security policy actor, after decades of focusing on economic integration. In this strategy, the common recognized five key threats, namely regional conflicts, state failure, organized crime, terrorism and WMD proliferation, were complemented by new ones, including military aggression by Russia against Ukraine, turmoil in North Africa and the Middle East, the concomitant migration crisis, climate change and hybrid threats like cyber-attacks, disinformation and election-meddling. The EGS explicitly rejects the current realist worldview by stressing the EU's commitment to a win-win approach in IR and its openness to partnering with a wide range of actors, including states, civil society actors and the private sector. As a result, today the EU is probably the most strongly rules-based entity that goes beyond the nation-state, challenging the state-centric view of international relations. Nonetheless, while the EGS expresses strong continuity in terms of the European preference for a cooperative global order, it also claims that the higher sense of insecurity necessitates a new focus on self-protection[168]. Therefore, the

[166] See Toso de Alcântara B. (October 2018: 552-553).

[167] See De Haas M. and Van der Putter F. (November 2007: 57-59).

[168] See Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi (2018: 54)

EGS tries to find a new balance between idealist goals and what appears to be an increasingly realist world. The new approach focuses on improving the resilience of neighbours and helping them build up their own capabilities for improving security. At the same time, the increased concern about defending the EU's own territory and citizens has necessitated the rise of military aspects on the EU agenda. This does not exclude the EU commitment towards not-military problems like climate policies, which are still relevant and strengthened in the framework of the Paris Agreement. Indeed, the commitment of the EU and its Member States to fully implement the Paris Agreement has been reaffirmed in June 2017 by the European Council and then, in March 2018, the European Commission was invited by the Council in itself to present a proposal for a long-term EU climate strategy focused on greenhouse gas emissions reduction. Besides such a traditional EU's priority, an improvement in defence cooperation to face other security threats occurs. In the field of cyber-security, the Council adopted in May 2016 the European directive about Network and Information Security (NIS), coming into force in August 2016. The ultimate aim of NIS directive is to increase cooperation between Member States on vital cybersecurity question and define security obligations for operators of essential services (in critical sectors such as energy, transport, health and finance) and digital service providers (i.e. online markets, search engines and cloud services). Today, a further increase in cyber-attacks has led the EU to raise awareness and response among its Member States and European institutions. Thus, the Council have adopted a new cybersecurity regulation on April 9th, 2019 to introduce a set of certification systems at EU level, which is a series of rules, technical requirements and procedures capable of reducing market fragmentation, eliminating regulatory obstacles and establishing a climate of trust, and a new EU cybersecurity agency, that updates and replaces the current European Union Network and Information Security Agency (ENISA)[169]. Moreover, the EU is strengthening the field of cyber-defence, in which the Commission has already presented a comprehensive cybersecurity package in September 2017 to improve resilience, detection and response to threats. Overall, the EU is taking little steps to maintain and enhance security in the region, taking into account every potential threat. Even in the field of biological threat the EU has adopted in January 2019 a new Council Decision to support the Biological and Toxin Weapons Convention (BTWC). Such a decision has been justified by the speech of the Ambassador Walter Stevens, Head of the EU Delegation to the UN, who stated that "the threat of proliferation of biological and toxin weapons remains real in light of rapid advancements in life sciences. Thus, the European Union will remain vigilant and will ensure good governance structures, namely legislation, administration, judicial systems and law enforcement, to minimize the risk of malicious use of pathogens or toxins and respond quickly to them"[170]. The awareness about current emerging threats has been expressed also by the Secretary-General of United Nations (UN), Antonio Guterres, in the 2018 Report. Indeed, in this Report the expansion of new technological frontiers, namely artificial intelligence, genetic

[169] See European Parliament No 526/2013 (April 2019)

[170] See Council Decision (CFSP) 2019/97 (January 2019)

engineering and advances in cyberspace, the impacts of climate change, the threat of the use of weapons of mass destruction - especially the rise of chemical and biological weapons - and international terrorism are defined as the main challenges of the 21st century and thus they require a global response[171]. To date, UN have made relevant progress to deal with them, even if the limits of the UN structure impede to address directly certain issues. In fact, the primary responsible for the maintenance of international peace and security within UN's structure is the Security Council (UNSC), which takes the lead in determining the existence of a threat to the peace or act of aggression, calls upon the parties to a dispute to settle it by peaceful means and recommends methods of adjustment. However, the lack of a binding, legal oversight mechanism makes Security Council's efforts problematic and the power of veto of the five permanent members, i.e. China, France, Russia, United Kingdom and United States, have still the ability to block any "substantive" resolution. This rule not only prevents much needed international action from taking place, but it also undermines the entire basis of the UN, which is international cooperation.

It is undeniable how international cooperation has been undermined in these last years and the raising weakness of the multilateral agreements is a proof. In Italy such a situation has provoked controversial reaction, as enshrined in the *Relazione sulla politica dell'informazione per la sicurezza 2018*. In 2018, Italy has faced a volatile security environment characterized by instability and weaknesses, which has led to a rising fear of terrorism and hatred towards migrants, culminated with the favorable vote of both the Chamber of Deputies and the Senate of the so-called "Security Decree". The Security Decree, which has been already approved and published on the Official Gazette, is a package of measures wanted by the former Italian Minister of the Interior, Matteo Salvini about some delicate issues such as terrorism, the fight against mafias and public security. It includes also a part entirely focused on immigration. This last part is the most troubling, because it makes difficult for asylum seekers to stay in Italy and limits the work of the NGOs operating in the rescue of migrants. Regarding the public order, the Decree provides a substantial increase in the power of the mayor, the prefect, the quaestor and the law enforcement, introducing also harsher measures, like the use of tasers by the police. This is the outcome of the Italians' perception of "threat", a view aggravated by the current instable and competitive international scenario. The final result is the closure within the borders of the nation-state, national individualisms and a strict focus on domestic security rather than global one[172]. However, in the 21st century domestic security demand to enhance state cyber-capabilities, due to the significant propensity of various actors to resort to sophisticated cyber-attacks. In Italy, this led to a renewed determination to develop instruments of early detection, cyber-contrast and reaction. The most significant effort put in place by the Italian cyber-expertise concerns the contrasting of digital espionage campaigns and hybrid threat, whose operational translations have been amplified thanks to the digitization of social life. Along with the most

[171] See Guterres A. (2018: 3-4).

[172] See D.L. 113/2018 - A.C. 1346

significant initiatives for the development of the cyber national architecture, the operational start of the Cybernetic Security Team must be noted. It acts to prevent, prepare and response against cyber crisis, with the ultimate aim of strengthening the country's cyber defence capabilities. These capabilities have received a renewed impetus with the implementation of the "National Strategic Framework for cyber space security", established by the Cyber Technical Table (TTC) on April 3rd, 2013, and the subsequent "National Plan", which operates in the Security Information Department (DIS). Because of its centrality in the national "cyber ecosystem", the DIS has promoted various initiatives aimed at increasing the country's overall response capacity, actively contributing - in conjunction with other competent institutional actors - to ensure the timely transposition of the EU Directive 2016/1148 on the security of networks and information systems (NIS Directive) in Italy. This effort would be more concrete if associated with a parallel growth of cyber security culture which, apart from public and private subjects, interests every single citizen[173]. Thus, cyber has become recently a priority for Italy, leaving aside some older commitment, such as the disarmament and non-proliferation of WMD. This has always been a qualifying element of Italian foreign policy since 2001, based on a broad support from Parliament and civil society. In this field Italy has been active on several fronts, such as in the United Nations, the European Union, the G-8, in the review processes of the major international Conventions - first of all the Nuclear Non-Proliferation Treaty (NPT), the Conventions against Chemical and Biological weapons - and on a bilateral level with its main partners. Since the adoption of the European common approach to deal with WMD proliferation, Italian Permanent Representatives and Embassies has carried out daily activities and bilateral consultations with some of the main partners to advance its WMD non-proliferation program. For instance, it has demanded a more incisive role of the European Union, a progressive and extended adherence to the additional International Atomic Energy Agency (IAEA) protocols and the implementation of the G-8 Global partnership for the elimination of weapons of mass destruction. Many consultations confirmed the constructive role of Italy in that matter, which, through its balanced approach, has always represented a privileged interlocutor, both for nuclear countries and for the most active countries supporting nuclear disarmament[174]. However, today the multilateral approach toward the BTWC is controversial and present a wide range of limits due to the different visions between member states. These divisions are still present and they must be overcome to avoid the fragmentation of the regime against weapons of mass destruction, which would put in place less efficient strategies[175]. On the contrary, the approach inaugurated by the EU about climate change has been more successful and it has been efficiently transposed from the EU to Italy in the previous years. Indeed, on April 16th, 2013, the adoption of the European Climate Adaptation Strategy gave the impetus to European countries like Italy, lacking a coordinated national vision

[173] See Documento di Sicurezza Nazionale (2018: 16).
[174] See Terzi G. (2006: 336-337).
[175] See Maylis D., Konovalova E., and Bertherat C. (2017: 2-5).

on climate change adaptation, to begin the elaboration of a national strategy. Thus, the Italian National Strategy for adaptation to climate change (SNAC) has been created, developing a national vision about the common paths to follow in dealing with climate change, countering and mitigating its impacts. In this sense, SNAC identifies actions and guidelines to minimize the risks deriving from climate change, protect health, the well-being of the population, preserve the natural heritage and maintain or improve the resilience and adaptability of natural, social and economic systems[176]. This analysis is really important also for the Italian economic situation since a study developed by the World Bank have found out that climate change would reduce the Italian GDP in 2050 by -0.31 percent, due to an alleged decline in tourism. To deal with these problematic, the EU adaptation strategy have proposed some solutions, such as reducing water consumption, adapting building regulations, building flood defence systems and developing crops more resistant in drought conditions[177]. Initiatives like this, demonstrate that Italy maintains its role as multilateral player in the European and international chessboard. At the same time, it cannot be underestimated the rising geopolitical and geo-economic competition and the current pronounced push towards unilateralism. Today, the Italians perceive more domestic threats rather than global challenges, perception which led more to focus on the decrease in welfare levels and the socio-economic impact of illegal migration and terrorism. In the meanwhile, the scale and nature of the current global threats demonstrate that they are far from a solution and their negative effects are accelerating and degrading.

In brief, the case studies have confirmed that each state follows its priorities and adopts different responses to address global threats. These are less important in the approach of the US, Russia, China, SCO and NATO, while represent a real concern in the case of the EU, UN and - despite some controversy - Italy. The reason behind such a diversity can be found in the theory of the "red zone", assumed by the Italian analyst Edoardo Camilli in the framework of the Italian intelligence. According to Camilli, the choice of the priorities include in the national security strategy depends on the environment in which each state operates. This environment is affected by external inputs, like threats and international interests, to which the state must respond. Nonetheless, the rising complexity of the international system and the proliferation of several global threats demand to circumscribe the area of analysis to better grasp them. Then, the area of reference becomes a "red zone", defined by the interaction between inputs from the international system (threats and opportunities) and the state's ability to respond to these inputs, defending itself and promoting its interests. In other words, the shape and the extent of this area depend on state's capabilities and more a state is strong, in term of "smart power" (the union of hard and soft power), bigger the red zone will be. Following this reasoning, states prefer to focus on domestic security when they are uncapable to deal with global one. Such a weakness is the result of internal features, such as the lack of cohesion, less efficient institutions and the loss

[176] See Ministero dell'Ambiente e della Tutela del territorio e del mare (2014: 10)
[177] See EU Adaptation Strategy (2013)

of government legitimacy. These states are less able to turn resources into power and generate strategic plans to address global threats because the ruling elite is concerned only by its own political survival. In this context, the impact of values should not be underestimated. In effect, people have always interpreted the reality through the filter of cultural values and historical experiences, which make subjective the perception of world. In this sense, the strategic culture intervenes on the behaviour of the states influencing the understanding of the other, the morale of the troops in war, the politics of alignment and alliances and the state's sensitivity to threats, for instance towards those already suffered throughout history[178]. These are the reason why a national security strategy cannot be completely objective. According to this theory, the fact that in a globalized world the majority of states focus on internal security rather than global one is not a contradiction. In fact, globalization has provoked a rising instability worldwide, insecurity in the states and their consequent loss of power. Then, state weakness means a small “red zone”, focused on domestic security. As a result, today it is impossible to build a homogeneous global security strategy because of the global insecurity and global threats. This is a vicious cycle because in a close and heterogenous international scenario it is more difficult to find a common ground to deal with new threats. The key to overcome such a problem and maintain peace worldwide is to restore a cooperative environment, based on trusty multilateral assets and overcome state ancient grudges.

[178] See Camilli E. (2014: 8-12)