LUISS Università Guido Carli

Department of Political Science

Chair of Security Studies

The role of blockchain in revolutionizing and re-organizing security. Evidence and policy recommendations.

SUPERVISOR

Gen. S.A. Carlo MAGRASSI

CANDIDATE

Student Reg. No. 628832

Francesco GUASTAMACCHIA

CO-SUPERVISOR

Prof. Raffaele MARCHETTI

ACADEMIC YEAR 2016/2017

Acknowledgement

A compimento del mio percorso di studi, desidero ringraziare le molte persone che mi hanno affiancato per un tratto lungo o breve della navigazione.

Ringrazio il Generale S.A. Carlo Magrassi per l'opportunità di confrontarmi con temi poco noti ai più, ma di fondamentale importanza per il nostro Paese. Inoltre, al Colonnello Antonio Colella va il mio più sentito ringraziamento per il suo immancabile supporto nella stesura di questa tesi.

Sono infinitamente grato alla mia famiglia, per il supporto incondizionato e la fiducia che in me ha riposto durante questo tempestoso viaggio chiamato vita. Senza di Voi non avrei potuto inseguire i miei sogni.

Infine, dedico questa tesi all'Italia, il mio Paese, il Paese che amo e al quale sarò sempre fedele, che ogni giorno mi sorprende piacevolmente per lo straordinario ingegno a cui dà i natali.

Table of contents

1 Introduction....6
1.1 Research question....9
1.2 Research philosophy....10
2 Security studies: literature review....12
2.1 European schools....13
2.1.1 Critical Security Studies....14
2.1.2 The Copenhagen School....17
2.1.3 The Paris School....20
2.2 Critics to the European Schools of Security studies....22
2.2.1 The Welsh School....22
2.2.2 The Copenhagen School....23
2.3 The realist School: an American affair....25
2.3.1 Kenneth N. Waltz and neorealism....27
2.3.2 Offensive and Defensive Realism....28
2.4 The missing piece in Security Studies theories....30
2.4.1 An aside on the term Cyber Security. Defining the scope for analysts.....32
2.4.2 Actors' stance....34
2.4.3 Defining "liquid" boundaries: the cyberspace....35
3 Assessment of legal frameworks....37
3.1 Cyber security in Europe: timeline....37
3.2 The NIS Directive....39
3.2.1 Building cyber security capabilities at national level....41
3.2.2 EU-level cooperation....43
3.2.3 Operators of essential services and digital services providers....43
3.2.4 Critical evaluation....45
3.3 The Italian cyber security strategy and the cyber security framework....47
3.3.1 The national cyber security framework....48

3.3.2 The new Italian Decree for cyber security strategy *51*

3.3.3 Critical evaluation *56*

4 Revolution. The blockchain technology 58

4.1 DEFINITION AND CONCEPTUALIZATION 60

4.2 THE (BRIEF) HISTORY OF A PROMISING TECHNOLOGY 61

4.3 FEATURES AND CONFIGURATIONS 64

4.3.1 Public vs. private vs. hybrid blockchains *64*

4.3.2 Cryptography and pseudonymity *65*

4.3.3 Blockchain structure *67*

4.3.4 Licenses *68*

4.4 PARADIGM SHIFT IN CYBER SECURITY: THE STATE, DEFENSE AND BOUNDARIES 69

4.5 STRENGTHS AND WEAKNESSES 71

5 Applicability of blockchain solutions 74

5.1 APPLICATIONS OF THE BLOCKCHAIN 75

5.1.1 Anti-whistleblower systems *75*

5.1.2 Blockchain-enabled E-voting (BEV) systems *76*

5.1.3 Smart contracts *77*

5.1.4 Digital identity *79*

5.1.5 Supply chain *81*

5.1.6 Internet of Things (IoT) *82*

5.1.7 Applications in National Defense *83*

5.2 RISKS OF ADOPTING BLOCKCHAIN SOLUTIONS 84

6 Conclusions: Blockchain, the way ahead 87

Appendix 91

References 92

Abstract 102

1 Introduction

The advent of the Internet in the last decade of the twentieth century and its diffusion around the globe made social, economic, relational, military, political structures change dramatically. Time and space collapsed with the hyperbolic development of data transfer technologies. The fifth domain conceitedly acquired a considerable importance in people's everyday lives. Our memories are confined in a vulnerable and fragile domain.

What was first developed by Pentagon's DARPA in the 1960's for military purposes, and later by Tim Berners-Lee (1989), has changed the way we communicate, work and interact and has "come to characterize modern life" (Maj. Gen. Barrett et al., 2011, p. 34). The exchange of data has made costs drop and efficiency sharply increase. The digitalization is reaching all parts of society as CPUs' power is being used across every sector of the economy ranging from agriculture to the most advanced service sectors. Digital communities have also become a new factor within world politics and therefore also a new power element within the balance of sovereignty (Ibid.).

The development of technologies is constantly growing, creating a state of interconnectedness between different devices, as well as between industries and actors across the world (Eriksson & Giacomello, 2006). The growth has been so exponential that security implications did not have the chance to be studied and/or governed by policy analysts and theorists. Especially in Security Studies there has been little discussion on the implications of exchanging data in a space

where national borders constitute no frontier and actors of various nature operate.

Digital devices are also being produced at continually lower prices, making these technologies available to people outside first world countries. Therefore, these technologies are becoming obtainable for people outside the political and economic elite of the west (Eriksson & Giacomello, 2006). Moreover, the use of the Internet grew by roughly 924% in the period from 2000 to 2017 (Internet World Stats, 2017) and has become a fundamental component in daily life for all actors. It is estimated that in 2020 sixty per cent of the world's population will have access to the Internet. Fifty billion physical objects and devices will be connected to the Internet, which amounts to ten devices per online individual (Klimburg, 2012). The cyberspace is a global phenomenon that constitutes opportunities and challenges (Kuehl, 2009). For example, Dunn Cavelty's (2012) claim on the low probability of large scale cyberattacks is obsolete and nowadays there is the concrete possibility of large scale digital disasters that, like the Liberian case in 2016 (BBC.com, 2016), can halt an economy for entire days through Distributed Denial-of-Service (DDoS) attacks that take down the national cyberspace. A DDoS attack prevents the legitimate use of a service through multiple attacking entities (Mirkovic & Reiher, 2004). For NATO, this means that loss of access to the Internet will have critical consequences to the prosperity of a nation (Maj. Gen. Barrett et al., 2011).

I find it perhaps curious that although cyber threats are framed as a security issue, it seems no effective solution to monitor and secure cyberspace is tested as attacks continuously grow in number and complexity. Therefore, the

challenge is the effective governance of the flows of data without altering the features of the cyberspace, which means monitoring the cyberspace to spot harmful behaviors that could seriously damage national economies, infrastructures and citizens.

The blockchain technology creates the opportunity for analysts to study innovative policies to govern the cyberspace without a central authority. Blockchain is a sophisticated, distributed online ledger that has the potential, according to Goldman Sachs, to "change 'everything.'" From making businesses more efficient to recording property deeds to engendering the growth of 'smart' contracts, blockchain technology is now being investigated by a huge range of organizations and is attracting billions in venture funding. Even the U.S. Defence Advanced Research Projects Agency (DARPA) is investigating blockchain technology to "create an unhackable messaging system." In other words, a blockchain is a database that stores digital records. The group of network participants, all of whom can submit new records for inclusion, shares the database. However, those records are only added to the database based on the agreement, or consensus, of the majority of the group. Additionally, once the records are entered, they can never be changed or erased. In sum, blockchains record and secure digital information in such a way that it becomes the group's agreed-upon record of the past. This technology has the advantage to create the space for trustless exchanges of "data" exploiting the networked nature of the cyberspace. A further advantage is derived from the immediate measurability of the genuineness of exchanges by all the participants to the network.

Johan Eriksson and Giampiero Giacomello point out that past research on cyber security "has been idiosyncratic and policy oriented, with little or no effort made to apply or develop theory" (Eriksson & Giacomello, 2006, p. 3).

Hence, there is the need for a new paradigm in security that considers the features of the cyberspace, the role of actors in the cyberspace and the way blockchain can disrupt the governance of the cyberspace. This work aims at filling the gaps in the literature of Security Studies to better understand cyber security, provide it a definition that, without any pretense, can contribute to make order among the collection of definitions, and to highlight the implications in the governance of networks characterized by the active and immediate participation of national and international actors.

1.1 RESEARCH QUESTION

Academic works need to have a driving research question for the authors. It is perhaps useful to make the research question explicit.

Therefore, the questions that will be addressed are:

1) What is the expected change in approach in cyber security with the advent of blockchain?

I argue that the blockchain is a game-changer in cyber security, fostering public-private partnerships and changing the role of the State in providing cyber security. Using case studies, I highlight the shift in security from a top down guarantor, the State, to a bottom up approach, i.e. the distribution of responsibility among network participants. The decentralization is a key theme introduced by

the development and diffusion of this technology. However, cyber security has always been policy oriented and pragmatic. Giacomello stated: "[there has been] little or no effort made to apply or develop theory" (Eriksson & Giacomello, 2006, p. 3). The work aims to give theoretical contribution to the theory of cyber security. At the same time, the use of blockchain changes the roles and stances of the actors involved in security and this work takes this into account.

1.2 Research philosophy

Some may argue that a philosophy is needed to develop knowledge. Hence, the research philosophy is the foundation of the remaining part of this document. It includes the assumptions of how we see the world, choosing how the research is strategized and knowledge gained. Saunder, Thorn, & Lewis (2007) maintain that epistemological considerations are important, as we choose what is the acceptable knowledge for the field of study.

As I am approaching to cyber security, which is part of security, and therefore contextual to one of the five domains, I will adopt an interpretivist approach to the research. Interpretivists look at interactions and interpret them to obtain the meaning of social life (Abbott, 2004). Measurement is not part of interpretivism, but rather the meaning of social life is the focus of this philosophy.

Interpretivists argue that it is essential to acknowledge that the world is socially constructed and understand the difference between humans in our role as social actors. Moreover, the meaning of the object of research is subjective, as an objective view of the world is impossible. The interpretivist approach will thereby

support in understanding how cyber security is regarded and what should be done to deal with the issue.

"Knowledge is always situated", Abbott (2004) argues. I am aware of other potential outcomes of the research, but this study gives a picture of different situations and therefore is able to catch a small part of the trend in cyber security.

The work is divided as follows: chapter 2 presents an overview of the leading security schools and paradigms along with their critics and the proposal of a new theory of cyber security; chapter 3 offers the analysis of the recent normative initiatives in EU and in Italy to address the challenge of cyber security; chapter 4 is a primer on the history, the features, the implications of the blockchain technology and discusses its strengths and weaknesses; chapter 5 discusses the applicability of the blockchain and its risks; chapter 6 draws conclusions and policy recommendations.

2 Security studies: literature review

The European practice of Security Studies is highly discussed by the academic community as "schools" have developed in recent years. These researchers have drifted apart from sectorial manifestations of International Relations (IR) theories becoming an independent field. The discipline has always been led by United States research, this "sudden fertility of European soil" came as a surprise (Wæver, 2004). The debate within, among and across the "schools" is lively and it is almost entirely a European game.

Despite important contributions from non-western and American scholars, the emergence of distinct theories of security studies from IR is generally associated with European centres.

Authors in security studies dealt with "security theory" as a phenomenon in limited reviews and mostly focussed on IR (Baldwin, 1995; Booth, 1994; Buzan, 1984; Miller, 2001; Morgan, 1999; Smith, 1999; Wæver, 2004). Wæver (2004), for example, explores the peculiarity of European "schools" in order to assess the helpfulness of the theories in a core-periphery perspective [are the theories relevant in other contexts?] Following this preliminary attempt, this chapter aims at unlinking Security Studies from IR and developing an independent view on security theories. Therefore, the theories discussed below will overlap sometimes with IR theory, but they will be looked at in terms of security theory with the peculiar underlying criteria. Policy-oriented research, the core of security studies, is often a-theoretical or it mixes theories fragments in a common sense manner. This review will deal with the most influent European security

paradigms at the moment and will look at the debate between offensive and defensive realists to complete the picture of theoretical constellations.

European "schools" of security theory	United States "schools" of security theory
Critical Security Studies (Aberystwyth School or Welsh School)	Offensive realism
Copenhagen School	Defensive Realism
Paris School	other realisms (post-classical, …)
Radical post-modernists	Constructivism
feminists and other alternative theories	

The chapter is divided into four parts: the first section introduces the European security schools; the second section presents the critics to these theories; the third deals with the conflicting views pertaining to Realism; the fourth and last one describes the new frontier of cybersecurity and tries to navigate in relatively uncharted waters towards the conceptualization of a security paradigm in this highly contested environment.

2.1 EUROPEAN SCHOOLS

This section presents the reader with the main European theories and their characteristics. It is not an in-depth analysis of each theory, but rather an overview to build up the discussion of the following sections.

European scholars are very active in the debate on security. Several competing schools in security studies have established their authority without prevailing on the others: critical security studies (CSS), the Copenhagen School, radical post-

modernists, the Paris School, traditional realists and other alternative approaches. However, these debates enter marginally in the American journals of security studies. For example, *People, States and Fear* (Buzan, 1991) became one of the central references in Europe, while it had little impact in the United States. The relevant theories for this work are the Aberystwyth School (Wæver, 2004), the Copenhagen School (Mcsweeney, 1996) and the Paris School (Wæver, 2004).

2.1.1 Critical Security Studies

Critical Security Studies, also known as the Welsh School (Smith, 2005) or Aberystwyth School (Wæver, 2004) of security studies, is a school adopting the emancipatory approach. Since the publication of "security and Emancipation" (Booth, 1991), the scholars based in Aberystwyth University developed a critical approach towards security. Among the main proponents of the approach there are Ken Booth, Richard Wyn Jones and Pinar Bilgin.

CSS is an umbrella theory with a plurality of approaches. The approaches have in common the assumption of inability to give an ontological and epistemological explanation of security. In fact, this body of literature signals a critical stance to interpretations of orthodox positivist claims that State "sovereignty equals security". A key text for this approach is Critical Studies and World Politics (Booth, 2005). In the book the author makes an explicit attempt to link CSS to the post-Marxist Critical Theory. Critiquing traditional security theory, this theory offers a basis for social change. The test of this social theory is its capacity for fostering emancipation.

For Booth, Critical Security is both a theoretical commitment and a political orientation, the Theory is a critical and permanent exploration of the ontology, epistemology and praxis of security and politics has the role of enhancing security through emancipatory politics.

The social scientist has an active role in the social and political life. As such, theories are strongly shaped around social life. They are not mere descriptions of the *status quo.* The aim of CSS is the enhancement of human condition through the elimination of injustice/inequalities. Theory does not only present an expression of "the concrete historical situation", it also acts as "a force within it to stimulate change" (Adapted from Horkheimer, 1972). As Booth (2005) underscores, a critical theory of security "goes beyond problem-solving *within* the status quo and instead seeks to help engage with the problem *of* the status quo".

Linking security with emancipation is the battle of CSS scholars. In short, security is about freeing individuals from social and physical constraints and establishing principles of fairness to live fulfilled lives. The Welsh school argues that theory must take a stand and leave the way of neutrality. Ultimately, theory should have a commitment to progress. Security is, then, a means to an end that can always be improved through ongoing structural transformations based on the idea of emancipation.

Booth (1991) claims that the term *security* means the absence of threats. Emancipation is the means to free them from the constraints which hold them from carrying out what they would freely choose to do. Security and

emancipation represents two sides of the same coin. In this context, war and the threat of war are constraints on the same level of poverty, poor education, political oppression and so on. Emancipation produces true security, not power or order.

CSS meant to "broaden the neorealist conception of security to include a wider range of potential threats from economic and environmental issues to human rights and migration" and to "deepen the agenda of Security Studies by moving either down to the level of individual or human security or up to the level of international or global security, with regional and societal security as possible intermediate points" (Krause & Williams, 1996). Richard Wyn Jones (1999) agreed on the need to broaden the concept of security as abovementioned, he suggested to include referents other than the state, deepened to reflect "deeper assumptions about the nature of politics and the role of conflict in political life", and "focused, crucially on emancipation as the prism through which both theory and practice of security should be viewed". Proponents of the Welsh School thus recommend achieving security through the redressing of structures and relationships that hinder people from exploring their potential.

CSS embeds three key tenets, which are the idiosyncratic values of the approach:

- Politics and its implications are the substructure of security praxis;
- Individuals are the ultimate referents of security;
- Normative commitment towards emancipatory transformations.

In conclusion, this approach is an *enacting-oriented approach* that analyzes the political environment, its underlying assumptions and effects to challenge ideas

and practices of security. Insecurity is tackled through the attention towards social interactions and political struggle. Security then fosters the transformation of relationships of vulnerability through targeted political action, aimed at the disruption of constraints in people's lives so that they are enabled to make decision beyond survival.

2.1.2 The Copenhagen School

The appellation Copenhagen School was initially coined by Bill Mcsweeney (1996) in a critical review essay. The School usually refers to the work done since 1985 by the "European Security" research group at the Copenhagen Peace Research Institute.

The work of this group of scholars refers to the theoretical works of John L. Austin, Jacques Derrida, Carl Schmitt and Kenneth Waltz. The School is "built around three main ideas:1) securitization, 2) sectors and 3) regional security complexes" (Wæver, 2004). The central contribution, and identifying trait at least metatheoretically, is securitization. However, the remaining key concepts are useful to explain the dynamics in the development of the theory. Sectors and regional security complexes come from the work of Barry Buzan, although the main reference is the collective work of the Copenhagen School books (Buzan & Waever, 2003; Buzan, Wæver, & De Wilde, 1998). "Sectors" are divided into political, military, economic, societal and environmental security and were first explored in the book People, States and Fear (1991) by its author Barry Buzan. "security complexes" indicate the importance of the context in security analysis (the regional level) and facilitates analysts in providing them a scheme to link

security concerns and regional development (Buzan, 1991; Buzan & Waever, 2003; Wæver et al., 1993).

The School has become the pivotal point for significant theoretical debates on the implications of security discourse (Eriksson, 1999; Huysmans, 2006; Williams, 2003), the consequences of speech act epistemology (Balzacq, 2005; Bigo, 2002; Hansen, 2000), and the importance of the media and visual representations (Hansen, 2008; Williams, 2003).

These scholars define a security issue as "posing an existential threat to a designates referent object (traditionally, but not necessarily the state)" (Buzan et al., 1998; Wæver, 1995, 2004). The term security in the field of Security Studies has a different meaning from its everyday meaning. It is necessarily linked to power politics and ultimately, it is about "survival" (Buzan et al., 1998, p. 21). In the book "S*ecurity: a new framework for analysis",* the authors provided an innovative "constructivist operational method" to understand the timing and the way issues become security issues. They retain some assumptions of traditional security studies, the acceptance of a role of the State in security.

The definition of securitization is the intersubjective recognition of an *existential threat* sufficient to have relevant political implications. In other words, it refers to the process of transformation of an issue to a "security" issue by the *speech act* (Wæver, 1995) of an (élite) actor, a process of moving an issue out of the political sphere. Security issues are not objective and external but "determined by actors" and "socially constructed" (Buzan et al., 1998, p. 31). In the words of Wæver, "something is a security problem when the élites declare it so" (Wæver, 1995, p.

54). The referent object under threat is not always the State, but it differs from sector to sector. By speaking about "security" the securitizing actor is attempting to move the issue out of regular politics by means of audience persuasion and consensus. If the securitizing move is successful, the use of extraordinary measures to face the threat is granted. Nevertheless, it is not sure that the audience will accept the securitizing move (Buzan et al., 1998, p. 31). Securitized issues become too important to be subject to open debate and regular political procedure; they acquire priority in the eyes of the state's governing leaders. If the securitizing move has not reached enough momentum to begin emergency measures, it remains a securitizing move without securitization. Securitized issues acquire a rhetorical structure emphasizing urgency, survival and priority of action (Buzan et al., 1998, p. 26).

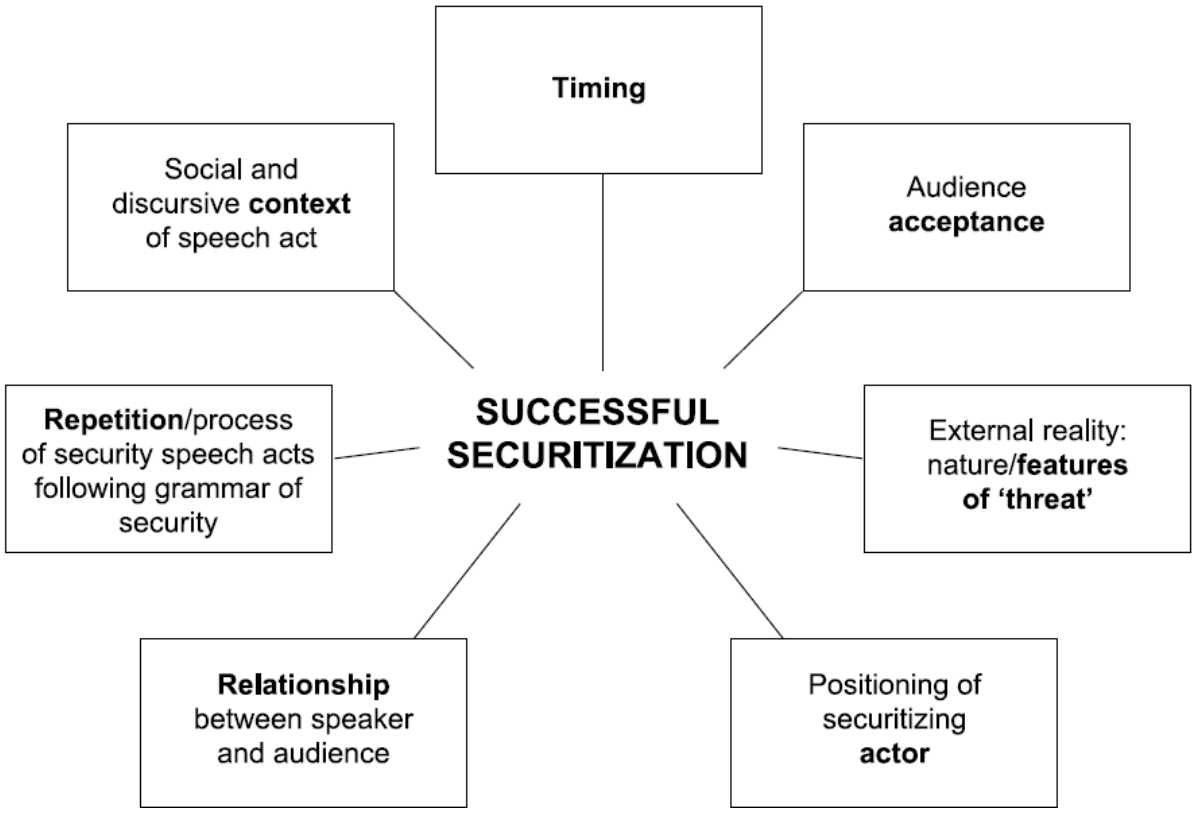

Figure 1 Factors of securitization success, from Shepherd, L.J. (2013). Critical approaches to security.

Desecuritization is, instead, the move out of the threat-defense sequence and reversion to the politicization of the issue. In a way is downgrading the priority of the matter from security issue to issue open to debate. Desecuritization offers advantages of focus, attention and mobilization. Wæver (2004) claims it is the optimal long-range option, since in a conflict resolution perspective it implies negotiation and she offers the process of European integration as an example. Buzan et al. (1998) argue that Desecuritization ought to be the aim, shifting issues back to politics with their peculiar negotiation.

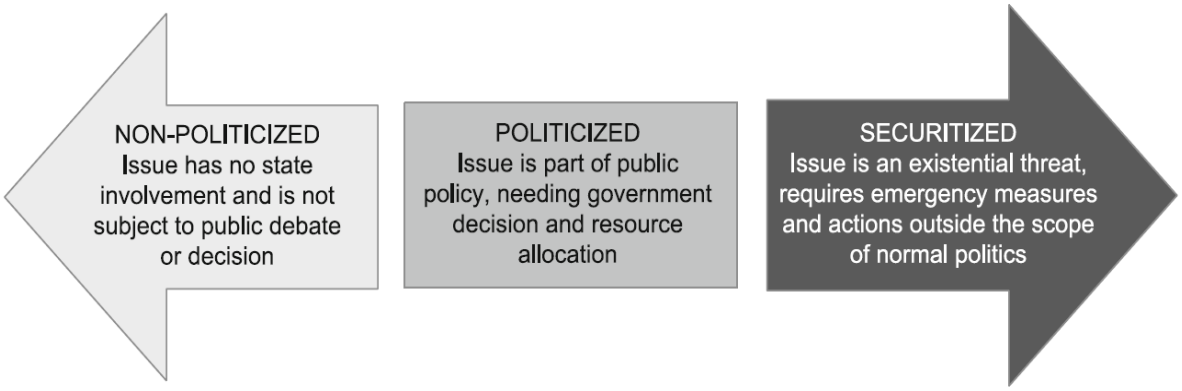

Figure 2 Issue scale, from Buzan, B. et al. (1998). Security: a new framework for analysis.

2.1.3 The Paris School

Pierre Bourdieu, Michel Foucault and other sociologists inspired the birth of a distinct theoretical development. Born in Paris, the homonym research program in security studies developed thanks to Didier Bigo and *his* journal "Cultures & Conflicts" on which a big amount of works has been published. Also, Jef Huysmans has dealt with the "Paris approach" and contributed to clarify and elaborate some of the most important assumptions of this theory.

The theoretical paradigm began with a different approach to studying security than the other non-traditionalist theories. Bigo wanted to study security practices to map actors and "fields" of security, a concept introduced in an earlier stage

and further elaborated in later works. It has soon become a well-documented and very elaborate mapping of practices also at the micro level by various agencies and firms involved in security. This approach has the advantage to include practices that deviate from official policy. It is also a quite demanding task, as the scholar has to penetrate and gain trust to study practices from a wide range of agencies and agents (Wæver, 2004).

Bigo (2002) argued that "security is often marked by the handing over of entire security fields to *professionals of unease* who are tasked with managing existing persistent threats and identifying new ones". These professionals are among the multitude of (in)securitizing actors in each field. Their speech acts, to use Wæver's lexicon, are not decisive but are the result of structural competition between actors over different, and sometimes contradictory, definition of security and different interests. He conceives (in)security as a by-product of security discourses and security policy.

Furthermore, an important piece of work by the same author argues that "transnational is blurring the distinction between the internal and external, and destabilizing related concepts: sovereignty, territoriality, security" (Bigo, 2000). He suggests that the merging of external and internal security is rearranging the way security is working. By saying this, Bigo is challenging the concept of State frontiers which are redrawn by the agencies to effectively act within or without the traditional borders (ibid.).

2.2 Critics to the European Schools of Security studies

European Schools present different point of views about the security discourse and the referent objects. While claiming that human networks' security is the goal, the scholars take different paths in getting to security. Therefore, an inter-scholar debate arises from this dissemblance in views. The most intense exchange in views has seen the Copenhagen School respond to the Welsh School and vice versa. The Paris School did not take a stand, as it has idiosyncrasies that set it aside from the debate and take under the lens agencies and agents.

2.2.1 The Welsh School

Scholars use the arguments of security as emancipation in the context of different agendas. "schools" denote doctrines, hierarchical relations, teaching being passed on and reproduced – connotations that are antithetical to the critical spirit of permanent unease" (Shepherd, 2013b, p. 65). The identification of the Welsh School as a school of thought is thus limiting the approach security as emancipation wishes to communicate.

The approach has had little to say about dynamic sectors such as political economy or cybersecurity. It rather focused on normative statements to reconnect security studies to "real people in real places". There is also need for more detailed exploration of power and its complexities in relation to the politics of security.

The Copenhagen School, by contrast, openly criticized the approach of CSS scholars stating that they "believe even the socially constituted is often

sedimented as structure and becomes so relatively stable as practice that one must do analysis also on the basis that it continues, using one's understanding of the social construction of security not only to criticize this fact but also to understand the dynamics of security and thereby maneuver them." (Buzan et al., 1998)

Wyn Jones, in an attempt to open the doors of security of emancipation approach claims that "all proponents of CSS depend on some notion of the existence of possibilities for progressive alternatives – that is, emancipation" (in Booth, 2005, p. 217), hence taking the views by Wæver in the CSS approach, even though he is associated with the Copenhagen School. Nonetheless, Wæver (2004) argues "CSS in its broad sense shows no clear "boundary" towards the Copenhagen School. In some sense, it is artificial to have Krause, Williams and Wæver located in different "schools"".

The question remains open if the Welsh School can be considered a relevant School in the field of Security Studies or if it can be moved to a considerable contribution in the poststructuralists" formation of Security Studies. In other words, the Welsh School could be considered complementary to the approach taken by Buzan and his School. Indeed, this may seem unclear or too hazardous, but the next subsection may clear out the mind of the skeptic reader.

2.2.2 The Copenhagen School

Securitization theory has likewise undergone several critiques and revisions. The main one is that it is still under the shadow of (neo)realism, and its effort to "incorporate some of the traditionalist positions"(Buzan et al., 1998, p. 4) is problematic. Human security scholars critique the privileged position of the State

in the securitization discourse. Complementary to CSS, it is also criticized for having no clear normative agenda (Hansen, 2010; McDonald, 2008). This is problematic as it is not sure whether securitization is preferable to desecuritization, as the scholars do not elaborate the concept of desecuritization more than what has been previously said above. They deny the opportunity for analysis by stating that securitization is a political choice, leaving analysts as passive observers.

Aradau (2004) sees desecuritization as a potential democratic emancipatory transformation and argues that there is a need to rework desecuritization "through a politics of emancipation as democratic politics". However, being under-theorized it is difficult to develop on the concept.

Another limit of securitization could be its ambiguous usage of speech act. Stritzel (2007) claims that there is a tension between the Copenhagen School's desire to have both "a social sphere (with "actors", "fields", "authority", "inter-subjectivity", "audience" and "facilitating conditions") and a (post-structural/postmodern) linguistic theory based on Derrida and performativity". This can explain the evolution of securitization theory in a sociological and a post-structural branch. Furthermore, a "focus on the moment of intervention only" also ignores gradual processes of security construction (McDonald, 2008).

Perhaps the central limit remains its focus on speech and language. It ignores a wide array of expressing security, from "non-verbal expressions of security" (Wilkinson, in Balzacq, 2010, p. 94) to physical action (McDonald, 2008) and visual representation (Hansen, 2008; Williams, 2003).

For Balzacq, securitization is centered on audience and "the challenge of a securitizing agent would be to convince the audience (e.g. a nation) to recognize the nature of a symbolic referent subject" (Balzacq, 2005). The problem of securitization theory is that it lacks a thorough definition of audience, which leads analysts to find it difficult to incorporate it in their research. It is difficult for them also to measure the acceptance of securitization both methodologically and empirically. This highlights a fundamental flaw in the securitization theory. It tends to analyze only successfully securitized issues, which underlies that the audience has already accepted the securitization move. This can "understate or overstate the relationship between the dependent and the independent variable" resulting in a "confirmation bias" (Balzacq, 2010). Besides the audience, it is also important to take into account the external context as an important factor, especially timing and external reality (Balzacq, 2005, p. 182).

2.3 The realist School: an American affair

Realism is the predominant school of thought in the United States. The school has a long tradition and it has its roots in many political thinkers of the past (Thucydides, Thomas Hobbes and Niccolò Machiavelli). For Haslam (2002), realism is "a spectrum of ideas [...] rather than as a fixed point of focus with sharp definition". Definitions of realism vary considerably in their details but reveal a striking family resemblance (Reus-Smit & Snidal, 2008). Current debates concentrate over defensive and offensive realism. These branches attracted scholars as potential shapers of United States foreign security policy.

Realists, in all their diversity, tend to converge around four main assumptions that provide a working definition of the realist tradition.

1. *Anarchy.* The absence of order and global governance dramatically shapes the nature of international politics. Anarchic political systems usually exacerbate egoism and survival instinct. The invisible constraints limit the ability of international actors to achieve their purposes.

2. *Egoism.* When individuals and groups act politically, they are driven by mere self-interest. This trait is deep-rooted in human nature. Its full expression may be mitigated by national and international political structures, institutions or values.

3. *Groupism.* It is the expression of politics. Group solidarity is a driver of cooperation or conflict between polities in international politics. To survive above subsistence levels, people need cohesion, which in turn generates potential for in-group conflict or conflict with other groups. Realism applies to any setting where groups interact, not just states interaction. There is a common misconception of states being the referent object of realism. However, states are commonly taken as examples of socially organized groups.

4. *Power politics.* It is the result of the intersection of groupism with egoism. As Waltz (1979) wrote "the web of social and political life is spun out of inclinations and incentives, deterrent threats and punishments. Eliminate the latter two, and the ordering of society depends entirely on the former– a utopian thought impractical this side of Eden." Realists are skeptical toward pursuing moral objectives in international relations.

In the 1970s it appeared clear that the realist school was declining because too wide. The failure of Morgenthau's attempt to pull together classical realists was discouraging. It was in the late 1970s that Kenneth Waltz tried again, with a new revivified realist theory that was later renamed "neorealism". The theory ruled over the ocean of theories in the 1980s, but the empirical setbacks jeopardized its leadership. By the 1990s it was just one of the many realist schools. There is nothing new about the existence of multiple schools within realism (Wohlforth, 2008).

2.3.1 Kenneth N. Waltz and neorealism

Kenneth Waltz is the father of neorealism. His work can be identified with two books, "Man, the State, and War" (1959) and "Theory of International Politics" (1979). In his works he states, for instance, that systemic interdependence is low and that this has been beneficial, that states can be seen as unitary actors, that non-state actors are relatively insignificant, that nuclear weapons are beneficial, that superpower superiority was a good thing that the United States of America has behaved much like the Soviet Union in the postwar period, that the domino theory is false and much of US global activism therefore redundant, that we do not "live in a world of change", that bipolarity persists, etc. At the time, these were all provocations to the trending viewpoints of the IR community.

The author believed that theories should be preferably simple, i.e. they ought to explain reality through one or few unifying explanatory mechanisms (1975). The same view was shared by Karl Popper (1972) with different tones.

For Waltz the anarchic structure of international politics is the underlying or facilitating cause of war: it *permits* the phenomenon of war to occur, because there simply is nothing to prevent it (Waltz, 1959, pp. 232–238). Anarchy as an ordering principle entails a self-help behavior among the units (nation-states, but not necessarily); as no unit can count on others to ensure well-being and survival, it must take care of all functions by itself, in principle (Waltz, 1979). Even if the units are not functionally different, they are not equal in terms of power (ibid.). However, *balancing* is a universal behavioral trait during anarchy. Balancing means building capacity or alliances to balance off the most powerful states. The nature of this behavior is pushed by different reasons varying with the number of poles in the system. In terms of peace, it is argued that few poles guarantee higher stability than many, and bipolarity is better than the presence of few poles. This is so because of the lower probability to miscalculate the rational behavior of other poles. On the other hand, Waltz argues that hierarchy leads to bandwagoning behavior, the typical behavior observable in domestic political systems.

2.3.2 Offensive and Defensive Realism

Introducing Kenneth Waltz's theory simplifies the introduction of offensive and defensive realism. The advent of neorealism forced scholars to think critically about the underlying forces that drive international politics. Soon scholars realized that Waltz's assumptions led to very different predictions/outcomes depending on the reasonable expectations they had around real-world conditions. This is so because Waltz neglected important mutable factors such as geography and technology. Out of the inclusion of these factors in the theory,

since the different conceptualization they could have, two new theoretical sub-schools were formed each of which built on the basic insights of neorealism.

Defensive and offensive realism emerged as distinct sub-schools emerged in the 1990s. Both representatives of the schools thought to be articulating *the* realist theory *par excellence* in line with the tradition of Waltz and Morgenthau. For example, in *The Tragedy of Great Power Politics,* Mearsheimer portrayed offensive realism as the only successor of Waltz's neorealism, which he equated to defensive realism. These two sub-schools do not exhaust realism's diversity, but are the two most representative and most current (Wæver, 2004). Often, the sub-schools are therefore tools of convenient criticism in the intra-theoretical dispute (Rynning & Guzzini, 2001).

Defensive realists claimed that under reasonable conditions the potential threat of war is attenuated (Taliaferro, 2001). Defensive stands for "the overriding goal of survival" that causes states to balance "strategies in order to prevent the rise of dominating powers" (Rynning & Guzzini, 2001). Proceeding from groupism, the core realist assumption, Van Evera (1999) argued that the stronger the group identity is the harder it is to conquer and subjugate other groups. In turn, this makes states more secure. A similar reasoning can be applied to technology as dissuader of threats of war. The nuclear capacity made a conventional war between Russia and the United States of America unlikely. Therefore, even under Waltz's assumptions over the insecurity of states in an anarchic environment, under the condition posed by defensive realists states could still find defensive tools without directly threatening others, or could signal their peaceful intentions, with more potential for peace than many realists argued before (Glaser, 1997).

The result was analysts carrying domestic explorations for the root causes of war and peace.

Offensive realists were more interested in the conflict-generating features of anarchy. They are different from defensive realists because they claim defensive realism operates in a "world of all cops and no robbers" (Schweller, 1994, 1996), thus failing to explain conflict. They reasoned that, with no authority to enforce agreements, states could never be confident that any peace-causing measure would be stable in the future. Even if conquest is not a viable option today because of geography or technology, that does not guarantee peace. Another State could develop a lethal technology to overcome those barriers in the future. Given this uncertainty, security is not achievable and states ought to actively respond to other states" increases of power. Because of suspicion, states will be caught in a spiral of strengthening (or weakening opponents) and expansion to survive over the long term. These assumptions reinforce the realist belief in the competitive nature of life under anarchy, regardless the domestic values of states.

2.4 The missing piece in Security Studies theories

The broad overview on the prevailing security theories in the international scene offers the advantage to highlight the driving factors towards security. Until recently, there has been little explicit discussion within Security Studies on the cyberspace and what "cyber security" implies.

Kuehl (2009) claims that "The existence of cyberspace as a new global domain presents fresh opportunities for its employment and vulnerabilities to be

defended against [...] and the strategist will be challenged to integrate its capabilities with other elements and instruments of power". Cyber security is there to address the concerns about vulnerabilities and a theory of cyber security would help strategists and analysts to address those challenges.

The term "cyber security" first appeared in the 1991 report by the Computer Science and Telecommunications Board (CSTB). The Board outlined security as the "protection against unwanted disclosure, modification, or destruction of data in a system and also [to] the safeguarding of systems themselves" (Computer Science and Telecommunications Board, 1991; Hansen & Nissenbaum, 2009). It did not have a political connotation and was relevant only in computer and information science. Nevertheless, the term became a buzzword in technical discourses since then. Academics focused on programs to reduce attack risks and mitigate viruses damage rather than moving the issue at the systemic level to securitize it. The move from "computer security" to "cyber security" has involved the combination of technical discourse and national strategies on cyber security that have emerged since 2000s, hence undergoing the process of securitization (Nissenbaum, 2005). Some have proposed to expand the Copenhagen School's securitization theory to this new sector (Hansen & Nissenbaum, 2009).

Most of the theories in Security Studies discussed above were criticized for the adoption of a narrow referent object, mainly the State. This critique is a valuable input also for cyber security. Adopting one referent object would imply the denial of the intensely, densely interconnected nature of the cyberspace where data flow regardless of national boundaries (Franklin, 2013). While this is true, Dunn Cavelty (2012) maintains however that two factors contribute to the militarization

of the cyberspace: the main focus on highly vulnerable critical infrastructures as "referent object" and the threat representation based on the inherent insecurity of the information infrastructure and the way it could be manipulated by technologically skillful individuals. The competing claims derive from an unclear definition of the object of study, i.e. cyber security.

2.4.1 An aside on the term Cyber Security. Defining the scope for analysts.

Before proceeding further in the discussion, a definition is desirable to clarify the object of a cyber security theory in Security Studies. C**yber safety** and **cyber security**, which will be defined below, are the terms used to frame the goal of policy discourses in Security Studies. This, in accordance with Hansen & Nissenbaum (2009) that there is a distinction between individuals and collectivities when analyzing security, especially in the cyberspace. Mayer, de Scalzi, Martino, & Chiarugi (2013) claim that "Without a shared definition of terms such as cyberspace, cyber power, cybersecurity, etc. it is difficult to dig beneath the surface, to grasp the deeper logic that governs the operation of cyberspace, and to explain the growing importance that cyberspace is acquiring in contemporary politics."

Cyber safety is a concept resulting from technical computer security. It is the protection of individuals or firms from direct threats to the data stored on their devices or networks via private solutions. Anderson (2003) maintained that computer security is driven more by the costumer's will than protection against objective threats. This field is then a market-driven process mostly influenced by speech acts and marketing. This acquires political importance when seen in the

context of collective referent objects like " "the state", "society", "the nation", "economy" " (Hansen & Nissenbaum, 2009).

Cyber safety is also referred to in fields like pedagogy with a different connotation. It is used to educate students to avoid cyber violence and surf the Web responsibly, i.e. avoiding cyberbullying, pornography, sexting, and other behaviors reputed against morality (for a comprehensive overview, see Third, Forrest-Lawrence, & Collier, 2014).

Hansen & Nissenbaum (2009) proposed that cyber security is a distinct sector of security "with a particular constellation of threats and referent objects". Drawing from Nissenbaum's (2005) definition, **cyber security** can be defined as the preservation of systems operating the cyberspace, be they hardware (critical infrastructures, machines, facilities, ...) or software (systems, applications, data, ...), carried out by the State in pursuit of national interests, or the protection of its citizens (Banerjee et al., 2012). The State is enabled to guarantee cyber security through co-responsibility with the private sector (Hansen & Nissenbaum, 2009, p. 1162). In a sense, we could see the State as the gate-keeper of the national cyberspace. Hence, the State is the ultimate responsible for the defense of national interests and the protection of its citizens from external and internal threats (Krasner, 1978; Morgenthau, 1951). This principle was first invoked by the Italian thinker Niccolò Machiavelli (1532) in the book "Il Principe" (The Prince).

Scholars have also used concepts like "cyber war" (Der Derian, 1992), "netwar" and "network security" (Arquilla & Ronfeldt, 1999, 2001; Deibert & Stein, 2002; Der Derian, 2003), "critical infrastructure protection" (Bendrath, 2003). Though

semantically similar, they have precise meanings that differ from cyber security and may confuse a reader who is not familiar with the subject. Furthermore, they belong to different classes. The lexicon used for cyber security refers to terms such as “protection”, “preservation”, “defense”, thus suggesting at primarily defensive practice. Hence, we need to distinguish it from cyberwarfare, which are "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2011), but other definitions include also non-state actors (Arquilla, 1999). Again, the lexicon used in cyberwarfare discourse refers to “attack”, “aggression”, “penetration” that are proper of an offensive practice.

For the remainder of this document, cyber security will be the focus of the discussion. It is more prone to tackle the nation-system security issues and help to minimize cases of cyber (un)safety, through innovative approaches (discussed in chapters 4 and 5).

2.4.2 Actors’ stance

The actors in cyberspace can adopt three types of stance: aggressive, neutral or defensive. **Aggressive stance** is adopted to steal information, do damage, tamper data transfers, take over the control of a system. This stance is typical of acts of cyber warfare (Clarke & Knake, 2011). **Neutral stance** is the use of cyber technologies as a source to augmenting the relationships' intensity that they would have in real life. The neutral stance needs to be addressed through the promotion of responsible behaviors that minimize the exposure to cyber threats and to achieve cyber safety. The **defensive stance** is adopted in response to attacks initiated by third parties or by means of proactive monitoring of the

system/network. To pursue cyber security, the State adopts the defensive stance. Differently from the definitive claims of defensive and offensive realists, stances in cyberspace are never statically defined and actors can adopt them dynamically depending on the cyberspace conditions.

2.4.3 Defining "liquid" boundaries: the cyberspace

The Copenhagen School has been criticized for the gap in the provision an analysis of the external context (Balzacq, 2005) in securitization. There is, then, the need to provide a simple, yet effective framework to facilitate analysts in the schematization of the environment in which actors operate.

The **cyberspace** is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (Kuehl, 2009). It is characterized by the **multi-level interaction** of actors which own nodes of the network or parts of it through legal means. Or, they can get a hold of them maliciously (see, for example, Angrishi, 2017; Farwell & Rohozinski, 2011). "The economic and social systems of advanced countries are strongly dependent on cyberspace" (AA.VV., 2016). The interaction is multi-level since there are hardly boundaries (Hundley & Anderson, 1995) for the flow of data and actors exchange them in any direction. There is also the need to study the impact of autonomous systems like artificial intelligence (AI) in this interaction.

Besides, there is no central authority regulating limits of exchange. The absence of global governance resembles the realist assumption of **anarchy**. The unfortunate point is that cyber power (Kuehl, 2009) cannot be measured as the development of technologies is registering an impressive growth and network vulnerabilities are discovered every day during this decade. A viable option, as proposed by Hansen & Nissenbaum (2009), is interdisciplinary work.

The **national cyberspace** is a subset of the cyberspace, but its definition encompasses the actors operating within national borders and it is useful for the scope of cyber security. Actors are the central element of cyber security as they operate and influence each other. Those who are comprised within the national cyberspace are: the State, through its Agencies and territorial articulations; firms based within the internationally recognized national borders, not including firms owned by a majority share of foreign investors; private citizens. These actors can aggregate within or across each category.

The achievement of cyber security for national cyberspace actors in the international cyberspace is an important matter. Therefore, there is the need to evaluate legislative steps to be taken to facilitate the sharing of information about vulnerabilities and during emergencies. This task is delegated to chapter 3.

3 Assessment of legal frameworks

Recently the European Union (EU) has taken position to counter cybercrime and bolster cyber security through diverse lines of action. It has adopted and formulated the following tools and strategy: the Network and Information Security (NIS) Directive, the General Data Protection Regulation (GDPR), and the EU Digital Single Market strategy (DSM). Additionally, considering the importance of private sector in the cyber security "arms race" (resulting from the market-driven process of network and information systems private security), the EU launched a public-private partnership on cyber security as announced in the DSM in 2015 (European Commission, 2015). To comply with the EU strategy, all the Member States are required to adopt measures to ensure the harmonization of cyber security practice.

3.1 CYBER SECURITY IN EUROPE: TIMELINE

In 2001, the European Commission had highlighted the importance of NIS in its report "Network and Information Security: Proposal for A European Policy Approach".

In 2004, the European Network and Information Security Agency (ENISA) was established with the objective to promote "a culture of network and information security for the benefit of citizens, consumers, business and public sector organizations in the European Union" (Regulation (EC) No 460/2004 of the European Parliament and of the Council, 2004). ENISA was tasked with assisting Member States in their development of industry-specific cyber security

strategies, enabling cooperation and information sharing between public and private sector entities, and tracking information security risks.

In 2006, the European Commission adopted a “Strategy for a Secure Information Society” with the goal of developing a culture of NIS in Europe. Its main elements, including the security and resilience of IT infrastructures, were recognized in the Council Resolution 2007/068/01.

In line with the 2006 strategy, the European Commission adopted in 2009 a Communication entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", which focused on the protection from cyber disruptions by enhancing security and resilience.

In 2012, the European Commission held an online public consultation on “Improving NIS in the EU”. The results showed a wide support for improving NIS in the EU. The results of the consultation, publicly available, helped informing the proposal for the 2013 “Proposal for a Network and Information Security Directive”.

In 2013, the European Commission published the “Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace”. The Strategy established a common approach for preventing and responding to cyber disruptions and attacks within the Union. It encourages Member States to organize and respond to cyber threats at the national level. It also grants ENISA the power to liaise with the public and private sectors to enhance the adoption of NIS standards and to support the drafting of guidelines that mirror best practices.

The European Parliament and the European Council proposed, in coincidence with the release of the Strategy, a "Network and Information Security Directive" to "ensure a high common level of network and information security standards among member states". The Directive proposal aimed at raising awareness on the need to improve the security of the Internet and private networks and information systems on which the digital society relies.

On 17 May 2016, the European Council formally adopted the NIS Directive. Upon the publication of the adopted text in the Official Journal of European Union and its entry into force, on 19 July 2016, member states have 21 months to transpose it into national legislation.

3.2 The NIS Directive

As mentioned, the NIS Directive is the first EU legislation on cyber security. Its core objectives are to reach minimum harmonization and to make the cyberspace more secure, which will ultimately support the creation of the DSM. The opening sentence is particularly significant:" Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market".

It defines the security of network and information systems as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (Article 4.2).

The declared objectives of the Directive are:

(1) Improved cyber security capabilities at national level;

(2) Increased EU-level cooperation;

(3) Risk management and incident reporting obligations for operators of essential services and digital service provider.

As for (1), each Member State is obliged to adopt a national strategy on the security of network and information systems (Article 1.2a). Article 1.2b establishes the creation of a "Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them". (3) is there to promote a culture of risk management and ensures the most serious incidents are reported and analyzed to assess possible common threats. It further helps to keep the private sector co-responsible for the safety and security of the cyberspace.

The Directive is divided into seven chapters that address the themes discussed above and provide much needed clear definitions to be shared among Member States in order to facilitate cooperation and coordination.

Moreover, it establishes a timeline for the implementation and entry into full force. The table below illustrates the main dates and milestones.

Date	Milestone
9 August 2016	Entry into force
9 February 2017	Work beginning for the Cooperation Group
9 August 2017	Security and notification requirements adopted by Digital Service Providers
9 February 2018	Cooperation Group work programme established
9 May 2018	Mandatory transposition into national laws
9 November 2018	Identification of operators of essential services by Member States
9 May 2019	Commission report
9 May 2021	Commission review of the functioning of the Directive

3.2.1 Building cyber security capabilities at national level

The NIS Directive requires Member States to adopt a **national strategy on cyber security** with a view to achieving and maintaining a high level of security of network and information systems across "essential services". As part of this strategy, Member States should:

- define objectives and priorities of the national strategy;
- create a governance framework to achieve them;
- Identify measures relating to preparedness, response and recovery;
- Indication on education, awareness-raising and training programs relating the national strategy;
- Indication on research and development plans relating the strategy;
- Provide a risk assessment plan;
- Create a list of the various actors involved in the implementation of the strategy.

Member States, in accordance to Article 7.3 have the obligation to communicate the adoption of a national strategy within three months from its adoption to the European Commission. Furthermore, the Member States have the faculty of requesting support from ENISA in developing national strategies.

Article 8 demands the designation of one or more **competent authorities** to monitor NIS implementation at the national level. The article clarifies that although multiple competent authorities can be designated to monitor different sectors, Member States have to establish a **single point of contact** to report to the Cooperation Group and to ensure cross-border cooperation with other Member States.

The Directive requires a third body, namely the Computer Security Incident Response Teams (**CSIRTs**). These teams are responsible for monitoring incidents, providing early threat warnings, responding to incidents, and cooperating with the private sector. Member States have to ensure (Article 9.3) that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level. The NIS Directive further launches a network of CSIRTS in which each Member State must participate.

Article 10.3 establishes that single point of contacts by 9 August 2018 and every year thereafter shall submit a summary report to the Cooperation Group on the work performed.

3.2.2 EU-level cooperation

The NIS Directive establishes a **Cooperation Group** "to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union". It is composed of representatives of the Member States, the European Commission and ENISA (Article 11.2).

The Cooperation Group will work based on biennial work programs, which will entry into force by 9 February 2018. It will lead the **planning**, the **steering**, the **reporting** and the **exchange of information** on best practices among Member States.

Article 12.1 establishes a **network of the national CSIRTs** to "promote swift and effective operational cooperation" in which Member States must participate. This network's duties include exchanging information about security incidents and identifying, where possible, a coordinated response, providing member States with support in addressing cross-border incidents, and exploring and identifying further forms of operational cooperation.

3.2.3 Operators of essential services and digital services providers

Article 5.2 of the Directive provides the criteria for the identification of an **operator of essential services:**

- an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

- the provision of that service depends on network and information systems; and

- an incident would have significant disruptive effects on the provision of that service.

They are identified in Annex II of the Directive within the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors. Member States must identify within 27 months from the entry into force of the Directive their national operators of essential services. Moreover, they have to monitor, having regard to the state of the art, that security measures taken by these operators are technically and organizationally proportionate to ensure level of security of NIS appropriate to the risk posed (Article 14.1).

The operators have the obligation to notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential service they provide (Article 14.3). The impact can be measured through the number of users affected, the duration of the incident and the geographical spread of the incident (Article 14.4). However, no thresholds are defined in the Directive. The competent authority or the CSIRT can, having regard to the confidential details of the incidents, inform the public where public awareness is necessary to prevent an incident or to deal with an ongoing incident (Article 14.6).

Important for the establishment of a trustworthy environment are what the Directive defines as **digital service providers,** legal persons providing a digital

service (Article 4.6). Annex III of the NIS Directive recognizes online marketplaces, cloud computing services and search engines as digital service providers.

Similarly to the operators of essential services, digital service providers will be required to take appropriate security measures and to notify substantial incidents to the competent authority. The providers should take into account some specific factors when designing and implementing security measures, such as: the security of system and facilities; incident handling; business continuity management; the monitoring, auditing and testing of measures; the compliance with international standards.

The Directive identifies two additional parameters for the reporting of incidents to competent authorities, namely the extent of disruption of the service and the impact on economic and societal activities.

To achieve a harmonized approach and allow no distortion in the economic activities of the digital service providers, the Commission will adopt implementing acts by August 2017 and Member States will not be able to impose stricter security and notification requirements.

3.2.4 Critical evaluation

The NIS Directive represents a milestone in the EU cyber security discourse, changing the Union regulatory scenario and affecting industries (even global firms). However, it remains unclear whether the Directive will be a game-changer or the cyber strategy will need major changes to have a proper impact in the Union.

Critics of the Directive believe there is much room for improvement. The "minimum" harmonization scheme allows Member States to adopt or maintain laws that may impose requirements on operators in their jurisdiction that are stricter than those set forth in the Directive (Weber & Studer, 2016). Nonetheless, this can lead to legal fragmentation given the varying degree of cyber security maturity among the Member states. Which is precisely what the Directive seeks to overcome (ibid.). The tracking of the impact of the NIS Directive will become very difficult and the social loss of this fragmentation should be carefully evaluated and monitored. Firms operating in multiple jurisdictions would potentially have higher compliance costs with the regulation in place than might otherwise be the case.

Second, the notification requirement under the NIS Directive has potential overlaps with other existing breach reporting requirements under other EU legislation, which increases fragmentation. Furthermore, firms have few incentives to unilaterally report breaches. The risk for them is a potential reputational damage deriving from the disclosure of cyberattacks details. To dissuade those to whom the Directive applies from concealing cyber security breaches, the introduction of penalties has been thought to be the solution (see Article 21 of the NIS Directive). However, Laube & Böhme (2016) using a principal-agent model show that even under optimistic assumptions regarding the effectiveness of mandatory security breach reporting to authorities in reducing individual losses, it may be difficult to adjust the sanction level such that breach notification laws generate social benefit. The dilemma will hardly have an

answer until an environment of trust is created between firms and competent authority.

Concerns have been also raised with respect to the exclusion of small and medium enterprises from the scope of the Directive. This is challenging if one considers that small and medium enterprises form the largest percentage of companies that use the NIS infrastructure (Weber & Studer, 2016). The exemption of hardware manufacturers and software developers is as well problematic. The recent WikiLeaks' "Vault 7" disclosure highlighted the critical role of hardware and software producers in cyber security, thus making them weakest link in the security chain and easy targets for attackers. This calls for a prompt action by the Member States through national cyber security legislation.

3.3 The Italian cyber security strategy and the cyber security framework

In 2016, the report released by the Italian National Security Lab with the collaboration of the Center for Cyber Intelligence and Information Security (CIIS) at La Sapienza University, highlighted the need for a national cyber security framework. The new cyber security program, has been presented by the Italian Prime Minister Paolo Gentiloni Silveri together with the Director General of the *Dipartimento Informazioni per la Sicurezza* (Security Intelligence Department, DIS), Prefetto Alessandro Pansa in February 2017 upon approval. The new framework complies with the NIS Directive requirements and abolishes the Decreto Monti in 2013, a decree issued by the Italian Prime Minister at the time, Senator Mario Monti.

Before analyzing the new Decree, published on April 13 2017, it is worth discussing the National framework proposed by the abovementioned research centers.

3.3.1 The national cyber security framework

The framework aims at providing a homogeneous and volunteer approach to face up cyber security in order to reduce risks linked to cyber threats. It derives from the NIST Framework the basic concepts of Framework Core, Profile and Implementation Tier, adding Priority and Maturity levels to the subcategories of the core. The priority and maturity levels help address a more rigorous contextualization than the NIST's business profile, sector vulnerabilities, organization size and other company or sector characteristics. This homogenization has been chosen to guarantee harmonization and an easy interpretation by international actors. The document gives also use cases and helps define relationships with the newborn insurance market for cyber risk management. The authors make a statement on the dynamic nature of threats and the commitment to keep the framework updated according to feedbacks and lessons learned over time. They also advise about the beneficial systemic effect the adoption by all the organizations this framework would have for the country.

The Italian business environment is mostly composed of small and medium enterprises (SMEs), most of which has never thought to invest in IT security. This is generally true for two reasons: the first one is a lack of IT culture for a large part of Italians; the second one Is a lack of cyber risk assessment.

The biggest issue, especially for small enterprises, is represented by costs. They are not able to identify simple practices to protect from cyber attacks. The wrong estimate of costs represents the main reason for entrepreneurs not to invest in cyber security practices. In fact, the CIIS presented in its Cyber Security 2016 Report fifteen simple controls for small enterprises which bring the level of protection and awareness against common cyber threats to a basic security value, sufficient for most of the firms. They had been already included in the 2015 Report, but they were not transposed by enterprises resulting in a disastrous 45.2% of firms being successfully attacked between September 2015 and September 2016 (Biancotti, 2017). The Framework could also be used by sector regulators as a tool to define standards or to issue regulations in a structured and compatible way for the Italian system. It avoids additional burdens and promotes dialogue between regulator and regulated entities.

The Framework core is hierarchically structured into **Function, Category**, and **Subcategory**. Functions are concurrent and continuous and they are: Identify, Protect, Detect, Respond, Recover. The 5 Functions are described as:

- ***Identify***. Understanding of the company context, assets and relevant associated risks.
- ***Protect***. Implementation of measures to protect the business processes and company assets, regardless of IT.
- ***Detect***. Definition and implementation of appropriate activities aimed at identifying IT security accidents on time.
- ***Respond***. Definition and implementation of appropriate activities to act in case of cyber security events.

- *Recover*. Definition and implementation of activities aimed at the management of plans and activities to restore processes and services after a cyber security event.

The Functions are vital to a proper cyber risk management. The core provides for each Function categories and subcategories, specifying processes and technologies to be put in place to manage the single Function. However virtuous, this practice can trick the less technologically inclined entrepreneurs into applying thoroughly the prescriptions, not triggering a proactive mindset proper to approach the problem.

Particularly important are the **Profiles** introduced in the Italian Framework. They represent the specific choices of Subcategories made by companies for each Function. They are also useful to make comparisons between the status quo (**current profile**) and the desired state (**target profile**). It functions as a guideline to support in the definition of priorities and for the measurement of the advancements towards the target profile. Lastly, profiles can be used to demand minimum requirements to strengthen the supply chain.

In this context, **maturity level** can help creating concrete steps towards achieving the target profile. The levels are defined by the company and the document advises on how to define them.

Moving to the **implementation tiers**, they assess the degree of attention the company and its management put into the assessment of cyber risks. The four tiers in growing order are: **partial, informed, repeatable, adaptive**.

The Framework is highly suggested for SMEs, but there are also indications for Critical Infrastructures, Sector regulators and Large Enterprises. For example, critical infrastructures may implement the Framework to support processes and activities of cyber intelligence to be carried out privately or in collaboration with authorities, depending on the methods for the sector of business.

3.3.2 The new Italian Decree for cyber security strategy

On 17 February 2017, the *Comitato Interministeriale per la Sicurezza della Repubblica* (CISR, Interministerial Committee for the Security of the Italian Republic) approved a Directive named "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*", dubbed Gentiloni Decree on cyber security. As said, the new Decree substitutes the Monti Decree of 24 January 2013.

The Decree was issued for the need to update the Italian legislation in transposal of the NIS Directive before 9 May 2018. The aim of the Decree is to unify the system of expertise involved in the management of crises, related to the prejudice of national security and its fundamental democratic Institutions. It was also needed for the rationalization and simplification of the institutional architecture in order to prevent, prepare and manage crisis situations of cybernetic nature from units that have a direct and effective link with the CISR.

The document is composed of 13 articles defining actors, functions and actions for the cybernetic protection of critical infrastructures (material and immaterial).

It is worth noting that Article 2 of the Decree contains definitions about cyberspace (2.1.h), cyber security (2.1.i), cyber threat (2.1.l), cyber event (2.1.m), cyber crisis (2.1.o).

Cyberspace is defined as the set of interconnected informatic infrastructures, comprising hardware, software, data and users, as well as the logic relationships, anyhow established, among them.

Cyber security is the condition for which the cyberspace is secured through the adoption of measures of material, logic and procedural security with respect to events, of voluntary or accidental nature, consisting in the acquisition and illegal transfer of data, in their modification or illegal destruction, or in the illegal control, damage or block of the regular functioning of networks and informative systems or of their constituting elements.

A **cyber threat** is the set of conducts that can be realized in the cyberspace or taking advantage of it, or by damaging it and its constituting elements, substantiating in actions by state or non-state, individuals or organizations, public or private finalized to destabilize the cyber security.

A **cybernetic event** is a significant occurrence of voluntary or accidental nature, consisting in a cyber threat.

A **cyber crisis** is a situation in which a cyber event has a large dimension and intensity, or it affects national security, or it cannot be managed by single competent administrations with ordinary means, but with a coordinated decision-making of the CISR.

During a cyber crisis, the chief decision-maker is the Prime Minister (*Presidente del Consiglio dei Ministri*), who calls for an emergency CISR meeting and gives directives to the DIS and the Agencies (Article 3.1.a and 3.1.e). The Prime minister has the role of transposing the strategic framework for cyber security and the National Plan for cyber security and safety, by issuing the directives and acts to address the necessary actions to reach the objectives of the National Plan (Article 3.1.c and 3.1.d).

The CISR, as anticipated, takes on a consultative and propositive role in case of cyber crises (Article 4.1.a). It proposes the adoption of the strategic framework for cyber security to the Prime Minister and deliberates on the National Plan (Article 4.1.b and 4.1.c). Furthermore, the CISR has the task of approving the guidelines to foster the effective collaboration between Institutions and private operators interested in cyber security, as well as the sharing of information to adopt best practices and measures that aim to achieve cyber security (Article 4.1.g). Article 4.1.l confers the power to CISR of formulating law proposals for the empowerment of preventative and responsive measures to cyber threats and crisis management. The work of the CISR is supported by a technical body that has the tasks laid down in Article 5.

Article 6 is about lines of action for cyber security. It covers the role of the DIS General Director, that is to take the needed action to guarantee an adequate level of protection and prevention (Article 6.1). The General Director has the right to organize, manage and outsource to public or private research centers tasks for the achievement of the lines of action for cyber security (Article 6.2). The General

Director can, only for the purposes of Article 6, partner with public or private actors in accordance to the laws in force.

Intelligence agencies have a strong role in participating to reach and maintain the desired cyber security level, to which article 7 is dedicated. The General Director of the DIS has the apical role of coordinating them in the "informative research" to guarantee cyber safety and national computer information security.

An innovation is introduced in Article 8, where the role of the *Nucleo per la sicurezza cibernetica* (Cyber Security Unit) is discussed. The Unit is the core support to the Prime Minister and the CISR and it is constituted under the authority of the DIS. It is directed by one of the Vice General Directors of the DIS, appointed by the Director General of the DIS. It is composed by the Military Counsellor to the Prime Minister and one representative per each of the following institutions: AISI (Internal Intelligence and Security Agency), AISE (External Intelligence and Security Agency), Ministry of Foreign Affairs, Ministry of Interiors, Ministry of Justice, Ministry for Economic Development, Ministry for Economy and Finance, Department for Civil Protection, and Agency for Digital Italy. The Unit is integrated with a representative for the Central Office for Secrecy. The Unit has a mandatory monthly meeting, called by the responsible for the Unit. The Unit reports directly to the General Director of the DIS, who is in charge to inform the Prime Minister and the CISR.

The *Nucleo per la sicurezza cibernetica* has several tasks to fulfill, laid down in Article 9 of the Gentiloni Decree. Its first and foremost function is to harmonize the actions of the different components of the institutional architecture. The Unit

promotes the planning of the response to cyber crises for public entities and private operators and the elaboration of the necessary interministerial coordination procedures, in accordance to the planning of civil defense and protection. It also has a 24/7 group for the alarm and response to cyber crisis. It functions as collection point for cases of cyber violations or attempts of violation to security or integrity loss for several Institutions.

The Cyber Security Unit promotes, together with the Agency for digital Italy and the Ministry for Economic development, interministerial drills to test the response capacity of the National System and to take part in international drills regarding cyber crises.

Most importantly, the *Nucleo per la sicurezza cibernetica* is the reference point for International Organizations such as the UN, NATO EU and other States. Obviously, the Unit cannot substitute itself to the competent Ministries, but it can function as support unit to them in cyber security matters.

Article 10 gives directives about the management of cyber crises. During a cyber crisis, the Cyber Security Unit activates the alert procedures and, in accordance to Article 10.2, representatives from the Ministry of Health, Ministry of Infrastructures and Transports, Fire Department, Public Aid Department and Civil Defense join the Unit depending on the needs and the implications of the ongoing cyber crisis. Private operators may be asked to join the Unit if the cyber crisis demands the intervention or coordination with some of them. It is as well the role of the Unit to coordinate the response of and gather information from local CERTs.

Private operators are listed in Article 11, which states the importance of public communication network providers, public electronic communication services providers, operators of essential services and digital services providers; especially those who manage relevant critical infrastructures at the national and European level. The duties to which these operators are subject are the ones also listed in the NIS.

Article 11.2 provides a *fulcrum* for the testing and evaluation of vulnerabilities of products. It establishes the Ministry of Economic Development as the responsible for the creation of an assessment center for products related to networks, services and infrastructures of national interest and relevance.

Articles 12 and 13 relate to the exchange of information and transitory dispositions.

3.3.3 Critical evaluation

The Gentiloni Decree is an innovation of the cyber security institutional architecture put in place by the Monti Decree of 2013.

The decree makes clear the position of the Italian Government about the strategic and delicate role of cyber security in defense of the national interests, allocating the national Cyber Security Unit within the Intelligence System.

The cooperation among Ministries is reassured through the participation of the CISR in the decision-making process even during cyber crises. The Decree further underlines the need for strengthening the cooperation among public and private operators. The coordinated action and response to cyber threats

strengthens the national system, making room for virtuous mechanisms, where public and private operators can be proactive in advancing proposals to elevate the security level. Research centers play also a pivotal role in strengthening the system and providing, through their academic work, evidence and new elements for the increase of protection.

The institutional architecture is heavily redesigned to facilitate the defense of critical infrastructures and citizens. The operative core of the architecture, as seen, is the Cyber Security Unit staffed at DIS. It is a true innovation, in accordance to the NIS Directive, to harmonize the system and have a coordination center. The flow of information is simplified, as well as the chain of command, which ensure a prompt response to cyber events.

The lack of involvement of the citizen and few awareness raising initiatives are still an evident gap in the cyber security strategy of Italy.

4 Revolution. The blockchain technology

In 2008, in a cryptography mailing list an individual (or group) nicknamed Satoshi Nakamoto, whose identity remains unknown, posted a document with the first specifics of the famous *cryptocurrency*[1] Bitcoin. In 2010, this person left the project and disappeared without ever intervening in the development of the currency. Since then, Bitcoin has grown exponentially going from an initial market capitalization of $ 287,933 in August 2010, to more than $25.5B today (May 2017). The nine pages manifesto (Nakamoto, 2008) of the cryptocurrency revolutionized the way money are exchanged around the world and it soon became a phenomenon studied in many respects.

Blockchain is the underlying mechanism for exchanges and it is perhaps the most important piece of information described in the document. It is a sophisticated, distributed online ledger that has the potential, according to Goldman Sachs, to "change 'everything'".

Most of the times the term blockchain is used to mean different concepts and products. People use it to name the Bitcoin blockchain, to talk about one of the more than 500 cryptocurrencies used around the globe, or to talk about smart contracts. However, the blockchain is not just a vector for digital transactions. Its full potential is still being investigated and it has already attracted billions in

[1] A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptocurrencies are a subset of alternative currencies, or specifically of digital currencies.

funding. It is revolutionizing not only the way many industries work, but most of all their mindset. Even the U.S. Defence Advanced Research Projects Agency (DARPA) is investigating blockchain technology to “create an un-hackable messaging system.”

The complexity of this technology and its innovative approach is particularly appealing, but it also creates some concerns as it disrupts many of the pre-blockchain era clichés.

The only unquestionable point about the cyberspace is that every system has a flaw and it is a matter of time and resources to find it. Assuming that this will hold true in the next decades, securing critical infrastructures and knowing how to slow down attackers (or to speed up attacks, depending on the point of view) is vital to facilitate the identification of and response to threats. Blockchain is going to help solving this issue and enable effective defense in data-fighting in the near future.

This chapter is devoted to a non-technical introduction to blockchain. It is divided as follows: the first section provides a definition of the blockchain; in the second section, the history of this technology is presented; the third section discusses the features of the blockchain; the fourth section considers the theory proposed in chapter 2.4 and describes the implication for the architecture of cyber security would the blockchain’s philosophy be adopted; section five discusses strengths and weaknesses of the technology.

4.1 DEFINITION AND CONCEPTUALIZATION

A blockchain is a shared, distributed, tamper-resistant database that every participant on a network can share, but that no single entity can control (Barnas, 2016). In his paper, Nakamoto (2008) describes the solution to the problem of a malicious user who would spend twice its Bitcoin cash (the problem of double spending) as a distributed database of time-stamped, consensus-based, cryptographically tagged transactions that form a record that cannot be changed – a blockchain.

In other words, a blockchain is a database that stores digital records. The group of network participants, all of whom can submit new records for inclusion, share the database. However, those records are only added to the database via the agreement, or consensus, of a majority of the group based on proof of work (Back et al., 2014). In basic terms, "blockchains record and secure digital information in such a way that it becomes the group's agreed-upon record of the past" (Barnas, 2016).

This technology ushered in a new era that extends beyond global payments, to social institutions, democratic participation, corporate governance and capital markets (Wright & De Filippi, 2015). Although less than ten years old, this technology is rapidly evolving and, in the past two years, new applications and features have been added. In fact, the new features allowed experts to begin talking about *blockchain 2.0*. The possible sectors of application of this technology will be discussed in chapter 5.

4.2 THE (BRIEF) HISTORY OF A PROMISING TECHNOLOGY

Peer-to-peer technologies were the precursors of Bitcoin. Napster, Gnutella, BitTorrent and others allowed users to access information by connecting with strangers on the Internet, thus enabling the exchange of data (Baron, Mahony, Manheim, & Dion-schwarz, 2015). These services dramatically changed the way data were accessible on the Internet and had a significant impact on some industries (e.g. the music industry). However, the security of these services was minimal and theft of data often occurred with attacks through these vectors. Some defined it as the "cyber availability without decentralization" phase of the cyberspace (Baron et al., 2015).

The Tor project[2] has been the first move towards decentralization in cyberspace. Typically, users of the Tor network are highly concerned with privacy and use it to conceal their identity through shared nodes that can be accessed sequentially in cyberspace. Indeed, the user appears to have the same identity of the last node he/she accessed through Tor services. These services are often called the Dark Web, as search engines fail to index them in their search results. The Dark Web represented the *middle age of decentralization*, where Bitcoin established itself as the means for gray economy transactions.

Then, in 2008, Satoshi Nakamoto posted on a cryptography mailing group about a project he had been working on for a few years before, looking for advice and help in implementing the technology.

[2] "The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet." Retrieved from https://www.torproject.org/about/overview.html.en

The message was quite simple:

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at: http://www.bitcoin.org/bitcoin.pdf

The main properties:

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style proof-of-work.

The proof-of-work for new coin generation also powers the network to prevent double-spending.

[...]

Satoshi Nakamoto

----------"

Before Nakamoto's Bitcoin, the blockchain was first described in the work by Haber & Stornetta (1991) followed by the 1996 publications of Ross J. Anderson and the 1998 publications of Schneider and Kelsey. Wei Dai, then, wrote the post "b-money" on his website (1998) preceded by a patent for a cryptographic exchange system (1997) and Nick Szabo worked in parallel on a decentralised digital currency named *bit gold*. Stefan Konst, in the year 2000, published a paper entitled "Secure log files based on cryptographically concatenated entries" (translated from German, original name *Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge*) and suggested a set of solutions for application.

No clear paternity can be attributed for the birth of this technology, however Nakamoto proved that the collaborative spirit of the cyberspace could boost the development of innovative technologies and led to the creation of the first viable product of blockchain.

Nakamoto continued to collaborate on the development of the technology until 2010, retaining roughly BTC[3] 1 million valued US$ 1.2 billion (March 2017), which are unspent and publicly monitored by fans of the mysterious inventor.

[3] Unofficial currency code for bitcoins, also known as XBT or by the symbol ฿.

4.3 FEATURES AND CONFIGURATIONS

4.3.1 Public vs. private vs. hybrid blockchains

The discussion on the features of blockchains architecture could not start from other points than the extent to which the blockchain is decentralized. Figure 3 shows typical network structures. Each of these types of network structure creates trade-offs between efficiency and security, or anonymity and decentralization.

A **public** blockchain is a distributed ledger accessible to every Internet user. As in Figure 3.(C), every node of the network has access to the blocks and can unconditionally participate in determining what blocks are added to the chain and what its current state is (Buterin, 2015a). These blockchains rest on a consensus mechanism of proof-of-work (or proof-of-stake) for validation: " in the case of

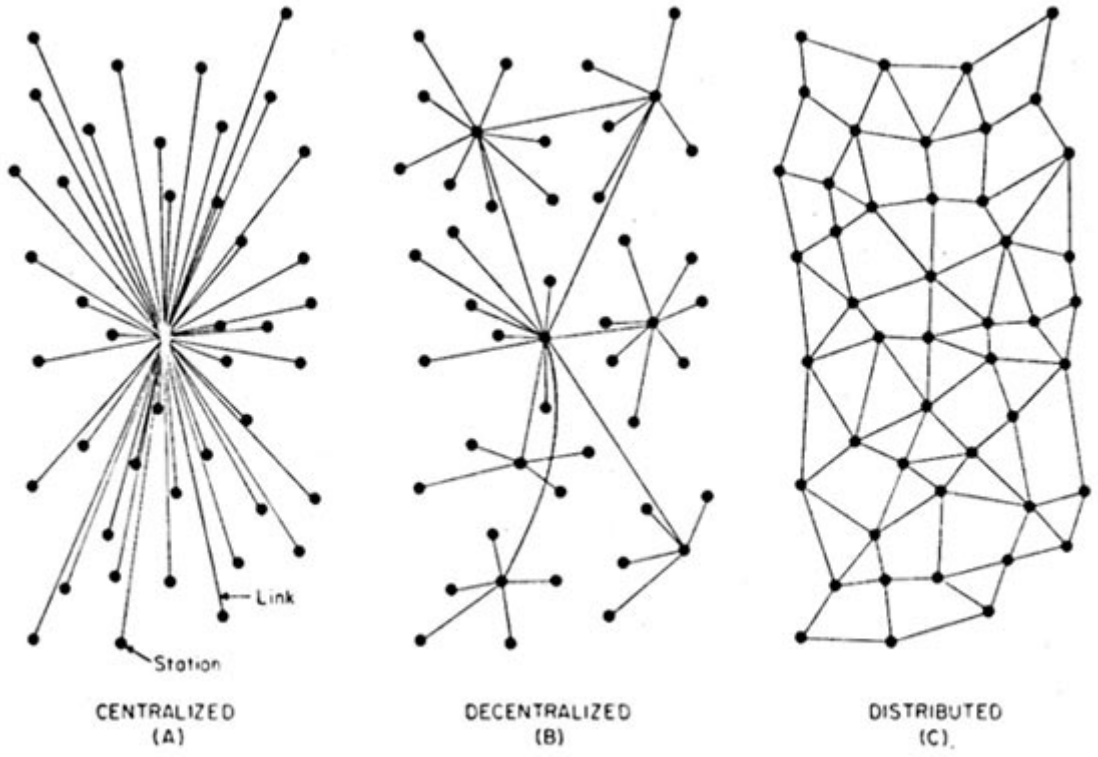

Figure 3 Types of network architecture. Source: Baran, P. (1962). On Distributed Communications.

Bitcoin, the "longest chain–the chain with the most proof-of-work– is considered to be the valid ledger" (Swanson, 2015, p. 4).

A **private** blockchain is a ledger where write-permissions and read-permissions are monitored and granted by a central locus of decision-making (Pilkington, 2015), "maintaining many kinds of partial guarantees of authenticity and decentralization that blockchains provide"(Buterin, 2015a). This entails an organizational process where user identity is known and cleared (or refused) by the most important node of the network. The process links all nodes to a central one (Figure 3**Errore. L'origine riferimento non è stata trovata.**.(A)).

There is no one-size-fits-all approach and therefore between the two types there exists a continuum of **hybrid** blockchains configurations (Allison, 2015; Brown, 2014) of "partially decentralized" blockchains (Buterin, 2015a) like in Figure 3**Errore. L'origine riferimento non è stata trovata.**.(B). Another name for these blockchains is **consortium** blockchains (ibid.). They allow the entity adopting/implementing the technology to decide whether the kingmaker points toward trust or anonymity.

4.3.2 Cryptography and pseudonymity

Barnas (2016) describes the blockchain technology as "trustworthy system in a trustless world". The 44% of the world population (World Bank Data, 2015) makes use of the Internet, carrying out transactions with parties hardly identifiable and on which trust is the main determinant for enabling transactions. Oftentimes the trust posed on the counterparty is not enough to guarantee the success of a transaction and new methods are applied to secure transactions,

especially economic ones. The reasons for claiming the trustworthiness of the blockchain are mainly two.

The first reason is that each user is identified by a univocally assigned alphanumeric string that identifies it in all the operations performed on the system. In a public blockchain, the real-life identity of the operator is preserved, ensuring anonymity, while holding the operator accountable for the actions performed. Some define this feature of blockchains as **pseudonymity** (Boucher, Nascimento, & Kritikos, 2017; Pilkington, 2015).

The second reason, which is the most important, is **cryptography**. Blockchain technology substitutes a system based on trust with one of "mathematically defined and mechanically enforceable rules" (Maxwell, 2015). This feature has led to a lively and growing discussion on how to define and interpret transactions on a blockchain, and Wright & De Filippi (2015) hold that a *Lex cryptographia* might be established. This characteristic of blockchain transaction is important as it ensures no double-spending (Nakamoto, 2008) and is based on precise mathematical rules and international cryptographic standards. For a non-currency use of blockchain it prevents the tampering of information and/or enables the punctual measurement of the chronology of changes to a piece of data within the blockchain. *Hashing*[4] relies on international standard, e.g. the SHA256 (Secure Hash Algorithm 256), usually issued by the National Institute for Standards and Technology (NIST).

[4] Hashing is the slang used by experts to indicate the process of transformation of any bit of data into an alphanumeric fixed length string through a cryptographic hash function.

4.3.3 Blockchain structure

The blockchain structure is composed by cryptographic "blocks" of records, with each block carrying information of the previous block, forming a chain of data, from which the term blockchain. The chain starts with a single block called **genesis block** on top of which are stacked the **children blocks**. **Errore. L'origine riferimento non è stata trovata.** provides a visual representation of a blockchain structure. Each block has a header containing the hash of the previous block (absent in the genesis block), the time stamp and the Merkle hash, which is derived by a cryptographic algorithm (the Merkle algorithm) that *hashes* all the information of the block. This allows the user to reconstruct rapidly the structure of the blockchain checking for its internal consistency (integrity of data).

Sometimes, authentication conflicts arise among nodes of the network. The problem, known as **forking**, derives from the disagreement about a proposed change to a public blockchain protocol or algorithm, which creates a bifurcation of the chain into two descendant blockchains with separate histories in the future. Apart from forking, bifurcation can occur in the blockchain as there are divergences in one or more key information of a single block. The conflicts are solved through the consensus mechanism, i.e. through the victory of the most CPU powered group of nodes (Mougayar, 2016; Swanson, 2015). **Size**, then,

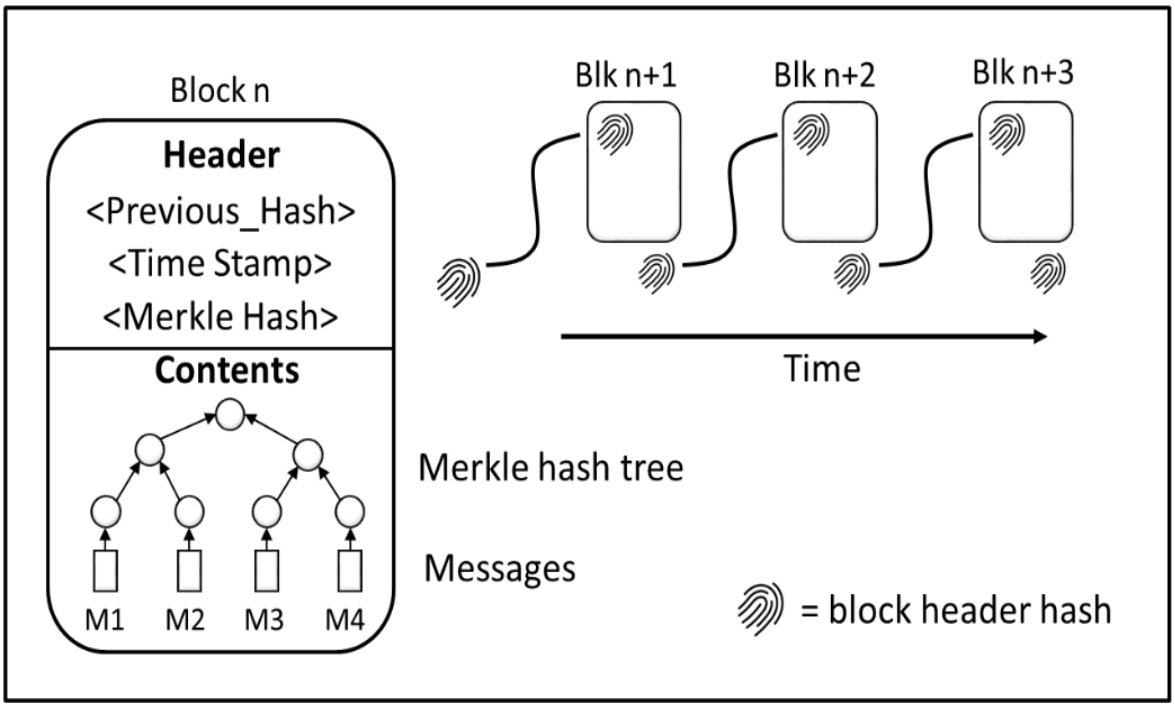

Figure 4 Blockchain structure formation. Barnas, N.B. (2016.) Blockchains in national defense.

does matter. The higher the number of nodes, the lesser is the probability of an external/internal attack aimed at tampering data. It has been calculated that the most popular blockchain application, the Bitcoin protocol, is virtually un-hackable. There is the need to combine 1000 times the computing capacity of the largest 500 supercomputers in the world to overtake the Bitcoin (source blockchain.info).

4.3.4 Licenses

The licensing model is one of the most relevant features, especially for public blockchains. Buterin (2015b) emphasized the licensing model for enabling changes to the software of the public ledger platforms. Open-source licenses are paramount so that users can adapt the platform in a collaborative style (Evans, 2014, p. 4). The term open development method (ODM), or community-led development, has been coined to describe this new collaborative mode of

governance, wherein the emphasis is primarily on collaboration and the community of users.

The Linux Foundation created the project Hyperledger[5], intending to unite individuals and firms, financial institutions included, for the development of the blockchain technology in an *open source* perspective.

4.4 Paradigm shift in cyber security: the State, Defense and Boundaries

The cutting edge of innovation, particularly in infrastructure, is often in the hands of the State (Mazzucato, 2015), and especially in the blockchain space this must be true. But, will the State be central in maintaining and administering any blockchain application?

The question puts into crisis the classic role of the State. Reconsidering the framework set out in §2.4 for cyber security, the introduction of blockchain systems in the picture may disrupt the cyberspace environment, eliminating the need for a trusted party as the middleman (Boucher et al., 2017; Wright & De Filippi, 2015). The central authority is not needed either, as the blockchain relies on protocols and the power of the group, in a sense empowering democracy and the diffusion of decentralized participation. The trend has also been underlined in the report "Global trends 2030: Alternative Worlds" by the US National Intelligence Council as being one of the megatrends for the next 15 years.

[5] https://www.hyperledger.org

The State assumes a defensive stance, but a minimal role in the system. The infrastructure is a relevant part of the blockchain system and the State should guarantee the smooth execution of the code, i.e. no zero-days bugs facilitating attackers. The system/s is/are then self-protecting from attacks (data-tampering, data theft, other attacks on the software side) and frauds are easily spotted. Furthermore, blockchain facilitates the monitoring of the activities within the system and the spotting of anomalies.

The absence of data governance in this regard is mediated through the agreement of the nodes participants to record their transactions on a ledger, be it public, private or hybrid. The collaborative features, highlighted above, foster the maintenance of the system and the validation of data.

The national cyberspace can be secured through a cost-effective infrastructure that the State should maintain in pursuit of national interests and defense. Co-responsibility is an even strengthened feature talking about blockchain, as firms have the utmost interest in strengthening the network and the infrastructure.

Actors in this context will work cooperatively, in a decentralized manner and with no central authority. Having the principles been set in the layout of the specific blockchain application, the rules are self-enforcing to keep the cyberspace secure.

In this way, also cyber safety is addressed, although part of it is still open to market-driven processes. Certainly, the blockchain cannot prevent users from opening malicious content on their machines. Nevertheless, unsafe behaviors

can be univocally tracked and, if the *lex cyptographia* is applied, it can help support legal evidence.

4.5 STRENGTHS AND WEAKNESSES

The blockchain technology is drawing attention and investments because of its multiple strengths and advantages of use. Still, it presents with some weaknesses that are worth being discussed, to acquire full awareness on the technology.

Tradeoffs occur in the design of a blockchain network. The **confidentiality** tradeoff is the most sensitive issue. Recalling §4.3.1, there are three ways blockchains can be configured to work: public blockchains, private blockchains, hybrid blockchains. Given the configuration, confidentiality can be completely inexistent or stringent. Public blockchains are efficient in validating information exchanged, but they do not guarantee any confidentiality on the data as the exchange is visible to every network participant. Private blockchains, on the other extreme, preserve the confidentiality of information exchanged and grant access to a restricted number of users, based on the permission cleared by a central authority. Hybrid blockchains are not easily framed. Depending on where they are positioned in the spectrum between public and private blockchains, they offer the blockchain designer with a good amount of freedom in deciding between efficiency and confidentiality.

The second element to be considered is the advantage to have a majoritarian consensus mechanism, mainly used to prevent hostile takeovers of the blockchain for data-tampering. It depends on some characteristics of the network (size, configuration of the network, alignment of interest of actors, CPU power of

the majority, degree of synchronization of the network, …), but it allows to have a clear validation of the transactions. In a military application, for example, it creates asymmetric advantage over an adversary by aligning the preponderance of "honest" nodes against a smaller number of "dishonest" nodes (Barnas, 2016). The **security** provided by blockchains is not dependent on secrets, neither on trust. There are no passwords, covert cryptographic keys or administrators (ibid.). Its core elements are sufficient to ensure security. Moreover, additional layers of security can be added, depending on the application.

Furthermore, in decentralized public blockchains there is the issue of **scalability**. The file size of the distributed ledger grows at every transaction and at the increment of the volume of transactions, the pace of growth soars. For example, the Bitcoin protocol file size increased exponentially through years and will more

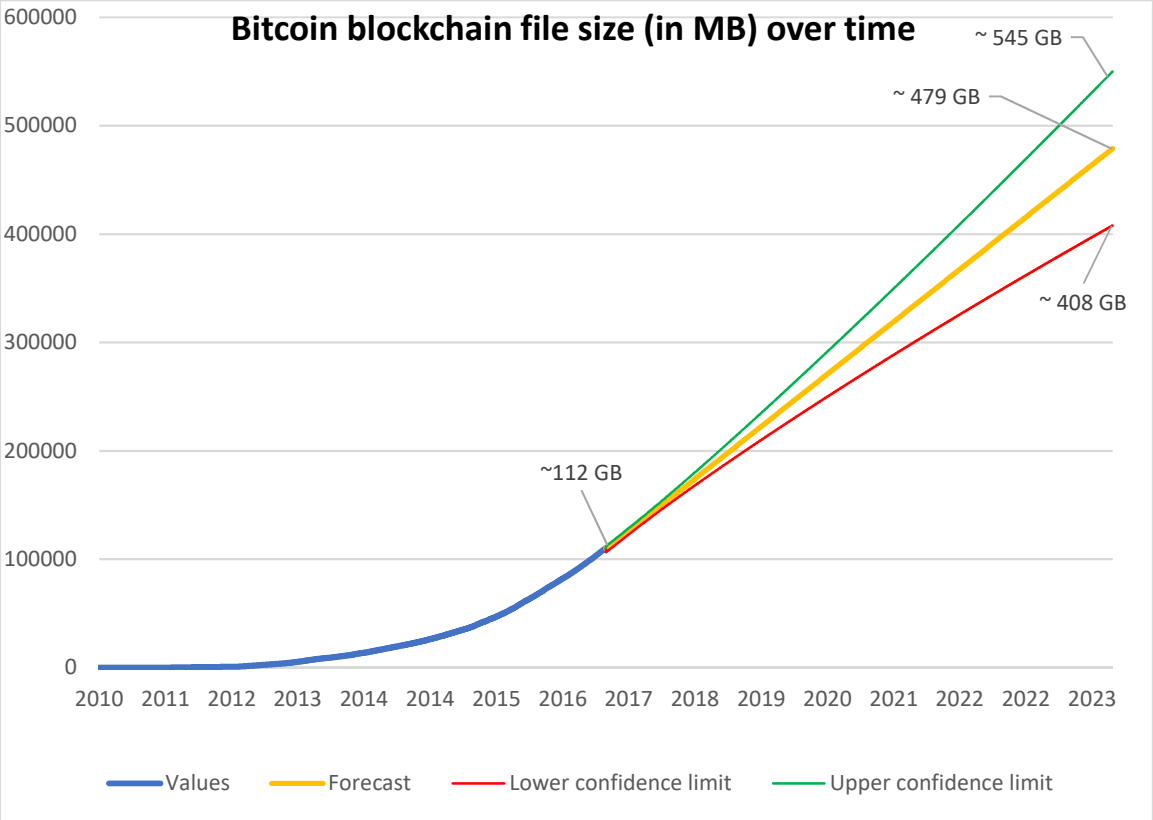

Figure 5 Bitcoin blockchain file size in a chronological perspective. Data source: blockchain.info elaborated for this document. Confidence interval 99%

than four-fold its dimensions in the period 2017-2024, as seen in **Errore. L'origine riferimento non è stata trovata.**, if it will keep the same pace. This is a critical issue as the file is not available for fragmentation, as it would corrupt the chain. Eventually, some nodes will quit the network as maintenance will be unbearable for most of them. Think of a private citizen using a laptop; with the present storage power the user will quit the network to save space on its drive. The issue is also called *blockchain bloat* (Wagner, 2014).

Transaction costs for transferring data or digital money are reduced dramatically and, as the hash rate of the network grows, the costs are increasingly cut (Buterin, 2015a) rendering inexpensive the system under this perspective, but they still take some time to be fully validated (Pilkington, 2015).

The system has the feature of **immutability**, which confers the intrinsic value to blockchains. Some of the characteristics of blockchains may change from application to application, but the immutability of data is crucial (Swanson, 2015, p. 59). Buterin (2015a) finds immutability to be a weakness of blockchain as Institution may need reversibility to be a desirable property of registries (e.g. land registries). However, Buterin (ibid.) acknowledges that a public ledger with smart contracts where government is one of the players in the network, shades the conclusion, without undermining it.

5 Applicability of blockchain solutions

The blockchain holds a high potential, as could be hinted in the previous chapter. A wide range of companies and organizations is investigating the extent to which the technology can be applied to their operations. Some are imagining the future of the world with blockchain being a fundamental part of exchanges.

Born as a cryptocurrency protocol, blockchain has gained traction and, year after year, investments are rising. Figure 6 shows the amount of investments in the period 2012-2016. As it can be noted, there was almost a threefold growth of investments between 2015 and 2016 that reached $1.4 billion according to Seamus Cushley, one of the 25 blockchain experts members of PricewaterhouseCoopers (PwC) in Belfast.

The investment in blockchain technologies is not just realized through start-ups, but also through in-house development and consortiums (Calzone, 2017).

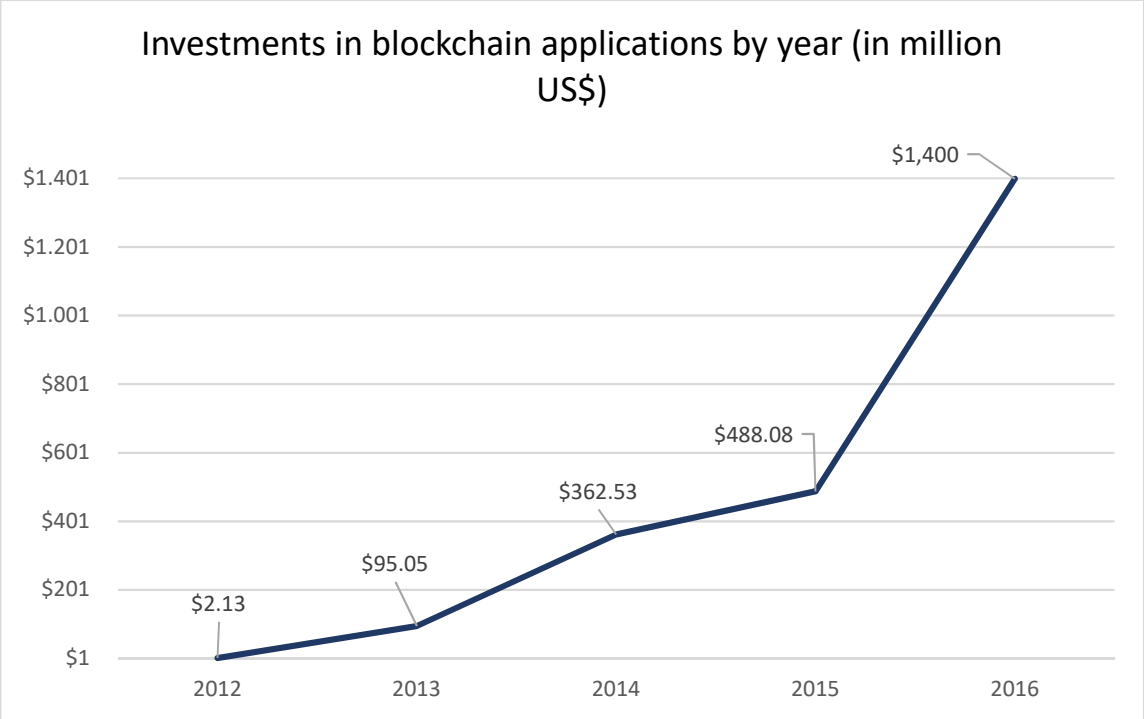

Figure 6 Blockchain investments by year. Various sources: businessinsider.com and PwC Belfast

Financial institutions are the main investors in the technology and there are already several patent requests for blockchain applications.

Previous chapters presented the challenges posed to security in and out of the cyberspace, examined the legislation for cyber security and the game-changing features of blockchain. This chapter aims at reviewing possible *non-financial* applications of the blockchain technology and the organizational changes brought about by the introduction of distributed ledger technologies.

5.1 APPLICATIONS OF THE BLOCKCHAIN

5.1.1 Anti-whistleblower systems

In 2013, the American Administration had to confront the reality of whistleblowers within its institutions. Edward Snowden[6], WikiLeaks[7] through American militaries and other exploited the privileged positions they had within the network they operated. Blockchains function independent of secrets and trust (Barnas, 2016). Snowden would not have had the opportunity to tamper the audit logs to cover his tracks, after downloading highly confidential files to leak to the press. "Blockchains enhance cyber Defense's perimeter security strategy, not by helping to hold up the walls, but by monitoring the walls and everything within them" (ibid.).

[6] Edward Joseph Snowden is an American computer professional, former Central Intelligence Agency employee, and former contractor for the NSA who disclosed numerous global surveillance programs run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunications companies and connivant governments. Source: en.wikipedia.org/wiki/Edward_Snowden

[7] WikiLeaks is an international non-profit organization that collects and publishes classified information from anonymous sources. At the time of writing, WikiLeaks holds a database of "more than 10 million [published] documents and associated analysis". Source: wikileaks.org/What-is-Wikileaks.html

Blockchains use consensus mechanisms to secure databases and register the log of activities for every user, that have the lowest probability of alteration. In this way, the configuration of systems can be stored on the network and monitored to spot (almost) instantly any change and tampering attempt. Blockchain is particularly promising for cybersecurity because the elimination of the need for trust enables the design of security systems not relying on a single central authority. And, a paradigm shift in security. "Instead of searching for vulnerabilities, equivalent to searching for a needle in a haystack, you can have mathematical certainty for every digital asset that constitutes the system you want to protect" (Gault, 2016).

5.1.2 Blockchain-enabled E-voting (BEV) systems

Notwithstanding the digitalization of many aspects of people's lives, voting is still bound in many parts of the world to paper and manual operations. The results of elections in countries where democracy is just a cover for dictatorship are easily tampered and piloted by one person/group of interests. E-voting is considered to be an inevitable development that could "speed up, simplify and reduce the cost of elections, and might even lead to higher voter turnouts" (Boucher, 2016).

Now we have a further choice. The decentralization is a trend that the blockchain technology wants to emphasize, a revolution in voting and security. The Bitcoin Foundation (2015) unveiled a project involving blockchain as founding element, a voting system which "provides even greater transparency into the voting process, with every vote being recorded on the blockchain".

Building on the features of immutability, consensus and transparency intrinsic of the blockchain technology, voting systems appear to have a major technological breakthrough (Pilkington, 2015). Every vote can be recorded under a cryptographic hash and communicated upon all the nodes of the voting system. The system has been developed and successfully tested in Russia by the National Settlement Depository (NSD). It operates on an e-proxy voting system running on a distributed ledger built with the NXT distributed cryptographic platform and its code is open-source. This system would facilitate the use of direct democracy; although most scholars and lay people are biased against direct democracy (Frey, 1994).

Some scholars are discussing the possibility of "techno-democratic systems" (Wright & De Filippi, 2015) and some virtual equivalents of national administrations are emerging, based upon blockchain technology (see, for example, BitNation).

5.1.3 Smart contracts

Smart contracts were defined by Szabo[8] in 1994 as "computerized transaction protocol that executes the terms of a contract". Brown (2015) provided a newer and clearer definition that applies to blockchains. In Brown's own words, smart contracts are "event-driven program[s], with state, which run on a replicated, shared ledger and which can take custody over assets on that ledger". By adjusting the code in the blockchain, "transactions can be executed automatically in response to certain conditions being met, providing a 'guarantee of execution'"

[8]http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

(Boucher et al., 2017). This interesting application of the blockchain is being developed in many forms and at an impressive rate. Trading assets could dramatically change, resulting in a simpler model with higher monitorability by every participant to the network. Figure 7 shows the transformation of the model for banks and payments with the adoption of smart contracts.

Since the blockchain is immutable, the agreed contract (and the underlying code) can only be changed if, at the time of entry, a precise condition for changes was foreseen. The traditional contract scheme gave the possibility to break the terms of the contract and face the consequences. The smart contract, being self-executing, rejects this possibility opening its flank to radical interpretations, such as "self-contained, self-performed and self-enforced", being supported by an "extreme" faction of the blockchain movement. However, when the code is associated to the law, like in Wright & De Filippi (2015), "any mistakes or accidental vulnerabilities become part of the contract too" (Boucher et al., 2017). The discussion is open as how to counter theft and illegal clauses. Considered within a broader system, the problem of illegal clauses is easily executed nullifying them through another self-executing "moralizer" code, previously entered in the blockchain.

"New government responsibilities could emerge in the process of applying traditional judicial processes to smart contracts, such as arbitration when bugs are found in contract-code. As programmers start to translate agreements into executable code, they are effectively making decisions about how they will be implemented in practice, which may mean they carry greater legal responsibilities" (ibid.).

5.1.4 Digital identity

The digital identity-related information is part of a discussion that involves interests in political, societal, legal and, arguably, philosophical terms.

In the digital age, blockchain can decentralize digital identity. The use of digital identity authentication methods is of great interests to many governments. India has the biggest program, but also EU is implementing e-ID programs (eIDAS) just to mention some.

An e-ID based on blockchain is useful to help fight corruption and crime, including people trafficking and slavery for over 2.4 billion poor people worldwide (Dahan

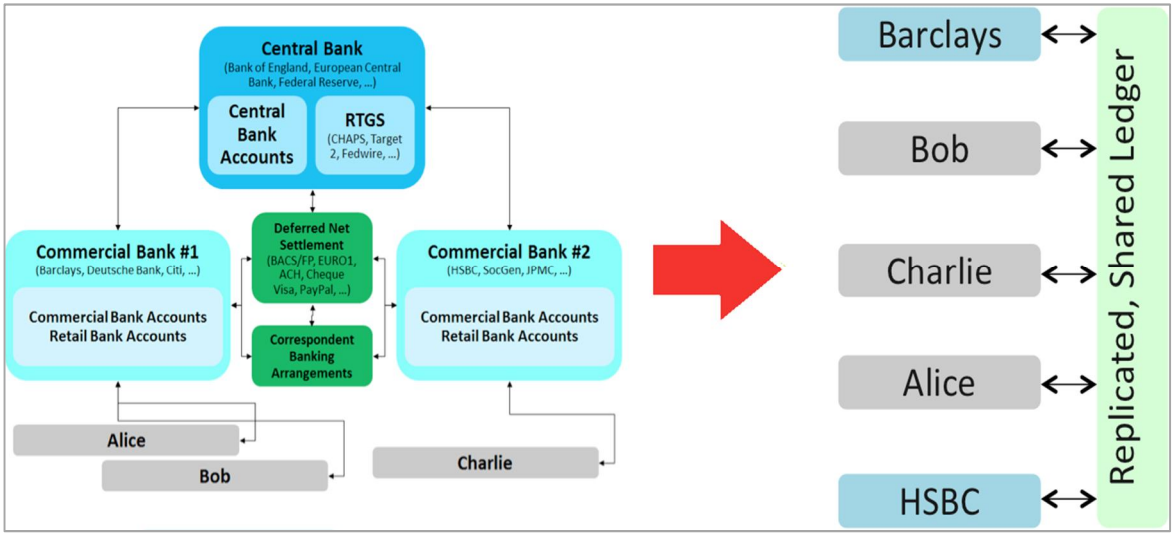

Figure 7 The revision of the system of banks and payments with the introduction of smart contracts

& Gelb, 2015). This is in line with the Sustainable Development Goal #16 about Peace, Justice, and Strong Institution, aiming to "provide legal identity to all, including birth registration, by 2030". It is, then, in the interest of a responsible government to implement the most robust system for identity verification universally accessible. The blockchain could be a cost-effective solution to prove identity, addressing the problem of rising costs due to population increase.

Here is a passage from the Harvard Business Review article "Blockchain Will Help Us Prove Our Identities in a Digital World" by Michael Mainelli, which describes best the changes triggered by the introduction of blockchain-backed digital identities:

> *The ultimate question surrounding an immutable identity ledger is this: Will it become a lifeline for people, or a burden? Using ledgers that never lose data could materially alter the way society views identity, privacy, and security. Bureaucratic slips such as a mistyped name can be corrected, but the slip can never be forgotten. Behaviors will change, and societal conventions will alter as a result. For example, we may be more tolerant of other people's histories when they can see our own unpaid fines or misdemeanors. Perhaps we will be more intrusive with important issues such as lying about academic qualifications, and more forgiving with lighter matters such as a few mediocre grades.*
>
> *And think of our permanent legacies. Perhaps we will act more responsibly if our legacy is indelible. For example, we might choose to donate our health data to research through smart contracts triggered by our death certificates. When our identities are forever etched in immutable stone, "Don't you forget about me" may prove to be a more enduring tune than we ever could have imagined.*

5.1.5 Supply chain

In a global world, supply chains are growing in complexity every day and it is difficult to maintain the same transparency and accountability of small supply chains. This is particularly a problem for food companies, which are not able to monitor suppliers in real time.

Blockchain would help making the supply chain trackability improve dramatically. Not only firms could transfer title and record permissions, but also activity logs to track the flow of goods and services everywhere. It resolves problems of disclosure and accountability between firms, individuals (i.e. the customers), and institutions (e.g. the Ministry of Health in the food sector) whose interests are not necessarily aligned. The blockchain would be time-effective as everyone in the blockchain would be updated instantly, removing the need for *a posteriori* reconciliation of internal records.

The technology can reveal hidden information and allows attaching digital tokens to the goods as they progress along the chain. This could open businesses to new markets and risk trading, since they can know the value of their goods at any point in time. A trivial example is a sudden market negative change triggered by an event. By the time the business acquires such information can redirect the supply chain by selling the intermediate products to other companies. In this sense, the blockchain becomes also a great tool for flexibility.

Advances in chip and sensor technology, which can translate data from the automated movement of physical goods, should enhance these emerging blockchain systems. It could be especially powerful when combined with smart

contracts (Casey & Wong, 2017). This would also allow the staff cleared to work on the blockchain to check on each other's work and monitor potential damaging actions (especially important in manufacturing).

5.1.6 Internet of Things (IoT)

The IoT is a recent phenomenon that was envisioned by Kevin Ashton during a presentation at Procter and Gamble in 1999. Ashton and his colleagues envisioned "a world in which all electronic devices are networked and every object, whether it is physical or electronic, is electronically tagged with information pertinent to that object" (Sarma, Brock, & Ashton, 2000). The first IoT product was and EPC (Electronic Product Code) network for automatically identifying and tracing the flow of goods in supply chains (Kaukalias & Chatzimisios, 2015). As shown in Figure 8, the development of such technologies brought to a wide array of applications, ranging from agriculture to home appliances. "The explosion in number of smart, connected, and inherently insecure devices is shifting the security paradigm" (Weber & Studer, 2016).

Poorly protected machines can be hijacked: in 2016, about 100,000 IoT devices were used, unbeknownst to the owners, to disrupt the operations of high-profile targets including social platforms Twitter and Reddit (Biancotti, 2017). The poor awareness of the potential threat these "things" represent demands for a rapid and game-changing solution. Bug bounty programs aside, the devices need to be protected from cyber theft and tampering.

The blockchain may be the solution to prevent inconveniences as the one above or like the Liberian example in in the Introduction.

Blockchain-based approaches provide decentralized security and privacy, yet they involve significant energy, delay, and computational overhead that is not suitable for most resource-constrained IoT devices. Recently, a new approach has been proposed that minimizes the energy spent and enhances security and privacy for the users (Dorri, Kanhere, Jurdak, & Gauravaram, 2017). The research provides detailed analysis to assess the efficiency for the approach in a smart home application (ibid.). However, the approach is still at its preliminary stages of evaluation and new IoT domains will be tested in the future.

5.1.7 Applications in National Defense

Barnas (2016), a US Air Force developmental engineer and acquisition manager, was the first to describe Cyber Defense as "the most near-term, low-cost, high-payoff application of blockchain technology."

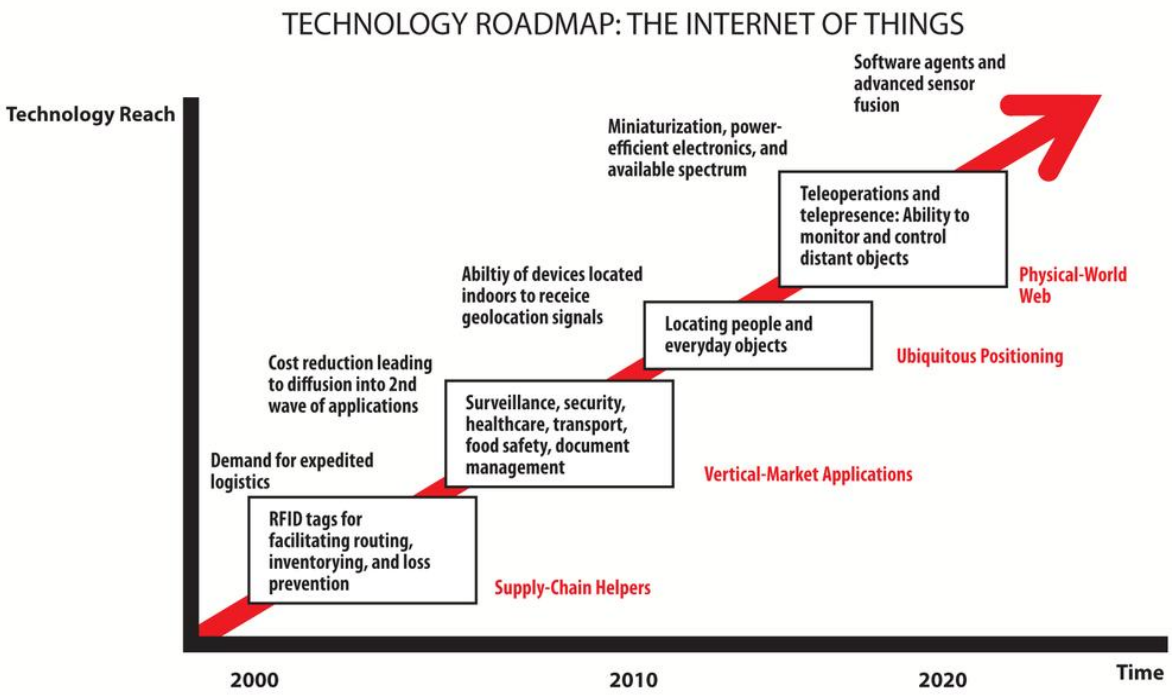

Figure 8 Internet of things technology roadmap (SRI Consulting Business Intelligence, 2008)

The data integrity that the technology offers is the most valuable piece of technology that can be desired by the National Defense in a hostile environment where the growth of threats outpaces the growth of effective countermeasures.

The supply chain for defense systems would benefit from the same advantages and strengths seen in §5.1.5. Establishing the exact ownership of an asset is critical to avoid deliberate vulnerabilities that could be implanted in a system by an adversary. The Defense Ministry could demand every design iteration to be logged in a blockchain, as well as every sale of batches and their allocation to specific assemblies (Barnas, 2016).

As the efficiency of secure blockchain networks increases, more time-sensitive applications can be implemented, such as secure voice-over-Internet-protocol (VOIP) applications – "a truly resilient and anonymous version of Skype"(Baron et al., 2015).

Such applications could be useful for national-security users. However, there are risks involving the use of such tools by adversaries or low skilled terrorists that would have access to more resilient services than they would have otherwise (ibid.).

5.2 Risks of Adopting Blockchain solutions

As described in the previous section, there are vast array of applications or dilemmas that can be solved using blockchain technology, spanning from financial to non-financial applications. Most of the solutions are disruptive for the sector of application. One of the main challenges in using blockchain for non-

financial applications will be the incentivization linked to the securing of a decentralized system (Baron et al., 2015, p. 60).

A mismanaged transition to blockchain-based products could be misunderstood by users and the technology could be put aside for more comprehensible and "tangible" technologies.

First, there is the **behavior change** problem. Everyone takes change for granted as a constant in life, but there is often resistance to change. People need to trust the technology before relying on it.

Scaling is the most taunting problem both for experts and entrepreneurs. The current nascent services based on blockchain present the challenge of the exponentially growing base of blockchain blocks. A first-time user would get discouraged in downloading a complete set of blocks and validate them before executing the first transaction. The first download could take hours or longer, given the exponential growth rate of blocks.

The growth of blocks is the minor problem considering the point of view of an Institution or a company willing to move on blockchain the existing documents/frameworks. The **bootstrapping** would comprise a significant set of migration tasks that need to be executed, all of which could be failed by the operator creating an indelible error. The move may also involve time and costs, holding the Institution from taking the step.

To add fuel on the fire, **government regulations** risk to significantly slow down the transactions on the blockchains because they were conceived for an analogic world and need to be adapted rapidly to facilitate the adoption of blockchain-

based solutions in multiple sectors. Not to count the hostility of governmental Agencies' employees that would see emptied the role of their Agency, facing shutdown. However, the problem would be overcome by introducing laws to monitor and regulate the industries for compliance (Nachiappan, Crosby, Pattanayak, Verma, & Kalyanaraman, 2016).

Fraudulent activities are also an issue, given the pseudonymous nature of blockchain transactions. Activities like money trafficking are not new to blockchain applications, as the Bitcoin is said to have favored the movement of illegal capitals for a long time. With enough regulations and the needed technology support, law enforcement agencies will be able to monitor and prosecute these individuals.

A side-discourse would be needed for technologies threatening the integrity and validity of blockchain. For example, the advent of **quantum computing**[9]could threaten the cryptographic keys security and bring the whole system to its knees (Nachiappan et al., 2016).

[9] Computers based on the quantum theory, i.e. the science that studies the energy and matter on the quantum (atomic and subatomic).

6 Conclusions: Blockchain, the way ahead

The Internet has changed the way we connect and act in the world. Time and space collapsed and at the present time people take the fifth domain for granted. The exchange of data has made costs drop and efficiency sharply increased. However, security implications are only acquiring importance since a few years.

In chapter 2 security paradigms have been discussed to understand the perception of how security should be achieved, its processes organized, and key actors included. The insights gained from the exploration reveal that although European Schools differ in views from their overseas counterparts, they fail to effectively address the challenges deriving from a huge technological advancement like the creation of a cyberspace. Some attempted to keep those Schools up to date, but the academic community seems to be puzzled about definitions and mechanisms to securitize the cyberspace and national interests.

Hence, a proposal to define and foster the shift of the security paradigm. The author argued that cyber security studies need to become a field of study, where interdisciplinary work is done in order to guarantee clarity when confronting issues that involve actions in the cyberspace, but also reflect on International Relations dynamics. The achievement of cyber security for national cyberspace actors in the international cyberspace is an important matter.

Legislative actions have been taken to ensure cyber security in Europe and in Italy in the last two years. The NIS directive, discussed in chapter 3, represents a milestone in the EU cyber security discourse, changing the Union regulatory scenario and affecting industries. It introduced a minimum harmonization

scheme, that is bound to become the backbone of the cyber security strategy in Europe. Nonetheless, there is the risk of legal fragmentation among states, creating harmful spillover for European industries. Also, the tracking of the impact of the NIS will become very difficult. There is the need to work on trust between firms and competent authorities with the aim to encourage cyberattacks reports.

The exclusion of small and medium enterprises is a gap to be filled in the European legislation, because of the role they have in the supply chain of big companies and the use they make of networks.

The Italian Decree for cyber security, recently approved and published in April 2017, creates a simple, yet effective, institutional architecture replacing the 2013 Monti Decree. Cyber security acquired a pivotal strategic role for Italy, considering the increasing complexity of threats. The national Cyber Security Unit has been staffed under the *Dipartimento di informazione per la Sicurezza,* making the intelligence community leader of the decision-making process. The Decree aims at facilitating the defense of critical infrastructures through a coordinated and prompt response involving public and private actors.

However, while new laws are passed, innovative technologies are developed at a faster pace. This is the case of the blockchain, the underlying mechanism of the more famous Bitcoin protocol. In chapter 4, the innovative approach to security and data exchange that this technology brings was discussed. It is a complex technology, but it is appealing for investors. The assumption of the chapter is that the cyberspace is flawed and, thus, insecure. It explained the features of the

technology, as well as its strengths and weaknesses in order to assess the role it could have in stepping up the cyber security challenge. A section was also devoted to assessing the changes that blockchain could bring in terms of approach to security.

Finally, chapter 5 presented the reader with seven non-financial applications of the blockchain to illustrate the way blockchain can be used to increase security. The amount of private investments on this technology is growing exponentially year after year. The seven cases were: anti-whistleblower systems, BEV systems, smart contracts, digital identity, supply chain applications, IoT, and applications in national defense. All these applications present risks for adoption relating to distinct factors, both technological and of human nature. However, scarce information on these risks prevented the author from further elaborating on them.

The evidence from non-financial applications hints at the benefits arising from decentralization and a progressive reduction of the role of the state in providing security. At the Defense level, the blockchain is not only good for cyber security, it serves also as a deterrence by denial mechanism. Indeed, deterrence is the most discussed issue for cyber security in military environments. In this sense, we cannot compare cyber weapons and cyber threats to any other historical threat. For example, any State could respond to nuclear threat by nuclear deterrence, thus building up an arsenal of nuclear weapons to discourage any opponent from attacking. Cyber weapons can be easily crafted to respond to the needs of the attacker, based on the profile of the target. There are no standard

countermeasures to be adopted, but blockchain could be the solution to implement deterrence by denial.

In any case, the human factor is still relevant, as any error in programming a smart contract or in BEV systems would cause irreversible damage. Therefore, there is probably the need to educate people to the cyber security and cyber safety culture.

Many challenges arise from this document that deserve future study. The most important one is to assess the risks and weaknesses of blockchain to find solutions that mitigate them. The tradeoffs between technological advancement and the willingness of a population to use such services is not to be underestimated, hence a usability study would be beneficial. Careful evaluation is needed to evaluate the illegal or immoral uses it may facilitate, especially for pedo-pornography and terrorism purposes.

Last, but not least, there is the need to integrate research in Security Studies (or, better, Cyber Security Studies) with the implications of a fully decentralized system.

Just like the Internet or the smartphone, the blockchain technology is a truly innovative technology. It deserves the same level of attention, if not more, by states of that private investors are putting into it.

Appendix

Policy recommendations for Italy

Recommendation 1: There is currently limited awareness in the public sector about this emerging technology. The CISR may propose effective Implementing Decrees to facilitate the work of the research committee in partnership with CIIS (Cyber Intelligence and Information Security Research Centre) Sapienza and other academic research centres. Research is needed to ensure a scalable, adaptable and secure design based on proprietary cryptographic standards. Early research provides an advantage in spotting vulnerabilities, perfecting design and developing powerful defences to the network. Some research is already there on the internet as the Bitcoin project is open source and a growing community is testing different coding alternatives. It is important to prepare for the future of data-fighting.

Recommendation 2: Italy may want to seek partnership opportunities with the private sector to develop blockchain technologies for mutual benefit. It may invest in Italian start-ups dedicated to blockchain and it may use the investment fund to acquire the necessary know-how to develop services based on the technology. The Italian Cyber Defence and the private sector face common challenges and threats, including cyber espionage. Further cooperation is needed to strengthen the Italian System (*Sistema Paese)* and the future Implementing Decrees may want to stress the role of cooperation incentivizing firms willing to share information and cooperate on cyber security.

References

- AA.VV. (2016). *Italian Cyber Security Report. A national Cyber Security Framework*. (R. Baldoni & L. Montanari, Eds.) (1.0). Rome.
- Abbott, A. (2004). *Methods of Discovery: Heuristics for the Social Sciences*. New York: Northon & Company.
- Allison, I. (2015). Bank of England: Central banks looking at "hybrid systems" using Bitcoin's blockchain technology. Retrieved April 2, 2017, from http://www.ibtimes.co.uk/bank-england-central-banks-looking-hybrid-systems-using-bitcoins-blockchain-technology-1511195
- Anderson, R. (2003). Cryptography and Competition Policy–Issues with Issues with Trusted Computing. *The European Journal for the Informatics Professional*, *IV*(3), 35–41.
- Angrishi, K. (2017). Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets.
- Aradau, C. (2004). Security and the Democratic Scene: Desecuritization and Emancipation. *Journal of International Relations and Development*, *7*(4), 388–413.
- Arquilla, J. (1999). Can information warfare ever be just? *Ethics and Information Technology*, *1*(3), 203–212.
- Arquilla, J., & Ronfeldt, D. (1999). The Advent of Netwar: Analytic Background. *Studies in Conflict & Terrorism*, *22*(3), 193–206.
- Arquilla, J., & Ronfeldt, R. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND.
- Back, A., Corallo, M., Dashjr, L., Friedenback, M., Maxwell, G., Miller, A., … Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. Retrieved from http://www.blockstream.com/sidechains.pdf
- Baldwin, D. A. (1995). Security studies and the end of the Cold War. *World Politics*, *48*(1), 117–141.
- Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations*, *11*(2), 171–201.

- Balzacq, T. (2010). *Securitization theory: how security problems emerge and dissolve*. Routledge.
- Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., & Gupta, S. K. S. (2012). Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems. In *Proceedings of the IEEE* (Vol. 100, pp. 283–299).
- Barnas, N. B. (2016). *Blockchains in national defense: trustworthy systems in a trustless world* (Blue horizons Fellowship). Maxwell Air Force Base, Alabama.
- Baron, J., Mahony, A. O., Manheim, D., & Dion-schwarz, C. (2015). *National Security Implications of Virtual Currency*. Santa Monica, California.
- Bendrath, R. (2003). The American cyber-angst and the real world - Any Link? In R. Latham (Ed.), *Bombs and bandwidth: the emerging relationship between Information Technology and Security*. The New Press.
- Berners-Lee, T. (1989). The original proposal of the WWW, HTMLized. Retrieved from https://www.w3.org/History/1989/proposal.html
- Biancotti, C. (2017). *Cyber attacks: preliminary evidence from the Bank of Italy's business surveys* (Occasional Papers No. 373).
- Bigo, D. (2000). When two become one: internal and external securitisations in Europe. In M. Kelstrup & M. C. Williams (Eds.), *International Relations Theory and the Politics of European Integration* (pp. 171–204). Routledge.
- Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives: Global, Local, Political*, *27*(1 suppl), 63–92.
- Booth, K. (1991). Security and emancipation. *Review of International Studies*, *17*(4), 313.
- Booth, K. (1994). Security and Self Reflections of a Fallen Realist. *Strategies in Conflict: Critical Approaches to Security Studies*, (26), 12–14.
- Booth, K. (2005). *Critical security studies and world politics*. Lynne Rienner Publishers.
- Boucher, P. (2016). *What if blockchain technology revolutionised voting ?* (What if...?).
- Boucher, P., Nascimento, S., & Kritikos, M. (2017). *How blockchain technology could change our lives* (No. PE 581.948).

- Brown, R. G. (2014). The "Unbundling of Trust": how to identify good cryptocurrency opportunities? Retrieved April 2, 2017, from https://gendal.me/2014/11/14/the-unbundling-of-trust-how-to-identify-good-cryptocurrency-opportunities/
- Brown, R. G. (2015). A Simple Model for Smart Contracts. Retrieved April 19, 2017, from https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/
- Buterin, V. (2015a). On Public and Private Blockchains. Retrieved April 2, 2017, from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
- Buterin, V. (2015b). The value of the blockchain technology. Retrieved April 5, 2017, from https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/
- Buzan, B. (1984). Peace, Power, and Security: Contending Concepts in the Study of International Relations. *Journal of Peace Research*, *21*(2), 109–125.
- Buzan, B. (1991). *People, States and Fear: An Agenda for International Security Studies in the post-cold war era*. Harvester Wheatsheaf.
- Buzan, B., & Waever, O. (2003). *Regions and powers: the structure of international security*. Cambridge University Press.
- Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: a new framework for analysis*. Lynne Rienner Publishers.
- Calzone, O. (2017). *Bitcoin e distributed ledger technology* (Il mondo dell'Intelligence).
- Casey, M. J., & Wong, P. (2017). Global Supply Chains Are About to Get Better, Thanks to Blockchain. Retrieved April 24, 2017, from https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain
- Clarke, R. A., & Knake, R. K. (2011). *Cyber War: The Next Threat to National Security and What To Do About It ."*. HarperCollins.
- Computer Science and Telecommunications Board. (1991). *Computers at Risk*. Washington, D.C.: National Academies Press.
- *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. (2013).

- Dahan, M., & Gelb, A. (2015). *The Identity Target in the Post-2015 Development Agenda* (Connections No. 19).
- Dai, W. (1997). Cryptographic system and method with fast decryption.
- Dai, W. (1998). b-money. Retrieved March 30, 2017, from http://www.weidai.com/bmoney.txt
- Deibert, R. J., & Stein, J. G. (2002). Hacking Networks of Terror. *Dialogue IO*, *1*(1), 1–14.
- Der Derian, J. (1992). *Antidiplomacy: spies, terror, speed, and war*. Blackwell.
- Der Derian, J. (2003). The Question of Information Technology in International Relations. *Millennium*, *32*(3), 441–456.
- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT Security and Privacy : The Case Study of a Smart Home Blockchain for IoT Security and Privacy : The Case Study of a Smart Home, (March).
- Dunn Cavelty, M. (2012). The militarisation of cyber security as a source of global tension. In D. Möckli (Ed.), *Strategic trends 2012* (pp. 103–124). Zurich: Center for Security Studies, ETH Zurich.
- ERIKSSON, J. (1999). Observers or Advocates? *Cooperation and Conflict*, *34*(3), 311–330.
- Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*, *27*(3), 221–244.
- European Commission. (2015). A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen. *European Commission - Press Release*.
- European Parliament, & Council of the European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, *2014*(March 2014).
- Evans, D. (2014). *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms* (No. Research Paper No. 685). https://doi.org/10.2139/ssrn.2424516
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War.

Survival, *53*(1), 23–40.

- Franklin, M. I. (2013). *Digital Dilemmas*.
- Frey, B. S. (1994). Direct Democracy: Politico-Economic Lessons from Swiss Experience. *The American Economic Review*, *84*(2), 338–342.
- Gault, M. (2016). Blockchain and implications for trust in cyber security | cyber security law & practice. *Cyber Security Law & Practice*, *2*(2).
- Glaser, C. L. (1997). The security dilemma revisited. *World Politics*, *50*(1), 171–201.
- Haber, S., & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*, *3*(2), 99–111.
- Hack Attacks cut internet access in Liberia. (2016). Retrieved March 16, 2017, from http://www.bbc.com/news/technology-37859678
- Hansen, L. (2000). The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. *Millennium*, *29*(2), 285–306.
- Hansen, L. (2008). Visual Securitization: Taking Discourse Analysis from the Word to the Image. In *49th International Studies Convention*. San Francisco.
- Hansen, L. (2010). De-Securitization, Counter-Securitization, or Visual Insurgency? Exploring Security Discourses through Responses to the Muhammad Cartoons. In *51th Annual Convention of the International Studies*. New Orleans.
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.
- Haslam, J. (2002). *No Virtue Like Necessity: Realist Thought in International Relations Since Machiavelli*. Yale University Press.
- Horkheimer, M. (1972). *Critical Theory: Selected Essays*. A&C Black.
- Hundley, R. O., & Anderson, R. H. (1995). Emerging challenge: security and safety in cyberspace. *IEEE Technology and Society Magazine*, *14*(4), 19–28.
- Huysmans, J. (2002). Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security. *Alternatives: Global, Local, Political*, *27*(1 suppl), 41–62.
- Huysmans, J. (2006). *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. (B. Buzan, Ed.). Routledge.
- Internet World Stats. (2017). World Internet Users and 2017 Population Stats.

Retrieved March 17, 2017, from http://www.internetworldstats.com/stats.htm

- Kaukalias, T., & Chatzimisios, P. (2015). Internet of Things (IoT). In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 7623–7632). IGI Global.
- Klimburg, A. (2012). *National cyber security framework manual*. NATO Cooperative Cyber Defence Centre of Excellence.
- Konst, S., & Wätjen, D. (2000). Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge.
- Krasner, S. D. (1978). *Defending the National Interest*. Princeton University Press.
- Krause, K., & Williams, M. C. (1996). Broadening the Agenda of Security Studies: Politics and Methods. *Mershon International Studies Review*, *40*(2), 229.
- Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 24–42). Potomac Books Inc.
- Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, *2*(1), 29–41.
- Machiavelli, N. (1532). *Il Principe*.
- Mainelli, M. (2017). Blockchain Will Help Us Prove Our Identities in a Digital World. *Harvard Business Review*.
- Maj. Gen. Barrett, M., Bedford, D., Skinner, E., & Vergles, E. (2011). *Assured Access to the Global Commons by Major General Mark Barrett Eva Vergles 3 April 2011 research , design and production expertise*. Norfolk, Virginia.
- Maxwell, G. (2015). Bringing New Elements to Bitcoin with Sidechains. In *San Francisco's Bitcoin Developers Meetup*. San Francisco.
- Mayer, M., de Scalzi, N., Martino, L., & Chiarugi, I. (2013). International Politics in the Digital Age: Power Diffusion or Power Concentration? In *XXVIIth SISP CONFERENCE* (p. 64). Florence.
- Mazzucato, M. (2015). *The Entrepreneurial State*.
- McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations*, *14*(4), 563–587.
- Mcsweeney, B. (1996). Identity and security: Buzan and the Copenhagen

school. *Review of International Studies*, *22*(1), 81.

- Mearsheimer, J. J. (2003). *The Tragedy of Great Power Politics*. *Book*.
- MEMO/16/2422. (2016). Brussels: European Commission.
- Miller, S. E. (2001). International Security at Twenty-five: From One World to Another. *International Security*, *26*(1), 5–39.
- Ministri, P. del C. dei. Decreto del Presidente del Consiglio dei ministri, 17 Febbraio 2017 (2017). Rome: Presidenza del Consiglio dei Ministri.
- Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39.
- Morgan, P. M. (1999). Liberalist and realist security studies at 2000: Two decades of progress? *Contemporary Security Policy*, *20*(3), 39–71.
- Morgenthau, H. J. (1951). *In Defense of the National Interest*. University Press of America.
- Mougayar, W. (2016). *The business blockchain : promise, practice, and application of the next Internet technology*. John Wiley & Sons Inc.
- Nachiappan, Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*, (2).
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- National Intelligence Council. (2012). *Global trends 2030: Alternative Worlds*.
- *Network and Information Security: Proposal for A European Policy Approach*. (2001).
- Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, *7*(2), 61–73.
- Pilkington, M. (2015). Blockchain Technology: Principles and Applications. *Research Handbook on Digital Transformations*, 1–39.
- *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*. (2009).
- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Official Journal L 077 § (2004). The European Parliament and the Council of the European Union.
- Reus-Smit, C., & Snidal, D. (2008). *The Oxford Handbook of International*

Relations. (C. Reus-Smit & D. Snidal, Eds.), *The Oxford handbook of international relations*. Oxford University Press.

- Rynning, S., & Guzzini, S. (2001). *Realism and Foreign Policy Analysis*.
- Sarma, S., Brock, D., & Ashton, K. (2000). The networked physical world.TR MIT-AUTOID-WH-001 MIT Auto-ID Centre,. *Auto-ID Center White Paper MIT- ...*, 1–16.
- Saunder, M., Thorn, H. A., & Lewis, P. (2007). *Research Methods for business students* (4th ed.).
- Schweller, R. L. (1994). Bandwagoning for Profit: Bringing the Revisionist State Back In. *International Security*, *19*(1), 72–107.
- Schweller, R. L. (1996). Neorealism's status-quo bias: What security dilemma? *Security Studies*, *5*(3), 90–121.
- Shepherd, L. J. (2013a). *Critical Approaches to Security: An Introduction to Theories and Methods*. *Journal of Chemical Information and Modeling* (Vol. 53).
- Shepherd, L. J. (2013b). *Critical Approaches to Security: An Introduction to Theories and Methods*.
- Smith, S. (1999). The increasing insecurity of security studies: Conceptualizing security in the last twenty years. *Contemporary Security Policy*, *20*(3), 72–101.
- Smith, S. (2005). The contested concept of security. In *Critical Security Studies and world politics* (pp. 27–62).
- Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations*, *13*(3), 357–383.
- Swanson, T. (2015). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*.
- Taliaferro, J. W. (2001). Security Seeking under Anarchy: Defensive Realism Revisited. *International Security*, *25*(3), 128–161.
- The Bitcoin Foundation. (2015). Voting on the Blockchain - Version 1.0 - Bitcoin Foundation. Retrieved April 15, 2017, from http://bitcoinfoundation.org/voting-on-the-blockchain-version-1-0/
- Third, A., Forrest-Lawrence, P., & Collier, A. (2014). *Addressing the Cyber Safety Challenge: from risk to resilience*. Sidney.
- Van Evera, S. (1999). *Causes of war: Power and the roots of conflict*. Ithaca,

NY: Cornell University Press.

- Wæver, O. (1995). Securitization and Desecuritization. In R. D. Lipschutz (Ed.), *On Security* (pp. 46–86). New York: Columbia University Press.
- Wæver, O. (2004). Aberystwyth, Paris, Copenhagen New "Schools" in Security Theory and their Origins between Core and Periphery. *Paper Presented at the Annual Meeting of the International Studies Association, Montreal, March 17- 20, 2004*, *Geo-Cultur*, 23.
- Wæver, O., Buzan, B., Kelstrup, M., & Lemaitre, P. (1993). *Identity, migration and the new security agenda in Europe*.
- Wagner, A. (2014). Ensuring Network Scalibility: How to Fight Blockchain Bloat. Retrieved April 10, 2017, from https://bitcoinmagazine.com/articles/how-to-ensure-network-scalibility-fighting-blockchain-bloat-1415304056/
- Waltz, K. N. (1959). *Man, the state, and war: a theoretical analysis*. New York: Columbia University Press.
- Waltz, K. N. (1975). Theory of International Relations. In F. I. Greenstein & N. W. Polsby (Eds.), *International Politics, Handbook of Political Science* (pp. 1–85). Reading.
- Waltz, K. N. (1979). Theory of International Politics. *Theory of International Politics*, 1–251.
- Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law and Security Review*, *32*(5), 715–728.
- Williams, M. C. (2003). Words , Images , Enemies : Securitization and International Politics. *International Studies Quarterly*, *47*, 511–531.
- Wohlforth, W. C. (2008). Realism. In C. Reus-Smit & D. Snidal (Eds.), *The Oxford handbook of international relations* (pp. 131–149). Oxford University Press.
- Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network*, 4–22.
- Wyn Jones, R. (1999). *Security, Strategy, and Critical Theory*. Lynne Rienner Publishers.

Abstract

The advent of the Internet in the last decade of the twentieth century and its diffusion around the globe made social, economic, relational, military, political structures change dramatically. Time and space collapsed with the hyperbolic development of data transfer technologies. The fifth domain conceitedly acquired a considerable importance in people's everyday lives. Our memories are confined in a vulnerable and fragile domain.

Furthermore, the development of technologies is constantly growing, creating a state of interconnectedness between different devices, as well as between industries and actors across the world (Eriksson & Giacomello, 2006). The growth has been so exponential that security implications did not have the chance to be studied and/or governed by policy analysts and theorists. Especially in Security Studies there has been little discussion on the implications of exchanging data in a space where national borders constitute no frontier and actors of various nature operate.

Moreover, the use of the Internet grew by roughly 924% in the period from 2000 to 2017 (Internet World Stats, 2017) and has become a fundamental component in daily life for all actors. It is estimated that in 2020 sixty per cent of the world's population will have access to the Internet. Fifty billion physical objects and devices will be connected to the Internet, which amounts to ten devices per online individual (Klimburg, 2012). The cyberspace is a global phenomenon that constitutes opportunities and challenges (Kuehl, 2009). For NATO, this means that loss of access to the Internet will have critical consequences to the prosperity of a nation (Maj. Gen. Barrett et al., 2011).

I find it perhaps curious that although cyber threats are framed as a security issue, it seems no effective solution to monitor and secure cyberspace is tested as attacks continuously grow in number and complexity. Therefore, the challenge is the effective governance of the flows of data without altering the features of the cyberspace, i.e. monitoring the cyberspace to spot harmful behaviors that could seriously damage national economies, infrastructures and citizens.

The blockchain technology creates the opportunity for analysts to study innovative policies to govern the cyberspace without a central authority. A blockchain is a database that stores digital records. The group of network participants, all of whom can submit new records for inclusion, shares the database. However, those records are only added to the database based on the agreement, or consensus, of the majority of the group. Additionally, once the records are entered, they can never be changed or erased. In sum, blockchains record and secure digital information in such a way that it becomes the group's agreed-upon record of the past. This technology has the advantage to create the space for trustless exchanges of "data" exploiting the networked nature of the cyberspace. A further advantage is derived from the immediate measurability of the genuineness of exchanges by all the participants to the network.

I argue that the blockchain is a game-changer in cyber security, fostering public-private partnerships and changing the role of the State in providing cyber security. Using case studies, I highlight the shift in security from a top down guarantor, the State, to a bottom up approach, i.e. the distribution of responsibility among network participants. The decentralization is a key theme introduced by the development and diffusion of this technology. However, cyber security has always been policy-oriented and pragmatic. Giacomello stated: "[there has been] little or no effort made to apply or develop theory"

(Eriksson & Giacomello, 2006, p. 3). The work aims to give theoretical contribution to the theory of cyber security. At the same time, the use of blockchain changes the roles and stances of the actors involved in security and this work takes this into account.

For the research, I adopted an interpretivist approach. Interpretivists look at interactions and interpret them to obtain the meaning of social life (Abbott, 2004). Measurement is not part of interpretivism, but rather the meaning of social life is the focus of this philosophy.

My work starts in chapter 2 with the discussion of security paradigms across Europe, to understand the perception of how security should be achieved, its processes organized, and key actors included.

The European practice of Security Studies is highly discussed by the academic community as "schools" have developed in recent years. These researchers have drifted apart from sectorial manifestations of International Relations (IR) theories becoming an independent field. The discipline has always been led by US research, this "sudden fertility of European soil" came as a surprise (Wæver, 2004). The debate within, among and across the "schools" is lively and it is almost entirely a European game.

European Schools present different point of views about the security discourse and the referent objects. While claiming that human networks' security is the goal, the scholars take different paths in getting to security. Therefore, an inter-scholar debate arises from this dissemblance in views. The most intense exchange in views has seen the Copenhagen School respond to the Welsh School and vice versa. The Paris School did not take a stand, as it has idiosyncrasies that set it aside from the debate and take under the lens agencies and agents.

Then, I considered realism, which is the predominant school of thought in the United States. The school has a long tradition and it has its roots in many political thinkers of the past (Thucydides, Thomas Hobbes and Niccolò Machiavelli). For Haslam (2002), realism is "a spectrum of ideas [...] rather than as a fixed point of focus with sharp definition". Definitions of realism vary considerably in their details but reveal a striking family resemblance (Reus-Smit & Snidal, 2008). Current debates concentrate over defensive and offensive realism. These branches attracted scholars as potential shapers of US foreign security policy.

The insights gained from the exploration reveal that although European Schools differ in views from their overseas counterparts, they fail to effectively address the challenges deriving from a huge technological advancement like the creation of a cyberspace. Some attempted to keep those Schools up to date, but the academic community seems to be puzzled about definitions and mechanisms to securitize the cyberspace and national interests.

Hence, a proposal to define and foster the shift of the security paradigm. I argue that cyber security studies need to become a field of study, where interdisciplinary work is done to guarantee clarity when confronting issues that involve actions in the cyberspace, but also reflect on International Relations dynamics.

C**yber safety** and **cyber security**, which will be defined below, are the terms used to frame the goal of policy discourses in Security Studies. This, in accordance with Hansen & Nissenbaum (2009) that there is a distinction between individuals and collectivities when analyzing security, especially in the cyberspace. Mayer, de Scalzi, Martino, & Chiarugi (2013) claim that "Without a shared definition of terms such as cyberspace, cyber power, cybersecurity, etc. it is difficult to dig beneath the surface, to grasp the deeper logic that

governs the operation of cyberspace, and to explain the growing importance that cyberspace is acquiring in contemporary politics."

Cyber safety is a concept resulting from technical computer security. It is the protection of individuals or firms from direct threats to the data stored on their devices or networks via private solutions. Anderson (2003) maintained that computer security is driven more by the costumer's will than by protection against objective threats. This field is then a market-driven process mostly influenced by speech acts and marketing. This acquires political importance when seen in the context of collective referent objects like " "the state", "society", "the nation", "economy" " (Hansen & Nissenbaum, 2009).

Drawing from Nissenbaum's (2005) definition, **cyber security** can be defined as the preservation of systems operating the cyberspace, be they hardware (critical infrastructures, machines, facilities, ...) or software (systems, applications, data, ...), carried out by the State in pursuit of national interests, or the protection of its citizens (Banerjee et al., 2012). The State is enabled to guarantee cyber security through co-responsibility with the private sector (Hansen & Nissenbaum, 2009, p. 1162). In a sense, we could see the State as the gate-keeper of the national cyberspace. Hence, the State is the ultimate responsible for the defense of national interests and the protection of its citizens from external and internal threats (Krasner, 1978; Morgenthau, 1951). This principle was first invoked by the Italian thinker Niccolò Machiavelli (1532) in the book "Il Principe" (The Prince).

To provide a spatial definition of the context in which actors operate, **cyberspace** is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (Kuehl, 2009). It is characterized by the **multi-**

level interaction of actors which own nodes of the network or parts of it through legal means. Or, they can get a hold of them maliciously (see, for example, Angrishi, 2017; Farwell & Rohozinski, 2011). "The economic and social systems of advanced countries are strongly dependent on cyberspace" (AA.VV., 2016). The interaction is multi-level since there are hardly boundaries (Hundley & Anderson, 1995) for the flow of data and actors exchange them in any direction. There is also the need to study the impact of autonomous systems like artificial intelligence (AI) in this interaction.

Besides, there is no central authority regulating limits of exchange. The absence of global governance resembles the realist assumption of **anarchy**. The unfortunate point is that cyber power (Kuehl, 2009) cannot be measured as the development of technologies is registering an impressive growth and network vulnerabilities are discovered every day during this decade. A viable option, as proposed by Hansen & Nissenbaum (2009), is interdisciplinary work.

The **national cyberspace** is a subset of the cyberspace, but its definition encompasses the actors operating within national borders and it is useful for the scope of cyber security. Actors are the central element of cyber security as they operate and influence each other. Those who are comprised within the national cyberspace are: the State, through its Agencies and territorial articulations; firms based within the internationally recognized national borders, not including firms owned by a majority share of foreign investors; private citizens. These actors can aggregate within or across each category.

The achievement of cyber security for national cyberspace actors in the international cyberspace is an important matter. Therefore, there is the need to evaluate legislative steps to be taken to facilitate the sharing of information about vulnerabilities and during emergencies.

Legislative actions have been taken to ensure cyber security in Europe and in Italy in the last two years. The NIS directive, discussed in chapter 3, represents a milestone in the EU cyber security discourse, changing the Union regulatory scenario and affecting industries. It introduced a minimum harmonization scheme, that is bound to become the backbone of the cyber security strategy in Europe. Nonetheless, there is the risk of legal fragmentation among states, creating harmful spillover for European industries. Also, the tracking of the impact of the NIS will become very difficult. There is the need to work on trust between firms and competent authorities with the aim to encourage cyberattacks reports.

The exclusion of small and medium enterprises is a gap to be filled in the European legislation, because of the role they have in the supply chain of big companies and the use they make of networks.

The Italian Decree for cyber security, recently approved and published in April 2017, creates a simple, yet effective, institutional architecture replacing the 2013 Monti Decree. Cyber security acquired a pivotal strategic role for Italy, considering the increasing complexity of threats. The national Cyber Security Unit has been staffed under the *Dipartimento di informazione per la Sicurezza,* making the intelligence community leader of the decision-making process. The Decree aims at facilitating the defense of critical infrastructures through a coordinated and prompt response involving public and private actors.

However, while new laws are passed, innovative technologies are developed at a faster pace. This is the case of the blockchain, the underlying mechanism of the more famous Bitcoin protocol. In chapter 4, the innovative approach to security and data exchange that this technology brings was discussed. It is a complex technology, but it is appealing for investors. Blockchain is the underlying mechanism for exchanges and it is perhaps the most

important piece of information described in the document. It is a sophisticated, distributed online ledger that has the potential, according to Goldman Sachs, to "change 'everything'".

Most of the times the term blockchain is used to mean different concepts and products. People use it to name the Bitcoin blockchain, to talk about one of the more than 500 cryptocurrencies used around the globe, or to talk about smart contracts. However, the blockchain is not just a vector for digital transactions. Its full potential is still being investigated and it has already attracted billions in funding. It is revolutionizing not only the way many industries work, but most of all their mindset. Even the U.S. Defence Advanced Research Projects Agency (DARPA) is investigating blockchain technology to "create an un-hackable messaging system."

The complexity of this technology and its innovative approach is particularly appealing, but it also creates some concerns as it disrupts many of the pre-blockchain era clichés. The assumption of the chapter is that the cyberspace is flawed and, thus, insecure. It explained the features of the technology, as well as its strengths and weaknesses in order to assess the role it could have in stepping up the cyber security challenge.

A section was also devoted to assessing the changes that blockchain could bring in terms of approach to security. Reconsidering the framework set out in §2.4 for cyber security, the introduction of blockchain systems in the picture may disrupt the cyberspace environment, eliminating the need for a trusted party as the middleman (Boucher et al., 2017; Wright & De Filippi, 2015). The central authority is not needed either, as the blockchain relies on protocols and the power of the group, in a sense empowering democracy and the diffusion of decentralized participation. The trend has also been underlined in the report "Global trends 2030: Alternative Worlds" by the US National Intelligence Council as being one of the megatrends for the next 15 years.

The State assumes a defensive stance, but a minimal role in the system. The infrastructure is a relevant part of the blockchain system and the State should guarantee the smooth execution of the code, i.e. no zero-days bugs facilitating attackers. The system/s is/are then self-protecting from attacks (data-tampering, data theft, other attacks on the software side) and frauds are easily spotted. Furthermore, blockchain facilitates the monitoring of the activities within the system and the spotting of anomalies.

Finally, chapter 5 presented the reader with seven non-financial applications of the blockchain to illustrate the way blockchain can be used to increase security. The amount of private investments on this technology is growing exponentially year after year. The seven cases were: anti-whistleblower systems, BEV systems, smart contracts, digital identity, supply chain applications, IoT, and applications in national defense. All these applications present risks for adoption relating to distinct factors, both technological and of human nature. A mismanaged transition to blockchain-based products could be misunderstood by users and the technology could be put aside for more comprehensible and "tangible" technologies. However, scarce information on these risks prevented the author from further elaborating on them.

The evidence from non-financial applications hints at the benefits arising from decentralization and a progressive reduction of the role of the state in providing security. In any case, the human factor is still relevant, as any error in programming a smart contract or in BEV systems would cause irreversible damage. Hence, there is probably the need to educate people to the cyber security and cyber safety culture.

At the Defense level, the blockchain is not only good for cyber security, it serves also as a deterrence by denial mechanism. Indeed, deterrence is the most discussed issue for cyber security in military environments. In this sense, we cannot compare cyber weapons and

cyber threats to any other historical threat. For example, any State could respond to nuclear threat by nuclear deterrence, thus building up an arsenal of nuclear weapons to discourage any opponent from attacking. Cyber weapons can be easily crafted to respond to the needs of the attacker, based on the profile of the target. There are no standard countermeasures to be adopted, but blockchain could be the solution to implement deterrence by denial.

I added an appendix with policy recommendations for the Italian government to advocate for early research and development of blockchain solutions for cyber security in Public Administration and the Defense field. The first recommendation is to partner with academic research centres to raise awareness on the potential of the blockchain and to prepare for the future of data-fighting in Defense. The second is to explore common grounds for the development of partnerships with the private sector, since both the State and companies face common challenges in the cyberspace. Further cooperation is needed to strengthen the Italian System (*Sistema Paese)*.

Many challenges arise from this document that deserve future study. The most important is to assess the risks and weaknesses of blockchain to find solutions that mitigate them. The tradeoffs between technological advancement and the willingness of a population to use such services is not to be underestimated, hence a usability study would be beneficial. Careful evaluation is needed to evaluate the illegal or immoral uses it may facilitate, especially for pedo-pornography and terrorism purposes. There is also the need to integrate research in Security Studies (or, better, Cyber Security Studies) with the implications of a fully decentralized system.

Just like the Internet or the smartphone, the blockchain technology is a truly innovative technology. It deserves the same level of attention, if not more, by states of that private investors are putting into it.