Cybersecurity in Italy Governance, Policies and Ecosystem

Cyber Security in Italy

Governance, Policies and Ecosystem

Luigi Martino

To my wife *Rugiada*

"We do raise to high degrees of knowledge
whomever We will - but above everyone
who is endowed with knowledge there is
One who knows all"

Acknowledgments

I am profoundly grateful to several individuals whose invaluable contributions have shaped the essence of this book. Firstly, I extend my heartfelt gratitude to Umberto Gori, Giampiero Giacomello, Francesco Moro, Giorgio Scichilone, Madeline Carr, Massimo Mercati, Marco Mayer, and Samuele Foni, whose dedication to engaging in insightful conversations have enriched the depth of my understanding. Michele Colajanni's unwavering belief in the significance of this book served as a constant source of motivation, and I am profoundly grateful for his insistence on publishing it. Ernesto Damiani deserves special mention for his invaluable support and pragmatic advice, which not only enhanced the content but also contributed directly to the enhancement of the Italian cyber security. A sincere appreciation to the CINI and The Italian Cyber Security Lab for the active contribution to the Italian ecosystem. I would like to thank all the associates of the Center for Cyber Security and International Relations Studies, whose direct and indirect contributions have been crucial in shaping the contents of this book. A special mention goes to Valentina Luna Covella for her meticulous assistance in processing the figures and tables. Nadeen Gamal's unwavering support, editing prowess, and invaluable assistance have been indispensable throughout this journey. Additional thanks to the people involved in the Italian cyber security environment, whose daily efforts make the country a frontrunner in this sector. Several individuals have contributed to this book with their time and inputs, including 35 interviewees, and all of them have chosen to maintain their anonymity not out of fear for their safety but due to their typical preference to work behind the scenes. This approach is committed to contributing to the success of the country in a systemic way because, as one of my mentors once said, "if we want to receive the applause, we have to work at the circus". Last but not least, special thanks to my family, starting with my beloved wife for her patience, and to my extended family. This book represents the response to those who advocate for "using knowledge for good".

Table of contents

List of Figures

List of Graphs

List of Tables

Foreword

I first met Luigi Martino in 2018 when he came, as a visiting PhD student, to spend time with our team at University College London. Luigi was supervised by Giampiero Giacomello, an academic I greatly admired who had examined my own PhD at the Australian National University. Having Luigi spend time in our team was a concrete way to continue to build links within that intellectual community of scholars working at the intersection of emerging digital technologies and international relations. Luigi would later go on to head the Center for Cyber Security and International Relations Studies at Firenze which many of us have now visited and spent time at.

Luigi's participation in the diplomacy of global cybersecurity has provided him with a special perspective that views the national interest and multilateral practice as interdependent. We cannot understand discourse on the state of global affairs and cybersecurity without deep engagement with state level approaches to the legal, regulatory, governance and policy issues. Ultimately, cybersecurity has such profound and interconnected economic, social, political, and industrial implications that understanding domestic factors and drivers is essential to understanding the international ecosystem in which those implications play out.

Fundamentally, Luigi's work highlights that cybersecurity as it is not only a problem to be addressed but an enabler to be maximised. There are opportunity costs of not implementing cybersecurity that ripple through the ambitions and expectations of states and threaten to hold back extraordinary progress that might otherwise be open to us.

Cybersecurity is a classic 'wicked policy problem' in which initiatives that solve one problem can simultaneously create others. As Luigi's book documents, cybersecurity policy and governance are not simply a matter of 'evidence-based policy making' – this is a holistic and all-encompassing challenge that involves a multitude of actors, systems, interests, and values.

This book is an important counterweight to the dominant narrative of the past three decades that 'governments stifle innovation'. As we now recognise that market drivers alone have not, and will not, deliver cybersecurity in the manner, and on the scale, needed by society, works like this make a real contribution. The conversation must now turn to *how* governments can best ensure that cybersecurity outcomes are aligned to the broader national interest. This book carefully and

systematically details how Italy has approached the design and implementation of policy initiatives, regulations, incentives, and guidance to balance out the complex array of factors that shape, and are influenced by, cybersecurity.

The issue areas that Luigi selects for his study are an important indicator of his perspective and of how one might engage with the book. Certainly, there is a clear logic that runs through from the Introduction and his thoughts on the intersection of politics and cyberspace, right through to the Conclusion where he offers his views on the future of Italian cybersecurity governance. I read this book in this linear fashion and found that the narrative builds with each chapter to provide a really comprehensive understanding of the Italian cyberspace ecosystem. However, many of the chapters stand alone and a reader could certainly engage with the book in a non-linear, issues-driven approach. I found the historical elements of these chapters particularly compelling, as they provided a wider, socio-political context for the Italian view. But one could also focus on the regulatory chapter or the institutional chapter in a comparative case study.

The analysis of the Italian history and contemporary approach to cybersecurity governance that Luigi provides here will be an excellent resource for students, certainly. But also, for those working on similar problems in other government, private sector, and third sector settings who can learn from, compare with, and evaluate the Italian response to this epoch defining public policy challenge. Perhaps even more significantly, Luigi's work provides a clear, analytic framework for research, understanding, and comparing other state responses. This book is certain to be influential and impactful and I congratulate Luigi on his achievement and thank him for his contribution to the literature.

Madeline Carr

London, 2024

Preface

This book offers a focused perspective on the governance, policies, legal frameworks, ecosystem and national architecture implemented by Italy in the context of cyber security. Given Italy's significant geopolitical position and its status as an advanced country in the digital society, the comprehensive exploration included in this book attempts to shed light on the nuanced ways in which the nation addresses digital threats, adapts to technological advancements, and applies laws that protect and enhance the lifestyle of its citizens and organizations. For professionals working in Italy or with Italy, this detailed analysis is immediately applicable. Understanding Italy's governance structures, therefore, helps cybersecurity professionals navigate a complex and bureaucratic framework consisting of stakeholders and decision-makers, thereby improving their knowledge of the roles that require interactions with government entities or compliance with national policies and rules. This book also serves as an essential reference for those involved in policymaking or managing cybersecurity from both a public and private perspective.

However, this book is dedicated specifically to students who are interested in or want to become involved in the political aspect of cybersecurity. In this book, they will hopefully find valuable information on who does what in Italy in the context of cybersecurity. By studying the Italian approach, students can appreciate the practical implications of theoretical knowledge, such as the implementation of laws in the field, how policies are shaped in response to emerging threats, and how governance structures influence national cybersecurity strategies. Designed to promote a critical thinking approach, this book encourages students to analyze and question how and why certain decisions are made in the context of national cybersecurity. Addressing a significant gap in the existing literature, this book provides an updated and in-depth analysis of Italy's response to cybersecurity issues, setting a precedent for similar studies in other national contexts. As cybersecurity assumes a greater role in national security, the insights gleaned from Italy's experiences hold relevance not only for those within Italy studying or working in this field but also for the global community endeavoring to fortify its cybersecurity measures. Moreover, they offer valuable perspectives for individuals seeking to comprehend the strategic stance of a specific country in this field. By presenting a holistic view of the Italian cybersecurity framework, this book also aims to contribute to the dissemination of a culture of cybersecurity awareness in Italy. It highlights the significance of comprehending the Italian cybersecurity model, while also recognizing that Italy,

within the cybersecurity landscape, is a component of a broader framework encompassing its role as a Member State of the European Union and its position as a significant actor globally.

This book represents the culmination of extensive research, more than 15 years of personal experiences, and professional insights. However, it is important to note that the contents provided here are based on the author's interpretation and understanding of the subject at the time of writing. The author acknowledges the intrinsic limitations of the research and the possibility of inaccuracies or omissions in the information presented. As the author of this book, I hereby assume full responsibility for the contents provided herein. While every effort has been made to ensure the accuracy, reliability, and completeness of the information presented, I recognize that I am solely responsible for any errors, inaccuracies, or omissions that may be found.

Luigi Martino

Bologna, 2024

Chapter 1 Cyber Security: Intersecting Technology and Policy

Abstracts and Reference of the Chapters

Abstract Chapter 1

This chapter delves into the complex interplay between technological advancements and policy-making in the realm of cyber security, highlighting the evolution and challenges that have emerged in the digital era. The expansion of cyberspace has underscored the critical need for a policy-oriented approach towards cyber security. This need arises from the inherent vulnerabilities within information and communication technologies (ICT), which prioritize efficiency at the expense of security, leading to potential threats to national security and individual safety. This shift is driven by the awareness that cyber security is not merely a technical issue but a complex socio-political challenge that requires comprehensive strategies encompassing both technological solutions and policy frameworks. The chapter discusses the four converging factors in cyberspace that necessitate this integrated approach: the growing dependency on ICT, inherent technological vulnerabilities, human factors on cyber threats, and the political side of cyberspace by state and non-state actors. Further, the chapter explores the dynamics in cyberspace, examining how digital environments serve as arenas for political action, conflict, and negotiation. It also presents the introduction of a case study on Italy's cyber security strategy, illustrating the country's progression from recognizing the importance of implementing national cyber security policies.

Introduction

The expansion of cyberspace has marked a clear distinction between the time preceding and following the onset of the digital era. As in every stage of human evolution and the revolutions associated with it, the onset of the information technology revolution has sparked a gradual blending between the technological realm and the crafting of suitable policies for the cyber phenomenon. From its inception, this phenomenon has displayed social implications that stretch beyond mere technical aspects. The intersection of the technological domain and policy has been driven by the need to

address an inherent imbalance in the development of the information technology context, namely the evidence that innovations in the ICT domain tend to prioritize efficiency over security. To probe into this evidence, we can cite Weinberg's Law which states that "If builders built buildings the way programmers write programs, then the first woodpecker that came along would destroy civilization" (Chemituri, 2010, ix). This simple yet pragmatic observation is also closely related to an inherent paradox of digitization: a trade-off where increased computerization implies decreased security. Indeed, the implications arising from the expansion of technological innovations, especially in the information technology field, have shown the potential to negatively impact national security, the security of citizens, the realm of human rights, and, in other words, everything on which humans base their activities. Therefore, it was necessary to adopt a policy-oriented approach through the creation of a regulatory framework that, beyond the sector standards, aimed to govern the cyber phenomenon. In this way, starting from the late '90s and the early years of the new millennium, there was a decision to overcome the myopic barrier initially built by IT professionals but, to some extent, also fueled by the reluctance of policymakers who adopted the axiom that cyber dynamics "because exclusively of an informational nature, hence technical, and thus non-political, are the stuff of engineers or nerds" (Interview, Rome 2024).

This barrier, entirely myopic and at times ideological, has been shattered by the awareness that in the cyberspace context, four relevant factors converge to build a cybersecurity based on the intersection between policy and technology: 1) the exponential growth of dependence on ICT systems for vital functions of modern societies; 2) the inherent presence of vulnerabilities in the development of ICT technologies and the consequent cause of malfunction; 3) the human factor understood as a point of vulnerability and susceptibility to criminal activities; 4) the tendency of state and non-state actors to use ICT tools for political purposes with the risk of military escalation.

Hence, it follows the need to create a suitable security model to mitigate the risks and threats arising from cyber dynamics, which has both a technical component and a mere political component. The former is capable of addressing the "how" of securing ICT tools and the environment in which they operate from attacks or human errors, and a more political component. The latter can address the need for "how" to ensure that malicious dynamics produced in and through cyberspace can be limited, reduced, or eliminated, preserving social, national, and economic security, and identifying at the governmental level "who" is in charge of doing so.

The concept of cybersecurity is therefore to be understood in its dual scope, both as a technical practice and as a socio-political necessity, to address how policy and technology can confront the threats of the cyber world. Seen from both a technical and a political perspective, cybersecurity

includes measures and practices aimed at protecting computer systems, networks, and digital information from a wide range of threats, vulnerabilities, and attacks.

From a technical perspective, cybersecurity focuses on safeguarding the confidentiality, integrity, and availability of digital resources, information, and data. This technical perspective is accompanied by an analysis and intervention level of a political-administrative nature. From this standpoint, cybersecurity assumes broader implications as it concerns the protection of a nation's critical infrastructure, military resources, economic interests, and the general well-being of its citizens. In summary, cybersecurity should be understood as a dynamic approach oriented towards the management of technological processes and inclusive of policies aimed at preventing, countering, and mitigating the negative effects of events produced in and through cyberspace, including those with the aim of compromising national security. This process must be flexible enough to accommodate technological progress and evolving threats, while considering the capabilities of malicious actors and the multifaceted nature of cyber challenges. It encompasses not only safeguarding digital assets but also protecting national interests, security, and the welfare of a nation and its citizens in an interconnected and digitally reliant world.

1.1 Implications of Political Dynamics in Cyberspace

Cyberspace has simultaneously become the content, container, and medium for social, economic, political, military, symbolic, and technological activities in contemporary times. From an environmental viewpoint, cyberspace possesses peculiar characteristics such as "placelessness," ubiquity, and anonymity (Gray, 2013, 15), but these features do not exempt it from being included in the classic conceptual framework of politics. Similar to other environments where human activities unfold, cyberspace is also affected by conflicts, negotiations, and other political mechanisms (Choucri, 2012, Valeriano and Mens, 2015). While literature defines cyberspace as an artificial environment, in practical terms, its configuration is based on a hybrid interaction between geographic, physical, logical-virtual, social, and environmental components. This combination of physical and virtual elements implies that cyberspace is understood as a resource and an arena for political action in the 21st century. For instance, the physical layer of cyberspace (commonly understood as the combination of hardware and infrastructure such as terrestrial and submarine cables, satellites, antennas, routers, computers, servers, data centers, etc.) must be connected with the geographical dimension- i.e. the territory where the physical components are materially installed. Consequently, there is a political implication arising from the interaction between those governing the territory and

expressing their jurisdiction and those who own or manage the technological infrastructure installed in that specific territory.

However, the virtual feature of cyberspace contributes to challenging certain axioms that were previously taken for granted and immutable in the context of politics before the digital era. Among these implications, it is worth mentioning the erosion of the role of the nation-state in relation to the monopoly of violence and information, the speed of action execution, the low barrier of access to technology, and the implications of anonymity.

Focusing on the first implication, the advent of cyberspace has marked a revision of the concept of information sovereignty and the monopoly of internal and external violence of nation-states. In particular, the concepts of the monopoly of violence and information, classically understood as fundamental elements of the political power of state actors and government bureaucracies, are now shared and partly held by non-state actors who possess greater capabilities in terms of technological, human, and economic resources compared to states. Since these non-state actors control a share of essential resources for the well-being of contemporary societies, they also have the ability to impose rules aimed at protecting their own interests, which in some cases conflict with those of states.

A practical example of this situation is the role of non-state actors that own social platforms, where communication and social interaction are expressed today. The rules of terms and conditions for accessing, sharing content, managing data, and interacting on these platforms are dictated not by governments but by providers, based on their interests. Although it may seem like an obvious and simplistic fact, the implications become evident when understanding the extent of "who" holds the power to decide "what" to share and "how" to access such information.

Another political element wielded by cyberspace is the overshadowing of the concept of "trust" in the context of international relations, due to the use of cyber capabilities to achieve political and military objectives. In cyberspace, the fundamental principles of peace and stability in the international system, such as the assurance that agreements are honored and transparency in identifying allies and adversaries (Bull, 1977), are called into question. The certainty of identifying the perpetrator of a malicious act is subject to plausible deniability (Carr, 2017).

Anonymity tends to generate two conditions that push towards a vicious circle: an increase in the perception of danger with a consequent security dilemma and a rush towards the militarization of cyberspace by state actors, and reluctance to advance binding agreements due to a lack of trust and mutual transparency regarding the real intentions of the parties. An example of such a vicious circle is evident in the context of international fora where initiatives to govern deleterious dynamics for international peace and stability from cyberspace are discussed. The presence of duplications within the United Nations, where the General Assembly has created The UN groups operating in the Field

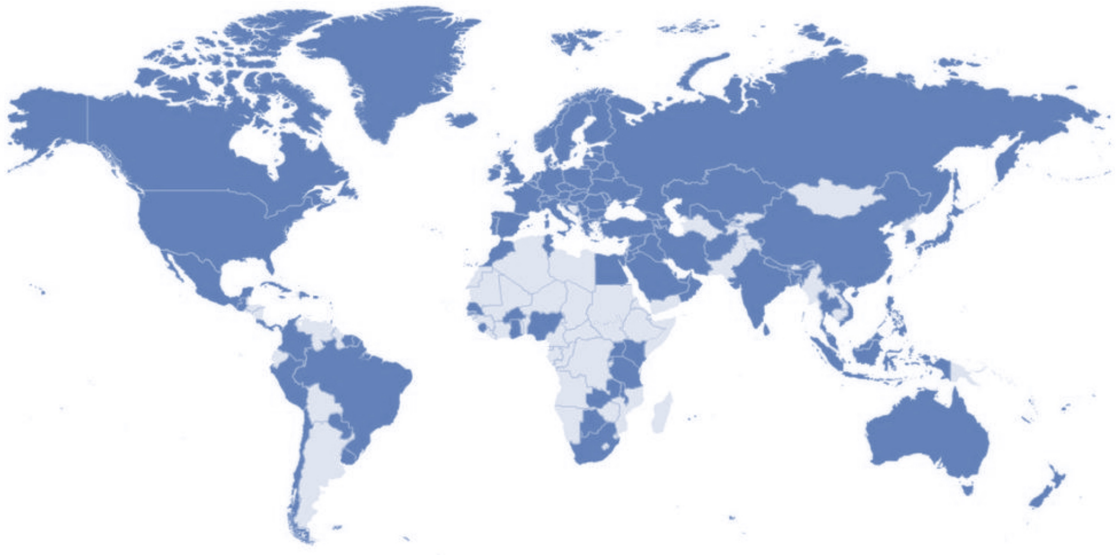
of Information and Telecommunications in the Context of International Security — the Open-Ended Working Group (OEWG) and the UN Governmental Group of Experts (GGE) to discuss the same issues, is a glaring example. To confirm this, consider that at the time this book is published, both UN groups, despite having issued vague and ambiguous proclamations recognizing the need to govern threats arising from the malicious use of ICTs, are essentially stuck on "how" and "which" part of existing international law to apply in cyberspace, being trapped by the issue of anonymity and victims of polarization due to geopolitical disputes (ASPI, 2022; Martino, 2021).

A final noteworthy political element is given by the diffusion and distribution of power in the cyber context. Empirical evidence shows that the threshold of access to capabilities in cyberspace is low compared to other dimensions where violence is manifested. In particular, as Nye (2011) rightly pointed out, with the advent of cyberspace, there has been a diffusion of power unparalleled in any era before the digital one. While in the past, there was a classic *translatio imperi* from one political entity to another, today we see the diffusion of power within the community of state actors and towards the outside, favoring non-state actors, including individuals (Nye, 2011). This implies a subversion not only in terms of who holds power but also in the very conception of power that has traditionally been used in the context of international relations and political-social relations. With the advent of cyberspace, power is no longer measurable exclusively in terms of military resources, national GDP, human resources, or the quality of leadership. Instead, alongside such categories and units of power analysis, an independent variable is introduced. This variable is characterized by the widespread capacity, facilitated by cyber tools, to achieve objectives while maximizing benefits with the least possible cost, in economic, military, and human terms. If we want to employ a doctrinal analogy commonly employed in the context of strategic studies, although the Clausewitzian approach persists in traditional military domains where the concentration of economic-military force is indispensable to achieve political objectives, the indirect approach theorized by Liddell Hart (1925) appears to hold greater relevance in the cyber context. In this approach, the greatest success is achieved by targeting the adversary's "Achilles' heel," and in the context of the digital society, this is represented by the information dimension. This should not lead to the misconception that cyberspace has rendered the role of the state and other traditional domains (land, sea, air, and space) obsolete, or that it will be the sole arena for intra- and international disputes or future warfare (Martino 2023). On the contrary, awareness should lean towards recognizing that this domain, far from being considered an exclusive realm *only for technical experts*, requires an active and fundamental role by the state and its institutional apparatus to govern the cyber phenomenon and the dynamics it produces.

1.2 Statecraft in Cyberspace: The Case of Italy

In Italy, the topic of cyber security has been addressed from an institutional and organizational perspective for about a decade starting from 2013, the year of the issuance of the decree by the President of the Council of Ministers that established the first national architecture dedicated to cybersecurity. Since the release of this government document, cyberspace security in Italy has become a fundamental prerogative for the protection of national and social well-being. This awareness has fostered the development of technological and organizational capabilities in the cyber domain which, alongside classic tools such as military, diplomatic, cultural, and economic measures, have found a consolidated position in the pursuit of national interests (Tabansky and Ben Israel, 2015). As illustrated in Figure 1, to date, most states have equipped themselves with a national cybersecurity strategy to pursue and protect their interests in the context of cyberspace.

Figure 1: The Diffusion of National Cyber Security Strategies 2024



Source: Elaborated by the Author, Luigi Martino (2024)

Similar to other nations, Italian political decision-makers have chosen (albeit, as we will later discuss, sometimes inconsistently) to establish an institutional framework and governance processes specifically aimed at managing the cyber phenomenon. Since 2013, this course of action has mostly been justified by the recognition of Italy's dual active role in the cyber domain. On the one hand, the

role of ensuring national and domestic security, protecting citizens, social well-being, and safeguarding critical infrastructure responsible for the vital functions of democratic institutions from threats and risks originating from cyberspace. On the other hand, Italy (although only from the second decade of the 2000s) has also decided to complement the risk-oriented approach with the pursuit of opportunities arising from the digital society. In particular, both the ruling class and Italian decision-makers have recognized the economic and social advantages of the ICT world, envisioning an investment plan, both economic and programmatic, in the field of research and technological development.

The dual strategy, focusing on threat prevention and seizing opportunities, largely arises from external pressures rather than choices driven by the maturity of the national political class (with a few rare exceptions that we will mention). It is driven by the necessity to keep pace with other countries considered "mature" in organizational bureaucracy, while simultaneously cultivating an ecosystem to position Italy significantly in technological development “to overcome the inferiority complex resulting from short-sighted economic policy choices and the inability of the industrial and academic sectors to understand the potential that would have resulted from the information revolution (Interview, Rome 2023). The paradigm shift was initiated in two distinct phases that led to an institutional and normative development somewhat atypical compared to other European and international cases. Indeed, the decision to equip Italy with a national architecture entirely dedicated to cyber security arises from a need induced both by the European Union and NATO, namely the priority to enhance the management, mitigation, and prevention capabilities of cyber risks in light of international events (primarily, but not only, the events in Estonia in 2007). As we will see in the chapter 3, it is worth highlighting that already from the early 2000s, Italy sought to manage cyber risks through a significant and in some cases exclusive role of homeland IT infrastructures against cyber attacks. As we have already mentioned, it is only since 2013 that Italy has decided to embark on the path of structuring a national cybersecurity governance, recognizing this matter among the prerogatives of national security and therefore the responsibility of the Prime Minister. This detail of a change in the allocation of responsibilities to the Prime Minister is an element that, as it will be illustrated later on chapter 3, will have repercussions on the peculiar Italian choice to initially entrust the entire operational management of national cybersecurity to intelligence services and then decide, in the early 2010s, to build an ad hoc agency known as the Italy's National Cybersecurity Authority protecting national interests in the field of cybersecurity.

1.3 Structure of the book

This book endeavors to critically analyze the excursus that Italy has undertaken in the context of cybersecurity from a governance and policy-making perspective implemented over the period 2013-2024. However, the analytical timeframe ranges from 2005 (when the first ministerial decree on the protection of computerized critical infrastructure was issued) to 2024 (the year of the publication of this book). A preliminary caveat must be specified: the temporal analysis represents a dynamic snapshot as both the subject matter and the national (and international) context lend themselves to daily dynamism and are therefore impossible to fix in a precise static timeframe. This book serves a dual purpose: a) contributing to filling an analytical gap useful for reconstructing the regulatory, policy, and governance path implemented by Italy in the context of cyber security; b) clarifying the current Italian national architecture and ecosystem dedicated to the governance of cyber security. Methodologically, the analysis proposed in this book starts from the assumption that Italy's journey has not been linear and has had to face a series of obstacles, mainly due to governmental instability and inputs primarily derived from external factors (such as regulations and strategic choices of both the EU and NATO) rather than internal political awareness. The chapter 2 reconstructs the Italian cyber ecosystem in order to provide a useful analysis to understand the various roles played by different actors in the Italian national system, from political, economic, and research perspectives. Chapters 3 and 4 will focus on a historical reconstruction of the policies implemented by Italy in the context of cyber security, aiming to understand the temporal trajectory that led to the establishment of the current national architecture – from where Italy started to where it stands today in this context. The third part is dedicated to the most innovative and debated legislation implemented by Italy in this context, namely the establishment of the national cyber security perimeter. Chapter 5 seeks to illustrate the strengths and weaknesses of this legislation, beyond just the legal aspects, with a primary focus on the practical effects of this initiative. The final part analyzes the organizational and operational aspects of the National Cybersecurity Agency, inaugurated in 2021, which also led to the issuance of the national cyber security strategy. In chapter 6, initiatives implemented by the agency, as well as the limits and opportunities of the new national governance system in the field of cyber security, are examined along with the strategic objectives outlined in the national strategy. Finally, chapter 7 will summarize the main outcomes of the book and the concluding remarks.

References Chapter 1

- ASPI (2022) Australian Strategic Policy Institute, UN norms of responsible state behaviour in cyberspace. Guidance on implementation for Member States of ASEAN. Available Online URL https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace
- Bull, H. (1977). The Anarchical Society. London: Macmillan.
- Carr, Madeline. (2015). "Power Plays in Global Internet Governance." Millennium: Journal of International Studies, 43(2), 640-659.
- Carr, Madeline. (2017). "Cyberspace and International Order." DOI: 10.1093/oso/9780198779605.003.0010. Pages 162–178.
- Choucri, Nazli. (2012). Cyberpolitics in International Relations. The MIT Press.
- Clarke, Richard A., and Knake, Robert K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, p. 32.
- D'Angelo, Gabriele; Giacomello, Giampiero. (2023). Cybersicurezza. Che cos'è e come funziona. Bologna: Il Mulino.
- Dunn-Cavelty, Miriam. (2008). Cyber-security and Threat Politics: US Efforts to Secure the Information Age. New York, NY: Routledge.
- Eriksson, Johan; Giacomello, Giampiero. (2006). "The Information Revolution, Security and International Relations: (IR)relevant Theory?" International Political Science Review, 27, pp. 221 – 244.
- Giacomello, G.; Verbeek, B. (2023). "Foreign Policy of Middle Powers." In: The Oxford Handbook of Foreign Policy Analysis. Oxford: Oxford University Press.
- Gray, Colin S. (2013). Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling. Carlisle, PA: US Army War College Press. Available: https://press.armywarcollege.edu/monographs/529
- Kello, Lucas. (2013). "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security, 38(2), 7-40.
- Kuehl, Daniel T. (2009). "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, & Larry K. Wentz (Eds.), Cyberpower and National Security. Washington, D.C.: National Defense University Press.
- Libicki, Martin C. (2007). Conquest in Cyberspace. Cambridge, UK: Cambridge University Press.
- Maness, Ryan C., and Valeriano, Brandon. (2016). "The Impact of Cyber Conflict on International Interactions." Armed Forces & Society, 42(2), 301–23. https://www.jstor.org/stable/48670248.
- Martino, Luigi; De Zan, Tommaso; Giacomello, Giampiero. (2021). Italy's Cyber Security Architecture and Critical Infrastructure. In Romaniuk, S.N., & Manjikian, M. (Eds.), Routledge Companion to Global Cyber-Security Strategy. Routledge. ISBN: 9780429399718.
- Martino, Luigi. (2023). "La guerra nel XXI secolo: la dimensione cyber e il conflitto russo-ucraino." In La guerra tiepida: Il conflitto ucraino e il futuro dei rapporti tra Russia e Occidente, edited by Andrea Manciulli & Enrico Casini. Koinè.
- Martino, Luigi. (2021). "Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza." IAI Papers, no. 21/13. Published by Istituto Affari Internazionali. Available online: [URL not provided].
- Martino, Luigi. (2019). "Confidence Building Measures (C.B.M.) in campo cyber: Attuali limiti e possibile contributo nazionale alla loro condivisione e applicazione." Published by Centro Alti Studi per la Difesa, Centro Militare di Studi Strategici.

- Martino, Luigi. (2018). "La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale." In Cyberspazio. La quinta dimensione delle interazioni umane, Società Editrice il Mulino, pp. 61-76.
- Martino, Luigi. (2018). "Cyber diplomacy e relazioni internazionali: le iniziative diplomatiche per mitigare il rischio di escalation militare nel cyberspazio." In Il ruolo dell'Italia nella sicurezza cibernetica. Minacce, sfide e opportunità, edited by Valerio De Luca, Giulio Terzi di Sant'Agata & Francesca Voce.
- Moore. (1993). Assessing the Impacts of Changes in the Information Technology R&D Ecosystem: Retaining Leadership in an Increasingly Global Environment. Washington, DC: The National Academies Press. National Academies of Sciences, Engineering, and Medicine. 2009.
- Nye, Joseph. (2011). The Future of Power in the 21st Century. Public Affairs Press.
- Perrow, C. (2011) [1984]. Normal Accidents: Living with High Risk Technologies. Princeton: Princeton University Press.
- Rid, Thomas. (2011). Cyber War Will Not Take Place. London, UK: Hurst & Company.
- Tabansky, Lior; Ben Israel, Isaac. (2015). Cybersecurity in Israel. Springer International Publishing.
- Valeriano, Brandon; Maness, Ryan C. (2014). "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011." Journal of Peace Research, 51(3), 347-360.