Luigi Martino

Cybersecurity in Italy
Governance, Policies and Ecosystem

Springer

SpringerBriefs in Cybersecurity

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money – all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The *SpringerBriefs in Cybersecurity* series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

Luigi Martino

Cybersecurity in Italy

Governance, Policies and Ecosystem

Springer

Luigi Martino
University of Bologna
Bologna, Italy

Khalifa University of Science and Technology
Abu Dhabi, UAE

If disposing of this product, please recycle the paper.

"To my beloved 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"

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 also an enabler to be maximized. 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 recognize 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.

London, UK
2024   Madeline Carr

Preface

This book offers a focused perspective on the governance, policies, legal frameworks, ecosystem, and national architecture implemented by Italy in the context of cybersecurity. Given Italy's significant geopolitical position, and its status as a mature 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 well-being 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 institutional (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, and based on empirical validation of data with 35 semi-structured interviews, 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,

the book offers 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 in different international (i.e. UN; G20 and G7 etc.) and regional (i.e. OSCE, etc.) fora.

This book represents the culmination of extensive research, more than 15 years of personal experiences, academic research and professional insights. However, it is important to note that the contents provided here are based on the author's interpretation and the content represents a snapshot of the subject at the time of writing. 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.

Bologna, Italy   Luigi Martino
June, 2024