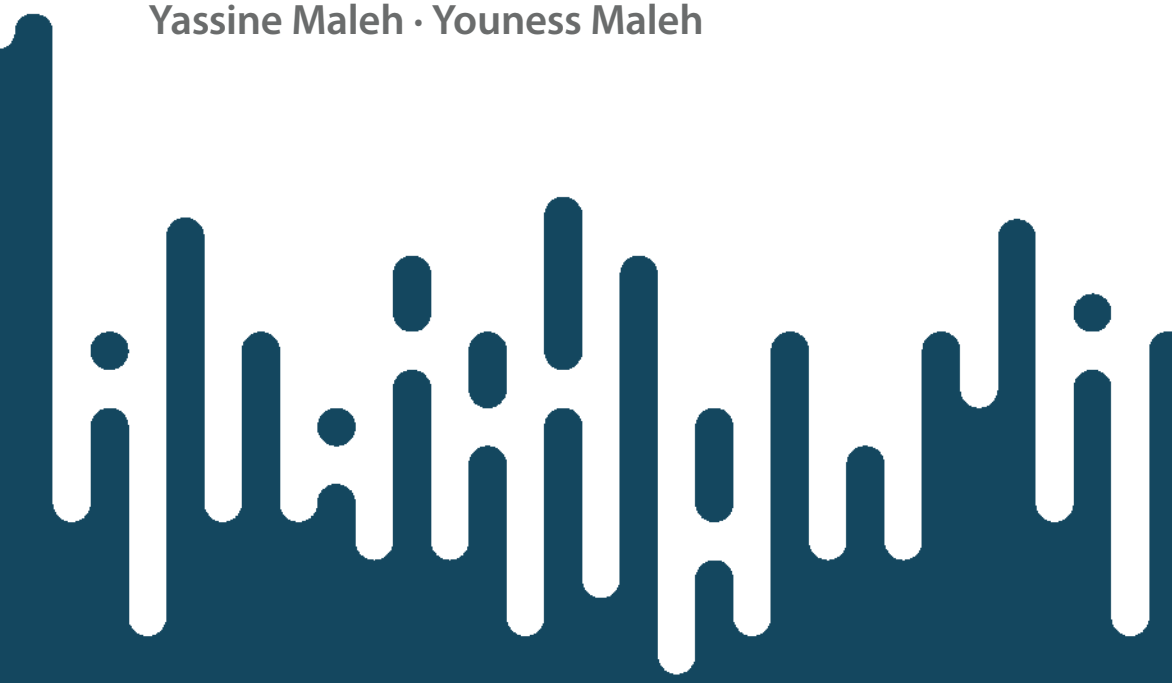
SpringerBriefs in Cybersecurity

Yassine Maleh · Youness Maleh



Cybersecurity in Morocco

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.

Yassine Maleh • Youness Maleh

Cybersecurity in Morocco

Springer

Yassine Maleh
University Sultan Moulay Slimane
Beni Mellal, Morocco

Youness Maleh
University Moulay Ismail
Meknes, Morocco

ISSN 2193-973X ISSN 2193-9748 (electronic)
SpringerBriefs in Cybersecurity
ISBN 978-3-031-18477-2 ISBN 978-3-031-18475-8 (eBook)
https://doi.org/10.1007/978-3-031-18475-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The outlook for risks and conflicts in cyberspace of national interest in the years 2020 and 2021 is, as in almost all areas, marked by the COVID-19 pandemic. This does not mean that many aspects that characterize cybersecurity during this period do not originate from other factors. Based on this starting point, we intend to offer a global analysis of the results of this report, considering not only the current context but also factors that are exogenous to it. A joint and delimited perspective of the main themes allows for a vision that is deemed more coherent on the subject, namely highlighting the most relevant threats, the risk perception that has developed, and the trends that are required, as in the case of the COVID-19 pandemic.

It should be noted that the term "cybersecurity" emerged and found its application in the world's major developed countries in the late 1990s and early 2000s. Subsequently, it found its recognition and application in the international communication environment during the development and signing of some international standards, declarations, appeals, and other documents in the field of international security. Major foreign countries have seen it as a substantial new essence in the national and international security field, have given it importance, and have developed and shaped its disclosure and conceptual apparatus to ensure clear understanding and communication. In this light, recognizing the paramount importance of national security, most major foreign countries have developed and promulgated several fundamental doctrinal documents on national security, such as Cybersecurity Concept, Strategy, and Policy, and others more specific. In this context, Morocco has become more attractive to foreign investment in Africa and the MENA region. All of these factors make Morocco an attractive location for cyber-attacks. Securing and controlling the information conveyed by information systems is becoming an increasingly pressing issue, given the growing number of cyber-attacks worldwide. How can we explain this increase in cybercrime? What are the challenges of cybersecurity in Morocco? What are Morocco's vision and strategy for cyber security and cyber defense? And finally, what is Morocco's vision for cyber resilience and cyber sovereignty?

This Springer brief has a discussion character and aims to draw attention to the need for effective implementation and development of cybersecurity in Morocco to

ensure national security in the context of the current and developing information confrontation in the international community. However, it cannot promise to provide an in-depth examination. The issue of cybersecurity is simply too wide-ranging for our purposes. This acknowledgment is meant to encourage more detailed research into the broader topics covered in this brief to better inform current approaches to national cybersecurity performance evaluation.

This SpringerBrief contains eight chapters, which are intended to be a relevant reference for diplomats, executives, CISOs, cybersecurity professionals, engineers, and researchers interested in exploring and understanding Morocco and its efforts in implementing its national cybersecurity strategy.

Beni Mellal, Morocco Yassine Maleh
Meknes, Morocco Youness Maleh

Acknowledgment

The authors would like to acknowledge the support of the African Center for Information Technology and Cybersecurity ARCIC.

University Sultan Moulay Slimane — Yassine Maleh
Beni Mellal, Morocco
University Moulay Ismail — Youness Maleh
Meknes, Morocco

Contents