Cyber Sovereignty in Morocco

Chapter · November 2022

DOI: 10.1007/978-3-031-18475-8_7

2 authors, including:

Maleh Yassine
Université Sultan Moulay Slimane
291 PUBLICATIONS **1,556** CITATIONS

SEE PROFILE

Chapter 7
Cyber Sovereignty in Morocco

7.1 The Concept of Digital Sovereignty

To unpack the concept of data sovereignty or digital sovereignty, one must first recall the historical importance and powerful hold on the political discourse of the concept of sovereignty itself. It emerged progressively, especially in Europe, through centuries of struggles between power regimes and intense philosophical and political debates, as evidenced by the writings of Jean Bodin, Grotius, Thomas Hobbes, John Locke, Montesquieu, and Rousseau (Bodin & Jean, 1992; Putterman, 2010).

Sovereignty is a term that can be applied to any situation where a person or organization can act autonomously and without interference from outside forces. The traditional concept of sovereignty was heavily inspired by Jean Bodin (Bodin & Jean, 1992), who believed that the ultimate decision-making power and exclusive right to use force in a state should be held by the ruler or sovereign. Rousseau (Putterman, 2010), a French philosopher of the Enlightenment, introduced a dramatic shift in the notion of sovereignty, from the rule of the ruler to that of the people, in his writings. Modern democracies gave rise to the concept that the people, in his view, had the ultimate authority in the state, but that they may delegate its execution to a sovereign or elected government (Linkov & Kott, 2019).

Similarly, the current concept of sovereignty, which refers to a legal entity's ability to make its own decisions, relies heavily on the term's legal interpretation. As a result, it is distinct from the external definition of self-sufficiency and/or full isolation, defined by autonomy and independence. Sovereignty in constitutional and international law refers to a state's internal self-organization and independence from other states (external sovereignty) (internal sovereignty). States are sovereign if they can operate mainly autonomously at all three levels of government, economics, and society, with other states. This idea of sovereignty is closely tied to that of territorially defined nation-states (Weil & Murugesan, 2020).

Y. Maleh, Y. Maleh, *Cybersecurity in Morocco*, SpringerBriefs in Cybersecurity,
https://doi.org/10.1007/978-3-031-18475-8_7

Sovereignty and the rule of law go hand in hand in modern democracies. A democratic state's sovereignty is based on guaranteeing that its citizens can exercise their fundamental rights. It aspires to empower all people to respect their rights and exercise their authority in accordance with those rights. The state must see that this happens, especially in light of the numerous difficulties that the digital transition brings to society.

So the term digital sovereignty is becoming increasingly frequent in the media as a result State control over their digital infrastructure and the personal data of its population is one of the many possible interpretations of the term. However, the phrase is increasingly being used in a more general sense. Global leadership is being fought over the digital technologies of today. As a result, tensions between China and the United States are rising (also known as the technical cold war). It comes down to who has the best next-generation communications, semiconductor, and AI leadership. In this context, the United States and China frequently draw on one other's sovereignty maps. According to Trump, prominent Chinese applications like TikTok and WeChat were banned because they threatened "national security, foreign policy and the economy" of the United States (Hong & Goodnight, 2020).

Before 2011, the term "data sovereignty" was virtually nonexistent in academic and popular debate. Most of the talk about "digital sovereignty" concerns national governments' abilities, notably in China, Russia, and France, to impose control over infrastructure and data generated on their own. However, when discussing sovereignty, several interpretations are highlighted (Budnitsky & Jia, 2021).

There are five types of discourses or views on the concept of "sovereignty" as it applies to the digital aspect:

- As a result of John Perry Barlow's 1996 proclamation of "cyberspace independence," which said that "cyberspace" was a new area that governments should not regulate, the term "cyberspace sovereignty" has historical importance. Milton Mueller's "People Sovereignty in Cyberspace" presents a more contemporary (and scholarly) take on the same issue. According to Mueller, multi-stakeholder engagement in Internet governance institutions like IGFs and ICANN should be the foundation for cyberspace sovereignty.
- In today's world, "state digital sovereignty" refers to a country's or nation's capabilities and attempts to manage its data and information infrastructure. Another cliché (what they term the "brand of the nation") is the discussion of digital sovereignty to develop a distinct national vision of the Internet in the United States.
- The sovereignty of the digital natives: People and nations have more power over their data, infrastructure, and fate than previously thought, similar to the preceding perspective. Indigenous sovereignty, self-determination, and revival are all emphasized in the context of the notion of "network sovereignty." Indigenous sovereignty can only be strengthened via the use of technology.
- This term alludes to social movements and activist organizations' power over their data and information through software, servers, and cryptography-based technology.

- Although this viewpoint is not widely accepted, it is important to address since it relates to our power over digital devices. As a result, social activists must use free and open-source software or encrypted communication tools to maintain their technological superiority.

7.2 The Realities of Digital Sovereignty

The international community has not agreed on whether cyberspace is part of the public domain, belongs to the territory of "physical" states, or is based on national origins, highlighting the digital sovereignty issue. According to the quarterly analysis of the current and projected growth of the global information technology sector by the International Data Corporation, global spending in the field in question will increase by 6% in 2020, reaching $5200 billion. At the current IT development stage, the digital economy's economic geography does not present the traditional North-South divide. It is led by two countries: the United States and China. For example, they account for 75% of all blockchain-related patents, 50% of global spending on the Internet of Things, and more than 75% of the global public cloud computing market. And, perhaps most strikingly, they account for 90% of the market capitalization of the world's 70 largest digital platforms. Europe's share is 4%, while Africa and Latin America account for just 1%. Seven "super platforms"—Microsoft, followed by Apple, Amazon, Google, Facebook, Tencent, and Alibaba—account for two-thirds of the total market value. Thus, in many digital technologies, the rest of the world, especially Africa and Latin America, lags far behind the United States and China. The United States, the most technologically advanced country, which in 2018 was home to 45% of the companies on the top lists of technology leaders,9 is the world's largest technology market in 2020, accounting for 32% of the total, or about $1.7 trillion in 2020. Among the regions, Western Europe continues to be a significant contributor to the IT sector, accounting for about one in five dollars spent on IT worldwide (Marta Taggart & Orlando Scott-Cowle, 2021).

The coronavirus infection (COVID-19) pandemic, which is sweeping and affecting the world in 2020, has demonstrated the critical role of the high-tech sector in ensuring the continuity of social life, business, and governance and has accelerated thinking about the need for digital sovereignty in the European Union (EU). Economic considerations reinforce this concern due to the unchecked behavior of large and growing Internet companies, notably the GAFAs. The astronomical growth of GAFA has forced the EU to reflect on its digital ecosystem to avoid a monopoly of US companies and to support innovation and Internet capabilities across Europe. The technological choices made by Apple and Google have encouraged some Member States to develop their contact tracing solutions (such as Stop Covid in France) and fueled aspirations for digital sovereignty. In this context, there is growing support for a new policy approach to strengthen Europe's strategic digital autonomy. There are growing calls in the EU for creating a European cloud and information infrastructure to strengthen European digital sovereignty and address

the fact that today the cloud and information storage market is almost exclusively dominated by non-European providers—with potentially detrimental consequences for the security and rights of European citizens. Germany and France jointly announced the Gaia-X project of the European Cloud Initiative and provided for the creation of a federated data infrastructure at the European level starting in 2020. In this context, the conclusion of a multi-annual financial framework for 2021–2027, which is currently under discussion, is crucial, as it provides for a budget of €100 billion for the Horizon Europe research program. In the long term, creating a truly sovereign e-environment will also require addressing the lack of regulatory coordination in this area. This, in turn, raises the question of rethinking the governance arrangements currently in place within the EU, both horizontally (between sectoral regulators with parallel and sometimes overlapping competencies) and vertically (between member state and EU levels of competence) (Dalton et al., 2017).

Notably, the concept of a sovereign Internet was first introduced by Fan Binxing, known as the "father of the Chinese firewall" and one of the developers of China's Internet censorship system, in a 2011 speech at the International Symposium on Information Security in Changsha. Four principles underlie the ideas of cyber sovereignty: each country should have complete control over its segment of the Internet, the state should be able to protect its segment of the Internet from outside attack, all countries should have equal rights to use resources on the Internet, and other countries should not control the root DNS servers through which the national segment of the Internet is accessed. China has established itself as a significant player in the global technology market. During the US-China trade war, the two sides have engaged in increasing competition for dominance in various areas of next-generation technologies, such as 5G networks and artificial intelligence. According to China's policy documents, one of the country's main economic goals is to achieve global leadership in various technology fields. China is preparing to release China Standards 2035, outlining plans to set global standards for future technologies. In 2017, China announced its ambition to become the world leader in artificial intelligence by 2030. The competition between the United States and China is mainly about who will control the global computing infrastructure and standards in this area.

A sovereign Internet would be based on technical means to counter threats, centralized management of telecommunication networks in the event of a threat, and a mechanism to control communication lines crossing national borders, as well as the introduction of a national domain name system (DNS), within the United Nations International Telecommunication Union (ITU).

Through this chapter, we will try to answer some questions: What does the term digital sovereignty mean? What are its most important manifestations and pillars? To what extent can we talk about digital sovereignty in Morocco?

7.3 Digital Sovereignty in the Time of COVID-19

When the COVID-19 pandemic emerged in 2020, much of the world's population moved to the Internet, accelerating the digital transformation underway for decades. As children accessing the Internet from home began to take courses remotely, many employees began to work from home. Many companies adopted digital business models to maintain operations and strengthen their reputations. Many companies have also adopted digital business models to maintain their operations and sustain certain revenue streams. At the same time, mobile apps have been developed to help "track and trace" the outbreak. Researchers have used artificial intelligence (AI) to learn more about the virus and speed the search for a vaccine. In some countries, Internet traffic increased by up to 60% shortly after the pandemic, confirming the digital acceleration caused by the pandemic (Maleh, 2021).

While these activities demonstrate the enormous potential of digital transformation, the pandemic has also highlighted the gaps that remain. While some digital divides have increased in recent years, others have not kept pace, leaving some people behind in the digital acceleration brought on by COVID. In addition, the growing use of digital solutions has increased concerns about privacy, digital security, and how to achieve digital sovereignty.

COVID-19 revealed the critical importance of technology to economic and health resilience. As a result, governments have used real-time data and disease tracking tools that determine the size, spread, and distribution of the new coronavirus (SARS-CoV-2 [COVID-19]) that emerged in 2019 to inform and influence decision- and policy-making. Coronavirus has disproportionately affected people through infections, deaths, economic losses, or changes in social interactions. While people need appropriate, timely, relevant, and quality data to guide their response to a pandemic, collecting and using such data is not without risk. Recently, concerns have been raised about data damage, group privacy, consent, racial surveillance, algorithmic targeting, and more (Weil & Murugesan, 2020).

7.4 Cyber Threats and Digital Sovereignty

Findings by Edward Snowden on the NSA widespread Internet monitoring program in 2013 indicated that technology is vulnerable to dominance by other nations in information and communications technology. It is not only about technological flaws when exposing information about another country's citizens and national security secrets. American electronic operations and technology have suffered because of Edward Snowden's revelations. As a result of the Snowden leaks, countries have rethought their approach to securing their cyber sovereignty. As it is, the phrase "cyber sovereignty" is inaccurate. State sovereignty has been compromised. However, it is vital to distinguish between concerns of strategic autonomy relating

to cyber security and cyber sovereignty as defined by international law (Pohle & Thiel, 2020).

Eighty-four of the world's 193 countries have publicly available national cybersecurity strategies, according to open-source research using the ITU Global Cybersecurity Index (2017) and the ITU National Strategy Repository (2018), and 69 countries have translated their national cybersecurity strategies into English as of December 2017. There were mentions of countries with national cybersecurity plans in several of the documents. Still, open-source searches could not locate the essential papers (e.g., Oman and Algeria) (ITU, 2022).

Only a few nations in Africa, the Middle East, and South America have a national cybersecurity strategy. Only 15 of the 69 nations with publicly available English-language national cybersecurity strategies used sovereignty-related phrases. In the Western countries, Canada, Finland, France, Hungary, Portugal, Spain, Australia, and the United Kingdom, the phrase "sovereignty" was used in over half of the strategy formulations. The remaining half comprised people from Chile, Colombia, Ghana, Japan, Nigeria, Russia, and Saudi Arabia.

The phrase "e-sovereignty" was first used by Canada. National cybersecurity policies seldom include the idea of "sovereignty," as seen by these findings. To infer that cybersecurity dominance is predominantly a Western notion, it is necessary to look at the nations that utilize the word. Since several nations in this category have implemented a national cybersecurity strategy, the Western nations are overrepresented in this group.

Sovereignty and cyber sovereignty are included in these cybersecurity measures, although they are rarely implemented. The term "rule" appears in the paper on average thrice. In Finland, Nigeria, and Portugal, the phrase "sovereignty" appeared at least three times in their plans. But France stood out by invoking the phrase "sovereignty" nine times in 2011 and five times in 2015 in its policies.

Sovereignty is a word that is rarely used in national cybersecurity policies, and even when it is used, it is infrequent and without a defined definition. Furthermore, countries do not seem to agree on what the phrase means. In cybersecurity, however, the Westphalian idea of sovereignty appears to dominate among governments. The term "sovereignty" in the plans does not appear to evolve or be impacted by Edward Snowden's revelations.

There were 55 records published prior to Edward Snowden's revelation in 2013 and 38 that were published following Snowden's disclosure, according to the study. "Sovereignty" and "E" sovereignty appear in 13 publications published before 2013 and 5 released subsequently. Although there is no evident distinction between texts written before 2013 and those written subsequently, the notion of sovereignty is used differently. Only after 2013 has cyberspace security become a more prominent theme in national security agendas.

To achieve digital sovereignty, we must ensure that our critical sectors, processes, and data are cyber-resilient. Growing cyber threats threaten our national security by jeopardizing key infrastructure, infiltrating social media to affect the democratic process, extorting our personal information, and stealing our intellectual property. Internal legitimacy of the state is undermined when key sections of our

government and the military cannot maintain control over essential procedures and data.

Digital sovereignty and the CIA (confidentiality, integrity, and availability) principles of information security are inseparably intertwined regarding cyber dangers. The CIA stands for confidentiality, integrity, and availability. There must be safeguards for autonomy not just at the level of a specific system in a certain sector (such as the sanction chain's ICT system), but also in the larger economic, social, and democratic contexts.

As an example of how the specialized government regime of ICT may erode sovereignty, consider the espionage and cyberattacks on the automation and industrial control systems of our essential infrastructure that take place when information from government officials is stolen (secrecy) (availability). These schemes are targeted explicitly by foreign state actors to achieve their geopolitical objectives.

Digital sovereignty can be directly translated into ICT system needs in certain circumstances. Digital sovereignty must also be seen in terms of the state's interest in economic growth, social cohesion, and democracy and the prohibition of foreign forces from accessing sensitive information. Consider, for example, the degree of control over the underlying economic ecosystems, the quality of democratic decision-making, the faith in the rule of law, and information and data.

7.5 The Possibilities of Digital Sovereignty in Morocco

Cyber resilience is a new concept that has been added to the panorama of information systems security concepts, but it does not change security fundamentals. It just emphasizes specific aspects inherent to business continuity.

Regarding strategy and regulation, these two components have contributed in one way or another to strengthening one or more of the previously mentioned pillars of resilience (i.e., preparation, identification, protection, detection, resolution, and recovery), as shown in Fig. 7.1.

As an illustration, in the national cybersecurity strategy adopted by Morocco in 2012, actions related to the census, identification and classification of information systems, and risk assessment directly impact the "identification" pillar. The implementation of a secure transmission network of the state, the involvement of operators and Internet service providers, the securing of websites and online public services, and, finally, the actions related to the strengthening of the foundations of security such as training and awareness have a direct impact on the pillar of "protection". The speaker thus made the correspondence between the programs and actions of the national strategy and the rest of the pillars of resilience. Regarding the contribution of regulation, correspondence was made between developing resilience and implementing three regulatory mechanisms. First, the National Directive on Information Systems Security (DNSSI) includes 104 security rules divided into 11 chapters inspired by the ISO 27002:2005 standard and represents the common and minimum base that all public departments are called upon to implement. He stressed

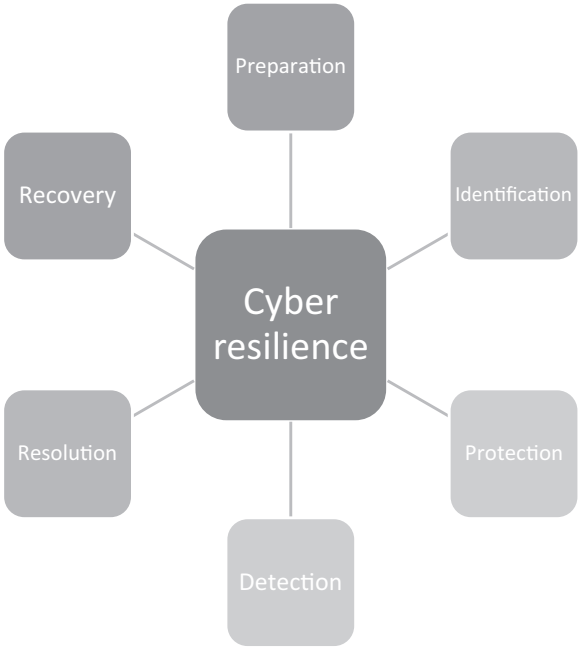

Fig. 7.1 Key pillars of cyber resilience

that entire chapters of this directive are devoted to incident management and business continuity, which represents a direct link to resilience. Secondly, the mechanism for protecting sensitive information systems of critical infrastructures was put in place through a decree in March 2016. On the one hand, this system has allowed the DGSSI to extend its scope of competence to private entities in sectors of vital importance (Chambre Française de Commerce et d'Industrie du Maroc, 2021; DGSSI, 2013). On the other hand, it has allowed the DGSSI to implement mandatory measures such as the identification of sensitive information systems, the implementation of supervision and detection means, the declaration and treatment of security incidents, and the implementation of continuity and activity recovery plans, as well as the performance of security audits periodically conducted by the DGSSI or by service providers approved by the DGSSI.

In this sense, the DGSSI has deployed some accompanying measures. These include the directive that sets out the security rules and the procedures for declaring sensitive systems, technical security guides and guidelines, and the system for approving audit providers. The latter will enable the creation of an ecosystem of expertise in evaluation and auditing at the national level and the designation of service providers who can carry out this activity according to the standards and good practices in force. The third mechanism that has been put in place by the DGSSI is cyber crisis management. This is an interministerial mechanism whose objective is to ensure better reactivity, coordinate action, and avoid improvisation. This system has been set up via a two-level organization: a decision-making level that approves the activation of the system, that invites the departments concerned to be

represented according to the situation, that can call on external expertise, and that also ensures communication with the public and an operational level that is in charge of the operational and technical management of the crisis from identifying the triggers to the closure.

In this sense, the special commission's report on the development model recommends understanding digital as a means of continuous evolution. In line with global transformations, digital infrastructure and digital technology adoption capabilities are important determinants of a country's competitiveness, given the increasing importance of new technologies in all sectors of the economy, which requires reliable and quality digital services. Strengthening the competitiveness of the Moroccan economy requires a proactive approach to generalizing access to high-speed Internet in all regions of the kingdom and to very high-speed Internet in areas of intense economic activity. The rehabilitation of the digital infrastructure should be accompanied by a rapid process of improving the capacity to use new technologies, as a special capacity, to intensify the internal offers of digital configuration and the standard job offer.

Under digital sovereignty, the special committee's report on the development model recommends completing the legal framework to ensure users' digital confidence and the kingdom's digital sovereignty. In this regard, the pace of production of legal texts and implementation decrees related to cybercrime, intellectual property, and personal data management must be accelerated, as well as an institutional framework that ensures full legal recognition of digital interactions and the legal value of digital.

Here, we must turn to the Agency for Digital Development in Morocco, known by its acronym (the Agency for Digital Development [ADD]), which is a strategic institution that enjoys legal personality and financial independence and then created under Law No. 16-61 published in the Official Gazette No. 6604 of September 14, 2017. This agency, under the supervision of the government authority in charge of the digital economy, ensures the implementation of the state strategy in the field of digital development and encourages the dissemination of digital means and the development of their uses among citizens. It also aims to encourage digital management by bringing it closer to users (citizens and businesses) by developing digital product and service repositories. This is in addition to reducing the digital divide, supporting the industrial revolution 4.0, and managing change for society through training and awareness. The agency also fosters research and development, stimulates social and entrepreneurial innovation, and ensures responsible and sustainable digital inclusion (El Achouri, 2019).

In addition, the Agency for Digital Development has developed a project to create an Interactive Digital Center in Morocco (IDC Morocco), an innovative academy for training and disseminating digital economy professions, including virtual and augmented reality technology (VAR). This project is part of a public-private partnership between the Agency for Digital Development; the University Mohammed VI Polytechnic; the US Agency for International Development (USAID); the Ministry of Industry, Trade, and Green and Digital Economy; the Ministry of National Education, Vocational Training, Higher Education, and Scientific Research;

and the University Mohammed the Fifth in Rabat, and the international company EON Reality. The Interactive Digital Center (IDC Morocco), which was inaugurated on February 11, 2020, allows the development of knowledge transfer solutions in the field of augmented reality (AR) and virtual reality (VR) technology for various academic and vocational training programs in order to contribute to the development of skills needed for the next-generation 4.0 industries and the expansion of the digital economy at the national and regional levels. In addition, this center provides training to young Moroccans in programming techniques for applications related to virtual and augmented reality (VAR) in education and vocational training to become future experts in this field. The center will also address the skills shortage in Morocco and North Africa by providing innovative and low-cost educational development solutions for students and professionals. Thus, this program will fight youth unemployment, promote digital sector entrepreneurship, and increase industrial productivity. This project will run for 5 years, during which it will be incubated by the Mohammed VI Polytechnic University of Benguerir, with the proactive participation of all project partners. In the expansion phase, it is envisaged to create subsidiary centers to meet the needs of beneficiaries in certain regions.

Active citizenship, increased efficiency in service delivery, and inclusive economic growth and transformation are just some of the challenges faced by the public sector today. According to the Moroccan government's aim, a digital platform would connect the public administration to the active citizen, stimulate economic growth and development, and assist regional and local integration.

The government's digital transformation will rely heavily on cloud services. Data may be processed and analyzed quickly on the cloud, resulting in actionable insights, smarter choices, and a more efficient use of resources. It is easier for the public to participate in decision-making when data is readily available and communicated through many channels. This makes it easier to foster cross-departmental cooperation and social inclusion.

Cloud computing can be defined as "the provision, use, and billing of information technology services that dynamically adapt to demand and are delivered over a network." They include, but are not limited to, infrastructure (such as processing capacity and storage space), platforms, and software. With the convergence of cloud computing with the Internet of Things and 5G, a paradigm shift will occur as increasing amounts of data (due to real-time needs or intellectual property and/or data protection) will be generated and processed on a decentralized basis.

Cloud services are superior to manual paper-based operations in cost reduction, data security, and open government capabilities. If you are moving to the cloud in the public sector, you need to ensure that the move complies with all standards and delivers demonstrable advantages without undue risk.

For some years, Morocco has placed the digital economy at the heart of its development challenges. This naturally requires a nondependence on other more advanced countries in this area. For the government, the Moroccan digital sovereignty must be considered a priority that is given to the developments in this field and the increasing use of digital technologies in everyday life.

As part of promoting this sovereignty, the kingdom has acceded to several international conventions in this area. Still, it is also in the process of finalizing a legal framework for "digital trust." She added that several laws have already been adopted and others will follow soon.

This digital policy includes the protection of digital infrastructures in "vital" areas. On this point, the recently announced decision aims to protect information and infrastructure of vital importance and prevent attacks against them. This prevents sensitive data from being relocated or stored outside the national territory. The law also defines the conditions and technical and regulatory requirements for the security of information systems of organizations and administrations in the face of digital risks.

The Mohammed VI Polytechnic University (UM6P) of Benguerir has proceeded, in early 2021, to the inauguration of its new Data Center housing the most powerful "Supercomputer" in Africa (African Supercomputing Center).

With this Data Center, a world-class facility, ensuring high security, maximum availability, high flexibility, and optimal connectivity, UM6P, true to its position of excellence at the national and continental levels, is at the service of the national digital ecosystem to contribute to ensuring the kingdom's digital sovereignty and to developing new 100% Moroccan digital services.

In the same context, the Moroccan Observatory of Digital Sovereignty (OMSN) was born in June 2021 and aims to bring together companies and digital actors to emerge a sovereign Moroccan digital ecosystem. This initiative stems from an awareness of the importance of encouraging the kingdom's technological and digital independence.

The observatory will therefore aim to bring together technological, economic, and academic actors around studies, scientific articles to build a case for Moroccan digital sovereignty, and a reference manual on the subject, but also the organization of training cycles and workshops to popularize the principles and issues of this new challenge nationally and internationally.

7.6 Cyber Sovereignty Challenges in Morocco

In the future, the trend of increasingly promoting digital sovereignty norms may lead to the next evolution of international legal regulation of cyberspace being left to states. Suppose the idea of digital sovereignty allows key actors in international law to agree on the formulation of international cyber law. In that case, the law itself may be primarily represented and driven by state interests.

If this is the case, future international cyberspace law will be based on digital sovereignty at the expense of non-state actors. These two scenarios show that international cyberspace law is difficult to implement by state actors alone and requires broader approaches to develop further rule-based regulation, freedoms, and norms of inclusive global Internet governance. At the same time, the benefits of a global Internet must be actively promoted, and key stakeholders, civil society actors, and

the business community must be engaged in a broad discussion of how to preserve and improve its future governance. The development of a long-term global strategy to preserve the Internet in its current, "non-segmented," and truly global form should occur within institutions such as the UN Internet Governance Forum. And norms for international legal regulation in cyberspace should be developed by a broad coalition of countries, businesses, technology companies, and civil society. Where international norms in cyberspace are not yet firmly established, decisions should be dictated by practice and customary international law.

As a result, now the most plausible scenario is that of a split Internet, where nations control and regulate specific Internet parts based on their national or regional interests. All of us are born with a diversity of ideas and experiences that cannot be contained by any notion or country's control over a particular sector. Digital sovereignty and international Internet governance go hand in hand when there is diversity and technical options. The right of nations to build their Internet and cyberspace governance models is a fundamental tenet of modern democratic technology. The foundation of state sovereignty is technological democracy, which may be applied to any form of government. There are several ways in which Morocco may be a driving force in the development of regional and national Internet governance frameworks.

7.7 Conclusion

Cyber resilience must be a priority to be incorporated into the operational strategies of national agencies so that they are better prepared to deal with cyber threats and able to resume normal operations within an acceptable timeframe in the event of a major incident. Resilience is not only about technology but also about the organization and good governance as well as emphasizing the importance and necessity of coordination, exchange, and sharing between institutions.

References

Bodin, J., & Jean, B. (1992). *Bodin: On sovereignty*. Cambridge University Press.

Budnitsky, S., & Jia, L. (2021). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594–613.

Chambre Française de Commerce et d'Industrie du Maroc. (2021). *Transformation digitale: l'heure de vérité*. https://www.cfcim.org/wp-content/uploads/2021/03/1034-mars-2021-Transformation-numerique.pdf

Dalton, W., van Vuuren, J. J., & Westcott, J. (2017). Building cybersecurity resilience in Africa. In *The 12th International Conference on Cyber Warfare and Security*.

DGSSI. (2013). *Stratégie Nationale en matière de cybersecurié*. https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf

el Achouri, M. F. (2019). Sovereignty in Morocco: Between royal legitimacy and democratic legitimacy. *Contemporary Arab Affairs, 12*(3), 83–98. https://doi.org/10.1525/caa.2019.123005

Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication, 13*(1), 8–26. https://doi.org/10.1080/17544750.2019.1687536

ITU. (2022). *National cybersecurity strategies repository*. ITU.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

Maleh, Y. (2021). Digital transformation and cybersecurity in the context of COVID-19 proliferation. *IEEE Technology Policy and Ethics, 6*(5), 1.

Marta Taggart, & Orlando Scott-Cowle. (2021). New IDC whitepaper released – Trusted cloud: Overcoming the tension between data sovereignty and accelerated digital transformation. *AWS Security Blog*.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4).

Putterman, E. (2010). *Rousseau, law and the sovereignty of the people*. Cambridge University Press.

Weil, T., & Murugesan, S. (2020). IT risk and resilience—Cybersecurity response to COVID-19. *IT Professional, 22*(3), 4–10. https://doi.org/10.1109/MITP.2020.2988330