# KINGDOM OF MOROCCO
# CYBER READINESS AT A GLANCE

Melissa Hathaway and Francesca Spidalieri

December 2018

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
*www.potomacinstitute.org*
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

***Acknowledgements***

The Potomac Institute for Policy Studies and the authors would like to thank the following individuals and organizations for their contributions: Suzanne Moyer-Baazet, Co-founder of Nevo Technologies; Ghita Mezzour, Assistant Professor, International University of Rabat; and senior officials at the General Directorate of Information Security Systems (DGSSI), the Moroccan Royal Armed Forces (FAR), and the US Embassy in Rabat. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

# KINGDOM OF MOROCCO
# CYBER READINESS AT A GLANCE

## TABLE OF CONTENTS

INTRODUCTION . . . . . . . . . . . . . . . . . . . . . . . . .2

1. NATIONAL STRATEGY . . . . . . . . . . . . . . . . . . . . . 10

2. INCIDENT RESPONSE . . . . . . . . . . . . . . . . . . . . . 13

3. E-CRIME AND LAW ENFORCEMENT . . . . . . . . . . . . 16

4. INFORMATION SHARING . . . . . . . . . . . . . . . . . . . 18

5. INVESTMENT IN RESEARCH AND DEVELOPMENT. . . . . 19

6. DIPLOMACY AND TRADE . . . . . . . . . . . . . . . . . . . 22

7. DEFENSE AND CRISIS RESPONSE. . . . . . . . . . . . . . . 23

CRI 2.0 BOTTOM LINE . . . . . . . . . . . . . . . . . . . . . 25

ENDNOTES . . . . . . . . . . . . . . . . . . . . . . . . . . . 27

ABOUT THE AUTHORS . . . . . . . . . . . . . . . . . . . . . 31

# KINGDOM OF MOROCCO

## *CYBER READINESS AT A GLANCE*

| | |
|---|---|
| Country Population | 35.740 million |
| Population Growth | 1.3% |
| GDP at market prices (current $US) | $109.140 billion |
| GDP Growth | 4.1% |
| Year Internet Introduced | 1993 |
| National Cyber Security Strategy | 2013 |
| Internet Domain | .ma |
| Internet users per 100 users | 58 |
| Fixed broadband subscriptions per 100 users | 3.56 |
| Mobile cellular subscriptions per 100 users | 118 |

Information and Communications Technology (ICT) Development and Connectivity Standing

| | | | |
|---|---|---|---|
| International Telecommunications Union (ITU) ICT Development Index (IDI) | **100** | World Economic Forum's Networked Readiness Index (NRI) | **78** |

*Sources: World Bank (2017), ITU (2017), NRI (2016).*

## INTRODUCTION

The Kingdom of Morocco regained its independence from France in 1956 and obtained most of the territories under Spanish control shortly thereafter. In 2011, King Mohammed VI announced a series of reforms to Morocco's 15-year-old constitution in response to the wave of pro-democracy movements that were sweeping through the Middle East and North Africa. The new constitution effectively made the country a constitutional monarchy and elevated the role of the prime minister to head of government, selected through party election rather than chosen by the King. However, the King remains the supreme commander of the military and continues to chair the Council of Ministers and the Supreme Security Council – the key councils that make security policy. Morocco has positioned itself as the strategic partner and leader in the region, embracing international standards and becoming the *de facto* getaway to Africa.

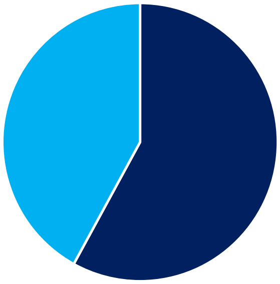
The Internet was first introduced in Morocco between 1992-1993 thanks a United States (U.S.) government sponsored project called the "Leland Initiative" — a five-year, $15 million effort to extend full Internet connectivity to more than 20 African countries.[1] In Morocco, the initiative was carried out by MTDS, a technology and development consulting company operating in Africa and headquartered in Morocco. Its engineers were essential to the inauguration of eight Internet Gateways in Sub-Saharan Africa from 1997-2002. In 1993, MTDS became Morocco's first Internet Service Provider (ISP).[2] In parallel, during 1993, the Ecole Mohammadia d'Ingénieurs obtained permission from the Internet Assigned Numbers Authority (IANA) to become the administrative and technical contact and operate the .ma Internet domain in the country. In 1995, the technical management of the .ma domain was taken over by state-owned National Posts and Telecommunications Board (*Office National des Postes et Télécommunications*, ONPT), which in 2008 was divided into two entities: Maroc Telecom (Ittisalat Al Maghrib or IAM in Arabic) for telecommunications – which remains the main telecommunications provider in Morocco – and Poste Maroc (Barid Al-Maghrib in Arabic) for postal services.[3]

Morocco was one of the first countries in the Middle East and North Africa (MENA) region to set up a regulatory environment for the ICT sector as a means of fostering a level playing field for private operators. In 1996, the government adopted Law n°24-96, which made it possible to launch the first stage of liberalization of the telecommunications sector and make the Internet publicly available — officially ending the monopoly of ONPT. In May 2006, IANA re-designated the administrative and technical contact for the .ma Internet domain and made the Moroccan National Telecommunications Regulatory Agency (*Agence Nationale de Réglementation des Télécommunications,* ANRT) the only official domain registrar in the country. In 2015, ANRT took control of .ma

*Internet access became available to all citizens in Morocco in 1996.*

and launched new automatic provisioning of .ma domains.

Since the Internet became widely available to the public in the early 2000s and the demand for Internet services started to increase, the number of Internet users in Morocco has increased exponentially, from less than 14 percent in 2008 to about 58 percent of the population in 2017 (or about 20 million users).[4] To facilitate further Internet penetration, Morocco implemented a national broadband plan (as part of Digital Morocco 2013) to close the connectivity gap across the country. However, Morocco still struggles to reach the "last mile" of rural areas, and therefore, the digital divide persists in the country – affecting the quality of services and accentuating differences between household income levels.[5] In fact, household Internet access remains limited to a minority of Moroccans, with less than 4 percent of the population having fixed broadband subscriptions. Mobile-cellular subscriptions dominate the market and the high rate of mobile phone ownership (118 percent market penetration) is driving up Internet usage and increasing the demand for mobile services. The Moroccan government clearly supports increased Internet uptake as a catalyst for economic growth. Morocco has passed five digital strategies since 1999 promoting electronic government services and operations and increasing access to education and public services. Additionally, the government has put forward several reforms to promote the digitalization of its society and to advance its digital economy.



*Morocco's Internet Penetration: 58%*

The liberalization of the telecommunications sector at the end of the 1990s was followed by the publication of several digital strategies aimed at positioning Morocco among the dynamic emerging countries in the ICT sector.[6] These strategies included the following:

- the "Morocco 1999-2003," which outlined the country's vision for ICT and its potential;
- the "E-Morocco 2010," which covered from 2005-2010 and promoted removing barriers via digital inclusion and ICT sector competitiveness;
- the 2009-2015 National Pact for Industrial Emergence (Pacte Nationale pour l'Emergence Industrielle, PNEI), which looked to support export-oriented industries – in this case with offshoring and ICT services – through incentives, targeted training and support measures;
- the "Digital Morocco 2013" Strategy, which covered from 2009-2013 and focused on making the IT sector a cornerstone of the economy – turning the country into a regional technology hub while at the same time driving the development of technical talent;
- and the latest "Digital Morocco 2020," which covers from 2017-2020 and aims to accelerate Morocco's digital transformation, encouraging ICT entrepreneurship, boosting its international position in cost-competitive IT services, and reinforcing the country's status as a regional leader and gateway to Africa.

As a result of the early push to develop the country's ICT sector in the mid-1990s, Morocco has become one of the leading destinations for investment – mostly from francophone countries – in the field of call centers, IT offshoring, electronic payments, and the outsourcing of other business processes. Today, Morocco's economy is highly dependent on a well-functioning and advanced ICT sector and over 3 percent of its gross domestic product (GDP) depends on contributions from the ICT sector.[7] The offshoring business, in particular, attracts significant foreign direct investments, and several multinational companies have established operations in the country.

In 2009, the ANRT in coordination with the Ministry of Industry, Commerce, Investment and Digital Economy (*Ministère de l'Industrie, du Commerce, de l'Investissement et de l'Economie Numérique*, MCINet) launched the wide-ranging National Strategy for Information Society and Digital Economy 2009-2013 (Digital Morocco 2013). Its goal was to position Morocco as a strategic ICT hub in the MENA region and ARNT and MCINet solicited input from the industry association Moroccan Federation of IT, Telecommunications and Offshoring (*Fédération Marocaine des Technologies de l' Information, des Télécommunications et de l'Offshoring*, APEBI) to increase the likelihood of success.[8] This digital plan recognized that the ICT sector already accounted for 7 percent of the world GDP, attracting 25 percent of the world economic growth as well as 60 percent of jobs in the industrialized world. The strategy articulated 51 ambitious objectives to transform Morocco into an information society and promote its digital economy and national competitiveness. It set four strategic priorities for the country:

1. consolidate ICT industries with a focus on excellence niches such as offshoring;
2. support the automation of small and medium-sized enterprises (SMEs);
3. boost e-government services; and
4. foster the dissemination of ICT usage among Moroccan households.[9]

Similar to earlier strategies, it continued to promote the need for "digital trust" as an essential component for Morocco to create confidence in the digital economy. The strategy intended to increase public access to broadband connectivity and transform the country's ICT sector into one of the economy's main pillars and source of productivity, competitiveness, and added-value. It also allocated 5.2 billion MAD ($546 million) over five years (2009-2013) to implement the initiatives and measures proposed, with over 80 percent of the budget dedicated to "socially transform" and create "user-oriented public services." The strategy also named government agencies to govern and provide direction for the strategy's implementation, including the National Council of Digital Economy and Information Technologies (CNTI), responsible for elaborating policies related to the protection of critical information infrastructure in the country, and an inter-ministerial committee in charge of steering e-government programs (CIGOV). The document, however, was not supplemented by sectoral action plans specifying desired outcomes and timelines for the projects and actions proposed. Despite the best of intentions, the strategy did not meet the government's ambitious expectations. More than half of the e-government projects in the plan were either not completed (e.g., healthcare, local government, capital markets procurements, and tenders) or were insufficiently implemented (e.g., judicial system, regional portals, land purchasers). Less than 1/3 of the initiatives had successful outcomes.[10] One of the main reasons for this was the absence of an effective coordination mechanism among ministries. Each ministry had its own IT security department and pursued the strategy's initiatives according to its own mandate or mission.

In 2015, the Ministry of Industry, Commerce, Investment and Digital Economy in collaboration with other relevant departments launched the updated "Digital Morocco 2020" strategy. This strategy is built upon the lessons learned and advancements of the previous digital strategies and articulated a vision to accelerate Morocco's digital transformation, foster the dissemination of ICT usage among Moroccan households, improve its regional competitiveness, and boost its digital economy.[11] In particular, the new digital strategy aimed at reinforcing Morocco's status as a regional digital hub in French-speaking Africa, while continuing to promote it as an attractive destination for outsourcing services, offshoring, electronic payment, and software development. These efforts have helped transform Morocco into one of the top performing countries in the region in terms of ICT infrastructure and favorable business environment. Digital Morocco 2020 allocated 7.146 billion MAD ($750 million) to reduce the digital divide by 50 percent via the following: the digitization of administrative services, improved access to the Internet through free Wi-Fi in public spaces, the creation of digital literacy programs, and training of over 30,000 ICT professionals a year by 2020.[12]

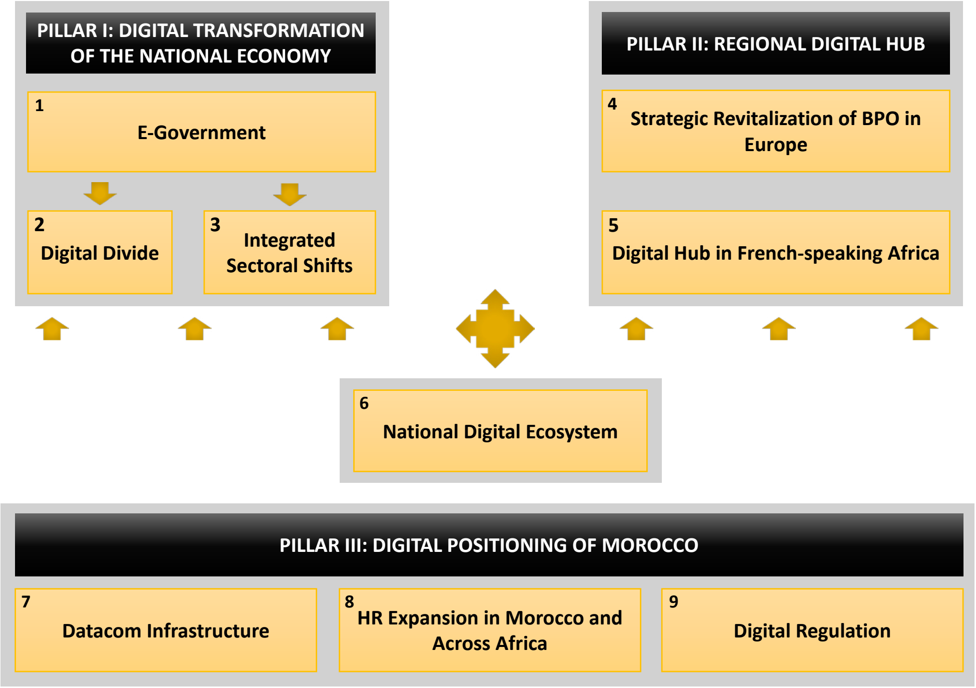

PILLAR I: DIGITAL TRANSFORMATION OF THE NATIONAL ECONOMY
1
E-Government
2
Digital Divide
3
Integrated Sectoral Shifts
PILLAR II: REGIONAL DIGITAL HUB
4
Strategic Revitalization of BPO in Europe
5
Digital Hub in French-speaking Africa
6
National Digital Ecosystem
PILLAR III: DIGITAL POSITIONING OF MOROCCO
7
Datacom Infrastructure
8
HR Expansion in Morocco and Across Africa
9
Digital Regulation

*Figure 1: Pillars of the 2020 Morocco Digital Strategy.*

As part of this strategy, the government launched several initiatives in parallel to promote Moroccan innovation. The initiatives promoted collaborative efforts domestically and abroad to strengthen digital trust in e-commerce, enforce legislation to protect personal data and e-commerce transactions, and encourage entrepreneurship. To increase Morocco's competitiveness, the government eliminated a ban enacted by the ANRT regarding voice over Internet protocol (VoIP) services, which only lasted 10 months (and was ended just a few days ahead of the 2016 United Nations Climate Change Conference held in Marrakech, Morocco). Previously, ANRT had blocked and taxed VoIP providers. In the first half of 2016, the operating costs of companies in the ICT sector had been negatively impacted by at least $320 million.[13] These new reforms helped the ICT sector to grow steadily.

Domestic and foreign investments have grown in the areas of IT security, mobile services, social networks, big data, and cloud computing. These new investments built upon the foundations of Morocco's well-established ICT industry in the areas of electronic payments, software development, and IT offshoring. Morocco also recognized that cyber security products and services are a growing opportunity in Africa. The market opportunity is set to grow from 12.7 billion MAD ($1.33 billion) in 2017, to 22.1 billion MAD ($2.32 billion) by 2020.[14] Morocco's regionally competitive ICT infrastructure and the structural and sectorial reforms undertaken in recent years to improve the digital economy have enabled Morocco to become one of the top performing countries in the region in terms of favorable business environment and a preferred location for technology companies trying to expand their presence in French-speaking Africa. In 2013, the Moroccan ICT sector achieved ICT export revenues of 9.5 billion MAD ($1 billion) and was ranked the best in Africa for business process outsourcing.[15] This success has been facilitated by the establishment of dedicated technology parks (e.g., Casanearshore,[16] Rabat Technopolis,[17] Tangiers Technical Park,[18] etc.), which operate under offshore status and attract companies using a variety of tax incentives.

Yet, despite the growing ICT and cyber security demands by private sector companies, the industry is still highly dependent on public sector tenders. The e-government initiatives, smart cities projects, renewable energy projects, and transportation infrastructure upgrades that were called for (and funded) in the Digital Morocco 2020 strategy — are government-led procurements and represent the majority of the ICT spending in Morocco.

With increased ICT uptake and Internet connectivity, Morocco is gaining a deeper appreciation of the risks and challenges associated with cyber crime, cyber fraud, and cyber terrorism. While only a few incidents have been officially reported, as the country becomes more connected, so too are the instances of identity theft, bank-card theft, fraud, illicit money transfers, phishing scams, malware targeting critical infrastructure, distributed denial of service (DDoS) attacks, "sextortion" cases, and even "cyberterrorism." In response to increasing cyber threats and recognizing the importance of protecting and securing information systems of administrations, public bodies, and infrastructures of vital importance, the 2009 National Strategy for Information Society and Digital Economy (Digital Morocco 2013) called for the development of a national cyber security strategy (policy) and provided the first national governance roadmap for cyber security focused on enhancing security capabilities, securing critical information infrastructures, and combating cyber crime.[19] Several institutions and organizational structures were established to support these goals, including:

- the Strategic Committee for the Security of Information Systems (*Comité Stratégique de la Sécurité des Systèmes d'Informations*, CSSSI);
- the General Directorate of Information Security Systems (*Direction Générale de la Sécurité des Systèmes d'Information*, DGSSI) – created in 2011 within the Administration of National Defense (ADN) and under the supervision of CSSSI to serve as the competent authority responsible for developing and implementing the national cyber security strategy, policy, and roadmap of the country;
- the National Control Commission for Protection of Personal Data (*Commission Nationale de Contrôle de la Protection des Données*, CNDP) responsible for the protection and processing of personal data;
- the Moroccan Computer Emergency Response Team (ma-CERT), established under the direction of ADN and responsible for responding and mitigating cyber security incidents of national importance; and
- regional forensics laboratories for digital and anti-cyber crime trace analysis (*laboratoires régionaux d'analyse de traces numériques et anti-cybercriminalité*), a division under the Moroccan Directorate General for National Security (*Direction Générale de la Sûreté Nationale*, DGSN) that deals with cyber crimes.

In addition, the ANRT was elevated as the government authority with a close relationship with telecommunications operators and Internet Service Providers (ISPs). Morocco also started to update and strengthen its legal and regulatory framework to address cyber crime and data protection.

In 2012, CSSSI adopted Morocco's first national cyber security strategy (*Stratégie nationale en Sécurité des Systèmes d'Information*) built on the Digital Morocco 2013 strategy and focused on four main strategic priorities, namely:

1. evaluating risks to information systems within government and in vital infrastructures;
2. protecting the information systems of government agencies, public organizations, and vital infrastructures;
3. strengthening the foundations of information systems security (legal framework, sensitization, training, research and development); and
4. promoting national and international cooperation.[20]

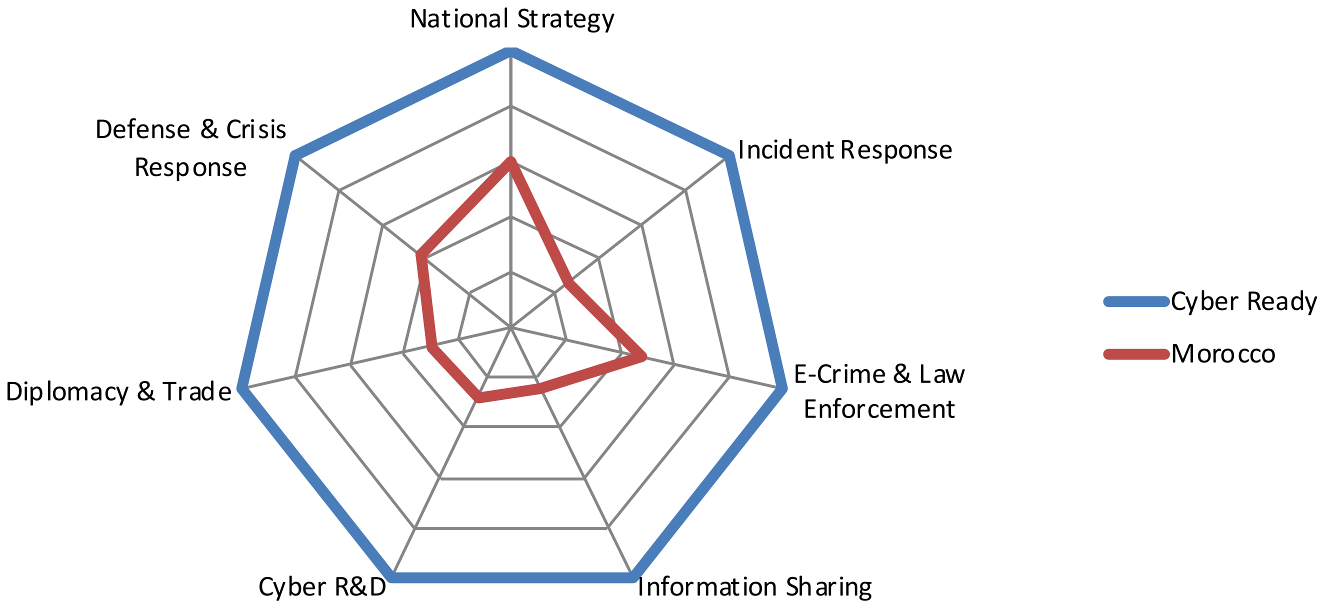
As part of the national cyber security strategy, CSSSI also developed an action plan for DGSSI "to operationalize the guidelines and directives included in the strategy."[21] One of the main actions prescribed was to develop and implement a National Directive on Information Systems Security (Directive Nationale de la Sécurité des Systèmes d'Information, DNSSI) and other specific directives aimed at "raising and homogenizing the level of protection and maturity of the security of the information systems of administrations, public entities, and infrastructures of vital importance."[22] The directives that have been enacted by decree, reaffirm the responsibility of DGSSI to establish specific security rules and standards for critical infrastructures and ensure their compliance. Each entity affected by these laws is required to develop additional necessary organizational and technical security measures to be adopted and subsequently shared with DGSSI, carry out audits of their information systems, and report all significant incidents to ma-CERT. Finally, these entities are required to submit annual reports to DGSSI indicating the degree of security maturity achieved and detailing progress made in implementing the directives.

In 2013, hackers working on behalf of the Algerian regime attempted to gain access to and sabotage the Moroccan government's information systems, national databases, and public administration websites.[23] Because of the security measures the Ministry of Defense had put in place to counter attacks to critical infrastructures and vital services, the DGSSI was able to detect and block most of the intrusion attempts coming from Algeria and many more from other countries. These events, however, show that there is more work to be done to secure the country's critical digital infrastructure and services upon which its digital future depends.

Awareness of the digital exposures and risks presented by ICT is still low among small and medium enterprises (SMEs) – the core of Morocco's private sector. Moreover, the cyber-related threats to Morocco's companies, assets, infrastructures, and services are not publicly discussed, so funds are not sufficiently allocated for risk reduction measures.[24] As Morocco embraces the digital transformation of its agriculture and energy (solar fields) sectors and prepares to have the second largest port (Tanger-Med port) in the Mediterranean soon, it will have to promote a better understanding of the risks and opportunities of this modernization. Raising awareness regarding the need for infrastructure resilience and data protection are foundational components of Morocco's strategies. Morocco is well positioned "as a 'best cost' country...with proximity to European markets and very competitive costs,"[25] and is on a path toward reaping the benefits associated with being part of the global digital economy. Its journey will be enhanced by increasing the number of personnel that are proficient in digital risk management across every sector, not just ICT.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Morocco's current preparedness levels for cyber risks. This analysis provides an actionable blueprint for

Morocco to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity to closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows:



*Kingdom of Morocco Cyber Readiness Assessment (2018).*

## 1. NATIONAL STRATEGY

In December 2012, the Strategic Committee for the Security of Information Systems (CSSSI), which is composed of representatives from 13 ministries chaired by the ADN, and is responsible for setting information security directives and guidelines for all key government entities and approving funding, adopted Morocco's first National Cyber Security Strategy. The document was built upon the Digital Morocco 2013 strategy and outlined programs and projects aimed at "ensuring the protection of the information systems of government agencies, public organizations, and vital infrastructures, […] as well as creating the conditions for a trusted and secure environment conducive of the development of an information society." It highlighted four main strategic priorities: 1) evaluating risks to information systems of government agencies, public organizations, and infrastructures of vital importance; 2) protecting and defending information systems of government agencies, public organizations, and vital infrastructures; 3) strengthening the foundations of information systems security (legal framework, sensitization, training, research and development (R&D); and 4) promoting national and international cooperation.[26] However, the strategy only provided an overview of the programs and projects to be implemented, suggesting that specific operational action plans were still necessary for each of those programs — including concrete measures implemented according to a predefined timeline and determination of which actors should contribute to the achievement of specific and quantifiable objectives. In order to create the right conditions for the implementation of those action plans, the strategy also called for the key organizations that developed the national cyber security strategy (CSSSI, DGSSI, etc.) to be involved in defining the relative action plans in accordance with the country's needs, priorities, and constraints. The national cyber security strategy concludes with a commitment to be periodically revised and adapted, as needed, to reflect new realities and requirements, but no new version has been published, to date.

*The first Morocco National Cyber Security Strategy was published in 2012 and was called for by the Digital Morocco strategy.*

The strategy did identify the key government entities involved in the cyber security architecture of the country and recognized DGSSI as the competent authority responsible for the cyber security of the nation and

*The General Directorate of Information Security Systems (DGSSI) is the competent authority responsible for the national cyber security of Morocco and the operationalization of the strategy.*

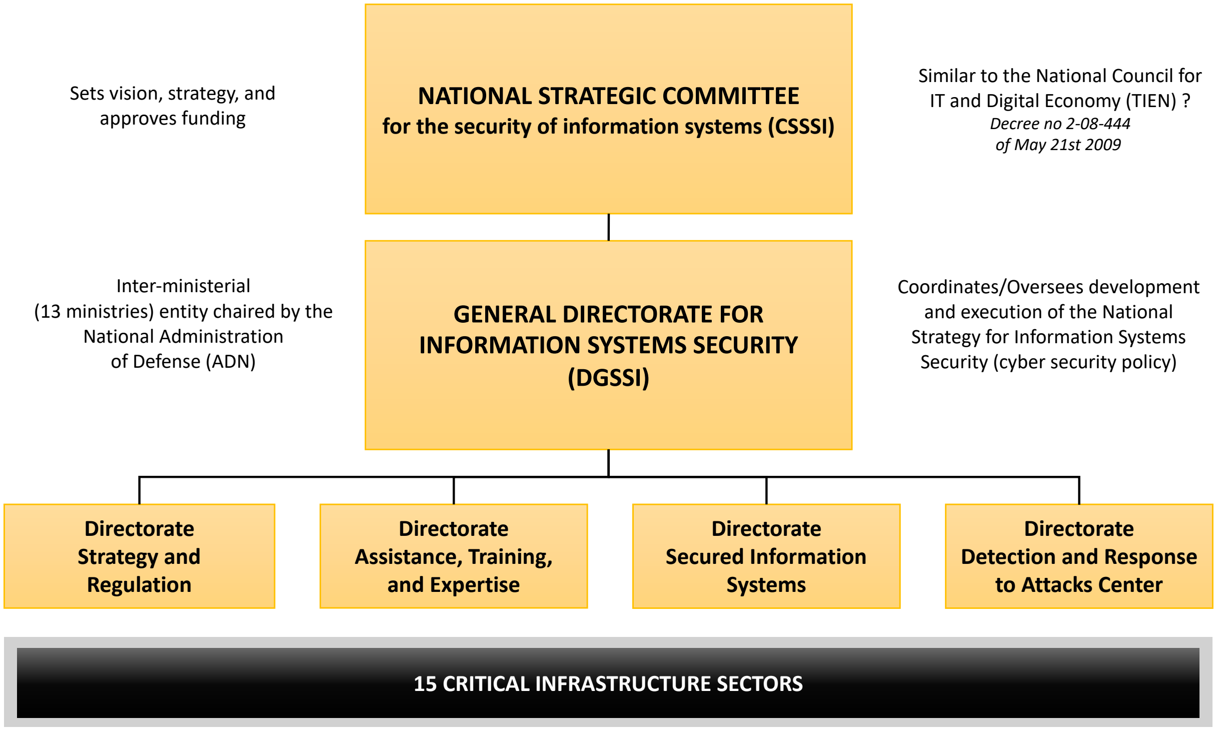

Sets vision, strategy, and approves funding
NATIONAL STRATEGIC COMMITTEE for the security of information systems (CSSSI)
Similar to the National Council for IT and Digital Economy (TIEN) ?
Decree no 2-08-444 of May 21st 2009
Inter-ministerial (13 ministries) entity chaired by the National Administration of Defense (ADN)
GENERAL DIRECTORATE FOR INFORMATION SYSTEMS SECURITY (DGSSI)
Coordinates/Oversees development and execution of the National Strategy for Information Systems Security (cyber security policy)
Directorate Strategy and Regulation
Directorate Assistance, Training, and Expertise
Directorate Secured Information Systems
Directorate Detection and Response to Attacks Center
15 CRITICAL INFRASTRUCTURE SECTORS

*Figure 2: Morocco Cyber Security Organizational Chart (2018).*

operationalization of the strategy. This joint inter-ministerial coordination body sits under the supervision of CSSSI and is composed of four directorates: 1) the Strategy and Regulation Directorate; 2) the Assistance, Training, Monitoring and Expertise Directorate; 3) the Secured Information Systems Directorate; and 4) the Detection and Response to Attacks Center Directorate.

DGSSI operates out of the capital Rabat, and is tasked with a number of responsibilities, including:

- ensuring the implementation of the directives and guidelines set out by CSSSI;
- operationalizing the national cyber security strategy;
- devising standards and specific rules for the security of national information systems and critical infrastructure;
- creating an annual action plan for all ministries to ensure vital national infrastructures have robust Internet access and are more resilient;
- assisting and advising public and private sector entities about the safety of their information security;
- establishing a monitoring system to detect and warn of events affecting or likely to affect national information security;
- developing scientific and technical expertise in the IT security field;

- ensuring that security audits of information systems are carried out in accordance with the scope and terms set by the CSSSI;
- organizing capacity building training courses and awareness actions through the development of international cooperation relations in the field of computer security;
- ensuring that Morocco meets its policy objectives in international treaties; and
- issuing licenses, managing declarations concerning means and cryptographic services, certifying devices for the creation and digital signature verification, and approving service providers for digital certification.

Some of these responsibilities, however, are still maturing and at different stages of operational effectiveness.

Following the commitments made in the national cyber security strategy, CSSSI developed a 2013 action plan for DGSSI "to operationalize the guidelines and directives included in the strategy."[27] One of the main actions prescribed was to further develop and implement a National Directive on Information Systems Security (Directive Nationale de la Sécurité des Systèmes d'Information, DNSSI) aimed at "raising and homogenizing the level of protection and maturity of the security of the information systems of administrations, public entities, and infrastructures of vital importance."[28] This is modeled after the European Union's Network and Information Security (NIS) Directive that requires businesses to establish minimum standards of care for their critical services. As part of Morocco's directive, the covered entities are required to adopt basic organizational and technical security measures and report to DGSSI any additional procedures and action plans they require to implement precautions for their information systems. The covered entities are also required to submit annual reports describing the maturity level achieved and progress made toward implementing the standards required by the directive. DGSSI then consolidates and summarizes the results for CSSSI, which can recommend further actions and audits by DGSSI. DGSSI has also the authority to compel government entities, National Critical Infrastructures (NCIs), and commercial-sector entities to conduct security audits of their information systems. In October 2018, a new national decree authorized DGSSI to certify private auditors to conduct such audits.[29]

In the event of a national-level digital crisis, DGSSI leads the coordination and response. In May 2017, DGSSI had to activate this coordination mechanism because Morocco was one of at least 100 countries affected by a global ransomware attack, known as WannaCry. The coordination cell includes the Royal Moroccan Armed Forces (Forces Armées Royales, FAR), ADN, and other Ministries, and is broken down into two branches – operations and decision-making. In addition to DGSSI, the FAR is responsible for safeguarding and ensuring the resilience and availability of the country's military operation networks (i.e., air defense and surveillance, ground surveillance, and special communications) as well as the exchange of data among the three military components (i.e., army, navy, and air force).

The FAR reports directly to the King, who is also the Supreme Commander and Chief of General Staff of the FAR.

Despite the notable progress in increased cyber security preparedness and capability that has made Morocco one of the more advanced countries in the region, the various digital strategies, economic initiatives, and national cyber security policies are not aligned. The digital economy only represents 7 percent of Morocco's current GDP. Its economy is primarily fueled by agriculture and textile exports and is a hub for Mediterranean shipping. Morocco is also set for online deployment of the world's largest concentrated solar power plant— the Noor Complex — that will produce enough energy to power over one million homes.[30] Of course, Morocco's share of the digital economy will grow as more of its businesses become digital and as broadband becomes more affordable and capable in reaching rural areas. As Morocco embraces the digitization of its critical infrastructures, services, and companies, it will need to align its risk reduction measures and set policies and standards. The public is largely unaware of the cyber threats to society and the digital economy, so they are unprepared for major digital crises incident response and recovery. Finally, the Moroccan government should further empower DGSSI to realize the vision that the digital economy requires trust, and that it cannot be achieved without the twin objectives of security and resilience at its core.

## 2. INCIDENT RESPONSE

The 2009 National Strategy for Information Society and Digital Economy (Digital Morocco 2013) called for the establishment of a national Computer Emergency Response Team (CERT) with the primary responsibility to "respond to security incidents, coordinate responses at the national level and propose different services related to the handling of these incidents, the analysis of their vulnerability and the restoration of systems under attack."[31]

It was not until 2011, however, that Morocco was able to develop a national CERT (ma-CERT). First, the International Multilateral Partnership Against Cyber Threats (IMPACT) – a key partner of the ITU (the United Nations' specialized agency for ICTs) – conducted an initial baseline assessment and outlined the requirements for standing up a CERT. Then, Morocco received both financial support and

*In 2011, Morocco established its first Computer Emergency Response Team (ma-CERT), under the supervision of DGSSI, and responsible for cyber incident response and analysis of threats and vulnerabilities.*

technical expertise from the Korea Internet & Security Agency (KISA), an ICT-focused organization within South Korea's Ministry of Science.[32] Thanks to these initiatives, ma-CERT was established and it joined the international Forum of Incident Response and Security Teams (FIRST) in April 2013.

Today, ma-CERT sits under the supervision of DGSSI, and is responsible for responding to cyber security incidents, coordinating responses at the national level, and providing different services related to incident handling and vulnerability analysis, and the restoration of systems under attack. Although its operations are 24x7 and it is providing incident response support and additional services to the government, ma-CERT has insufficient capacity to support a whole-of-government and whole-of-society incident response coordination and containment. It still needs to identify a network of authoritative national contact points within both the government and critical infrastructure sectors responsible for the operation and recovery of critical services in the event of a full-scale national digital incident (like WannaCry).

Additionally, there is no evidence of an emergency and crisis national incident response plan or an effective information warning and alert system that can be used to receive, address, and transmit urgent information in a timely manner. Ma-CERT is still largely perceived as a reactive organization, mostly focused on providing advisories, bulletins, and information on current threats, and offering *ad hoc* incident response support.

As stated earlier, Morocco is seeing increasing instances of identity theft, bank-card theft, illicit money transfers, phishing scams, malware targeting critical infrastructure, DDoS attacks, "sextortion" cases, and even "cyberterrorism." Yet, the DGSSI or ma-CERT do not publish national cyber threat assessment(s) to government agencies, critical infrastructure, and critical commercial services networks. It is unclear how the different Ministries work together to evaluate risks and assess their level of severity/urgency across organizations. According to Moroccan security practitioners, the country still lacks strong expertise in cyber security and cyber defense and has yet to establish a centralized system to effectively and expeditiously access and share threat intelligence information and situational awareness with government agencies and institutions.[33]

Nonetheless, the government has taken steps to increase its security posture. Two directives in particular aim to increase the level of protection and security of the information systems of government agencies, public entities, and entities of vital national importance. They were adopted by decree between 2014 and 2016 — the National Directive on Information Systems Security (*Directive Nationale de la Sécurité des Systèmes d'Information*, DNSSI) and the Decree on the Protection of Sensitive Information System and Infrastructures of Vital Importance.[34]

The DNSSI describes basic organizational and technical security measures that must be applied by public administrations and agencies as well as infrastructures of vital importance. The directive requires these covered entities to develop their own action plans, establish risk governance mechanisms and technical security measures, and submit to DGSSI their plans and an annual report documenting their actions and progress toward the reduction of risks to their enterprises. DGSSI then consolidates and summarizes the results of those reports for CSSSI, which can recommend further actions and audits by DGSSI.

The second decree complements the DNSSI and names the activities and entities of vital importance that DGSSI is tasked to oversee and protect. These sectors are defined as "those relating to the production and distribution of goods and services essential to satisfy the needs of people's lives, or to the exercise of the prerogatives of the State, or to the functioning of the economy, or to the maintenance of the country's security capabilities." They include: public safety, financial,[35] manufacturing, transportation, production and distribution of energy and mining, water supply and distribution, telecommunications and postal services, audio-visual and communication, healthcare, justice, and legislation. DGSSI determines the specific security standards and requirements that these sectors must meet.[36] The detailed list of "infrastructures of vital importance holding sensitive information systems" is kept secret by the government. However, the decree intends to cover all "installations, networks and systems essential for the maintenance of the critical functions of society, healthcare, safety, security, and the economic and social well-being," and that if damaged, rendered unavailable, or destroyed would cause the failure of these essential functions.[37]

As a result of this decree, DGSSI, in consultation with the National Defense Administration (*Administration de la Défense Nationale*, ADN), identified 15 specific NCIs and established specific certification schema for them. NCIs are required to implement the necessary resources for supervision and detection of cyber attacks, to develop contingency plans to protect critical functions from the negative effects of major information system failures or disasters, and to ensure operational continuity. There is a cross-border data flow determination in this decree. For example, entities are required to ensure their sensitive data remains within the national territory of Morocco. They are also required to establish a security operations center (SOC) and submit to a security audit program carried out by DGSSI or by certified private auditors of information systems under DGSSI supervision. In addition, entities must report all significant cyber incidents "affecting the security or operations of their sensitive information systems" and within 48 hours of an event, communicate to ma-CERT all information and technical data generated by any major security event targeting its sensitive information systems. Despite this, there are no standardized reporting and notification protocols in place. Within a month after any major security incident, DGSSI must then transmit a summary of its investigation and its recommendations to the affected entity.[38]

Morocco has recognized the importance of conducting regular national and sector-specific benchmarking exercises to measure the cyber security preparedness of the country, but the only programs that have been initiated so far are the initiatives highlighted above for identification and classification of sensitive information systems of vital infrastructures, measuring the level of security maturity achieved by these critical infrastructures, and the progress made to implement the DNSSI.

## 3. E-CRIME AND LAW ENFORCEMENT

Morocco has been working to reinforce its legal and regulatory framework to better protect its society from cyber crime and harmonize it with partner countries. The country has updated its penal code and legislation governing ICT, implemented new decrees and laws to combat cyber crime and protect personal information, and ratified international conventions like the Council of Europe's Convention on Cybercrime and its Additional Protocol on cloud infrastructures,[39] and the Arab Convention against Information Technology Crimes. While the Moroccan government does not publish statistics pertaining to cyber crime, it has passed or updated several related domestic laws, including:

- Law 07-03 introducing for the first time the notion of cyber crime to the Moroccan penal code, defined as "offenses related to automated data processing systems";
- Law 53-05 related to e-signatures and electronic exchange of legal data to facilitate the use of encryption means and electronic certification;
- Law 31-08 related to the protection of online consumers; and
- Law 09-08 regarding automated processing of personal data.

*Morocco has been working to reinforce its legal and regulatory framework to better protect its society from cyber crime and harmonize it with partner countries.*

In 2011, the National Control Commission for Protection of Personal Data (CNDP), responsible for ensuring data protection in Morocco, established a Data Protection Authority and law to bring Morocco in line with European regulations. In 2016, a decree was issued on the Protection of Sensitive Information System and Infrastructures of Vital Importance, which imposed strict data protection requirements, including limiting the cross-border data flows and establishing data residency requirements. For example,

*Morocco has ratified both the Council of Europe's Convention on Cybercrime and the Arab Convention against Information Technology Crimes.*

before any transfer of personal data to a foreign state, it must first receive authorization from the CNDP. Moreover, the decree states:

> "[the] person/entity in charge of the processing operation can transfer personal data to a foreign state only if the said state ensures under its applicable legal framework that it has an adequate level of protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which these data is or might be subject."[40]

This, of course, affects e-commerce and other transactions that utilize e-platforms. Therefore, the CNDP has designated a list of countries with acceptable laws and data can move across borders for only CNDP-approved countries. There are many sectors that collect and process sensitive information (e.g., healthcare, finance, national security) and they are working to comply with the requirements of this new law.

The Moroccan General Directorate for National Security (DGSN) is the entity responsible for combating and investigating cyber-related crimes. It has two broad cyber-related missions. First, it is charged with protecting its own systems and networks that contain sensitive information, such as the national identity database that has been classified as a "critical infrastructure." Secondly, it conducts investigations about cyber crime and other crimes that use new technology, such as cryptocurrency, and can investigate incidents of national interest in collaboration with DGSSI, if needed. DGSN's investigations include issues of malware within critical infrastructures, DDoS, bank-card theft, phishing attacks, illegal use of cryptocurrencies, cloud-based incidents, online terrorist propaganda, and "sextortion" cases.[41] Investigations into these types of crimes, however, are often hindered by the absence of a formal, legal cooperative relation with ISPs. If an incident or issue is considered a national security matter, than ISPs are compelled to provide support.

Penal proceedings in the case of cyber crimes are limited and the country still lacks sufficiently-trained legal professionals to effectively address different elements of cyber crime and successfully investigate and prosecute offenders. To respond to this need, the DGSN has established 29 units specialized in the fight against cyber crime, 19 regional commands with about 10 cyber specialists at each location, and regional forensics laboratories for digital and anti-cyber crime trace analysis. DGSN is also providing dedicated training programs on cyber security for legal professionals (e.g., court judges, prosecutors, law enforcement). Other offices within DGSN also deal with cyber-related issues, including the offices of immigration, economic/financial crimes, counter-narcotics, and counter-terrorism.

In July 2016, the Ministry of Justice, together with the Council of Europe, organized an international workshop in Rabat on best practices regarding cyber crime legislation and electronic evidence. Morocco also participates in an anti-cyber crime initiative sponsored by the EU called the Action Global sur la Cybercriminalité Elargie (GLACY+).[42]

Morocco has tried but did not succeed in establishing successful anti-botnet and malware remediation initiatives to reduce infections and criminal activity emanating from its own infrastructures and networks. As Internet use becomes more widespread and as more connected devices become avenues for infection and exploitation, Morocco will need to further increase the capacity of its law enforcement agencies, establish a coordinating agency responsible for ensuring that all its international cyber crime requirements are being met domestically and across jurisdictional lines, and commit more human and financial resources to effectively respond to increased cyber crime and reduce infrastructural weaknesses.

## 4. INFORMATION SHARING

While Morocco does not have a national information sharing policy and has yet to establish a centralized system to effectively and expeditiously access and share threat intelligence information and situational awareness within government agencies or with the private sector and international partners, it has recognized the importance of national and international information sharing and cooperation and regularly participates in efforts to exchange information, expertise, and training with European and North Atlantic Treaty Organization (NATO) allies.[43]

*While Morocco does not have a national information sharing policy, it has recognized the importance of national and international information sharing and cooperation.*

Currently, the only mechanisms used for sharing information within the government and across critical industries are offered by ma-CERT and DGSSI. Ma-CERT is also a member of the Organisation of Islamic Conference-Computer Emergency Response Team (OIC-CERT), a group of 18 countries, including Egypt, Iran, Nigeria, Saudi Arabia, and Turkey. This group includes national CERTs from the various countries and is intended to facilitate information sharing among Islamic countries. The OIC-CERT organizes training, workshops, and exercises designed to provide real-time experience in addressing cyber threats and crises, including timely and actionable information sharing.[44]

In addition, the country has established a Moroccan Academic Computer Emergency Response Team (EDU-CERT), which facilitates information sharing and incident response activities across the academic community. It also provides services to the Moroccan Academic Research Wide Area Network.[45]

Morocco recognizes that it requires much progress in this area. Ma-CERT and DGSSI have an opportunity to enhance and expand the exchange of actionable information both inside and outside the government. Each ministry, CNI, business, and international partner needs information that can improve their security posture, and DGSSI should prioritize the need for timely and actionable information sharing within government agencies and across critical industries, the private sector, and international partners.

## 5. INVESTMENT IN RESEARCH AND DEVELOPMENT

While Morocco does not have an officially recognized national or sector-specific R&D program dedicated to cyber security or advanced technology development, the "Digital Morocco 2013" strategy stated a clear intent to make the ICT sector a cornerstone of the Moroccan economy and a driver for human development. It also emphasized the importance of cyber security training and awareness programs, and human skills development to analyze and understand advanced coding, programming, and IT development techniques.[46] The "Digital Morocco 2020" strategy reiterated these objectives and set the ambitious goal of reducing the digital divide in the country by half and increasing training to 30,000 ICT professionals a year by 2020.[47]

*Morocco has become a regional leader in digital services and one of the top performing countries in Africa in terms of business environment.*

Morocco's regionally competitive ICT infrastructure, recent structural and sectorial reforms to foster its digital economy, and its talented, multilingual workforce have enabled the country to become a leader in outsourcing services, offshoring, electronic payment, and software development. It is one of the top performing countries in the region in terms of business environment. In 2013, the Moroccan ICT sector achieved IT export revenues of $1 billion and was ranked the best in Africa for business process outsourcing.[48] In 2015, the ICT sector contributed to over 3 percent of Morocco's GDP, bolstered by the diversification and internationalization of large sections of the software industry. The government's Digital Morocco 2020 strategy provided resources to further build on the country's international position providing cost-competitive IT services and emphasized greater diversification and entrepreneurship. This success has been facilitated by the establishment of dedicated technology parks which operate under offshore status and attract companies using a variety of tax incentives. For example, in 2006, Morocco launched its first and largest technology park – the Casanearshore Park, in Casablanca. It became the incubator of over 100 businesses and attracted international technology companies including Dell, IBM, Accenture, Atos, HP, and Logica. Its development was the result of a $341 million-dollar investment by MEDZ Sourcing – a state-driven development company that also operates technology parks throughout the country. MEDZ Sourcing facilitates access to land for export-oriented IT activities and

*Morocco has five technology parks – developed and managed by state-driven company MEDZ Sourcing – dedicated to advancing innovation and the country's position as a leader in the outsourcing industry.*

has established other technology parks at Technopolis in Rabat, Tetouan Shore near Tangiers, Fès Shore in Fez, and Oujda Shore in Oujda. Each park caps income tax at 20 percent, although lower tax rates are available in certain circumstances, and they offer training programs in order to meet demand for skilled IT workers.[49]

In July 2013, IBM created a service center with 400 employees at Casanearshore to serve Moroccan and other African markets. As part of a government agreement, IBM is collaborating with Moroccan academic institutions in growing technologies such as cloud computing, big data, system integration, and outsourcing. The Moroccan authorities have also set up funding mechanisms designed to encourage entrepreneurship and boost the development of start-ups. The most notable initiative is the Moroccan Digital Fund (*Maroc Numeric Fund*, MNF), which was established in 2010 by the state-owned Deposit and Management Fund (*Caisse de Dépôt et de Gestion*) and the country's three largest commercial banks – Attijariwafa Bank, BMCE, and Banque Central Populaire. MNF provides seed funding and other technical and financial assistance to local technology firms.[50] Since its launch, it has invested in a range of wide-range of start-ups, including the cyber security firm, Netpeas; the online invoicing platform, Greendizer; and e-commerce platforms like Soukaffaires and Mydeal. One of the Kingdom's digital success stories is the company, Involys SA, a software and information technology services provider. Involys SA greatly benefited from the government's commitment to promote the digitalization of small and medium enterprises to increase productivity, support local organizations to develop IT markets, and build greater potential for the exports in the ICT sector. Another successful start-up is HPS, an innovative payment solutions company, which is providing secure payment services to issuers, acquirers, card processors, independent sales organizations (ISOs), retailers, and national and regional switches all over Africa.[51] Aside from these success stories, however, the start-up scene in Morocco is currently still very limited.

In October 2018, Orange Cyberdefense announced the launch a new state-of-the-art cyber security center in Casablanca that would help Orange build a strong position in the Moroccan market, expand its presence in French-speaking Africa, and bring through a next generation of cyber security experts to Morocco. The new operations center will draw on the assistance of Orange's Cyber Security Centre of Excellence in France and plans to forge partnerships with universities in Morocco to make the new center its main tech hub to serve businesses in French-speaking African countries.[52]

Morocco is seeking new pathways to develop and retain its highly skilled professionals (e.g., IT and medicine). In the 1980s, Morocco moved away from the French educational system and embraced a classical approach. Today, there is discussion of using English as the primary language at the university level, recognizing that English is the preferred language of research.[53] Yet, the Moroccan government has not developed a formal program or set of incentives (e.g., grants or scholarships) to accelerate cyber security education programs or incubate basic and applied cyber security research initiatives at universities and academic institutions. However, some of the scientific and technical schools and universities in Morocco have started to integrate courses in cyber security into their computer science programs and other curricula to meet the growing demand for a national-level professional workforce. There are even some certificate and degree programs emerging. For example, Al Akhawayn University offers a cyber security certificate program and the International University of Rabat created a master's program in cyber security.

The government did recognize that it also needed to update the skills of its workforce and train information systems managers in cyber security. Therefore, the ANRT has started funding an executive master's program in cyber security at the National Institute of Posts and Telecommunications (*Institut National des Postes et Télécommunications*, INPT) for public sector employees with the support of DGSSI,[54] and the Bureau of Professional Training and Employment Promotion (*Office de la Formation Professionnelle et de la Promotion du Travail*, OFPPT) created a training academy dedicated to promoting mid-career professional skills development in IT and information security.[55] It also approved a national (and sector specific) cyber security framework for the certification and accreditation of national agencies and public sector professionals. The framework is called the Project of professional master for training and certification of professionals in the public sector.

In February 2016, the Moroccan Ministry of Industry, Commerce, Investment and Digital, in partnership with Moroccan universities, public and private organizations, launched the "National Campaign to Fight Cybercrime." This initiative, led by the Moroccan Centre for Polytechnic Research and Innovation (CMRPI) in Rabat, is an annual campaign designed to increase private sector awareness about cyber crime and promote security in society's use of technology by incorporating international best practices.[56] The campaign is the first of its kind and scale in Africa – incorporating seminars, training workshops specifically designed for Moroccan public and private sector organizations, and hosting a national symposia on cyber security and cyber crime. In addition, DGSSI organizes a large annual national seminar to raise awareness across the Ministries.

In April 2018, the country partnered with Trend Micro to host the Morocco National Cybersecurity Competition (CTF) with the intention of attracting more people into the field of cyber security. The winners of the competition would represent Morocco in the Arab Regional Cybersecurity competition that took place in Egypt in August 2018. The CTF was a Jeopardy-style CTF where every team was presented with a list of challenges in different technical categories like reverse engineering, web security, digital forensics, network security, etc. The teams that could both attack and defend were rewarded with advancement to the next level of competition.

Morocco has made progress toward achieving the goals set forth in their digital strategies. The initiatives launched in recent years to encourage entrepreneurship, boost the development of starts-up companies through the technology parks, and promote cyber security education and training are important and are helping to attract foreign investment, further positioning Morocco as a strategic partner in the MENA region. Morocco, however, is also experiencing a "brain drain" as many highly skilled professionals, including ICT experts, decide to leave the country to find better opportunities abroad. Therefore, the country must focus on the development and retention of technical talent to fuel the growth of its digital economy. In 2018, less than 20 percent of Moroccan students pursued technical subjects at the university level. Perhaps as the Moroccan government demonstrates its leadership in fielding the first high-speed rail line in Africa — connecting the economic hubs of Tangier and Casablanca — it can also set a priority toward closing the talent gap.

## 6. DIPLOMACY AND TRADE

Morocco does not consider cyber security a top tier foreign policy issue and has not prioritized this area within its Ministry of Foreign Affairs and Cooperation. However, Morocco has identified ICT and cyber security as important elements of its national security and economic prosperity, including in international trade and commerce negotiations, and is assuming a more prominent role in promoting regional cyber security cooperation and awareness. As part of these efforts, Morocco regularly hosts cyber security-related events for the World Bank, ITU, and NATO's Science for Peace and Security (SPS) Program. Additionally, the Moroccan Ministry of Foreign Affairs – Diplomatic Academy provides training to partner countries including Benin, Central African Republic, Chad, Gabon, Guinea, and Madagascar.

Morocco has also been involved in a number of high-level dialogues with European countries, the U.S., and members of the Gulf Cooperation Council (GCC) on security issues, counter-terrorism operations, and the use of cyberspace by terrorist and other criminal groups. Its strategic value, not only for its location between Europe and Africa, but also for its importance within the Maghreb area and ties to the greater Arab world, makes it a key security partner in the region. Moroccan agencies and their European counterparts, especially in Spain and France, regularly cooperate and exchange information and best practices on security issues, including cyber security, and consider Morocco their most reliable ally in the area.[57]

*Morocco is assuming a more prominent role in promoting regional cyber security cooperation and awareness, but has not prioritized cyber security as a top tier foreign policy issue within its Ministry of Foreign Affairs.*

The Digital Morocco 2020 strategy emphasizes Morocco's strategic location as a regional digital hub and gateway to Africa. The Moroccan government should use the country's key position in the region to further promote the free flow of goods, services, data, and capital across borders. Cyber diplomacy is not just about rules of engagement and constraining behaviors, it is also about promoting trade through the free flow of information. Balancing the twin goals of economic prosperity and national security requires a sophisticated diplomatic corps and a commitment to leading the region to realize the Digital Morocco 2020's vision and goals.

## 7. DEFENSE AND CRISIS RESPONSE

The Kingdom of Morocco plays a crucial role in maintaining security and stability in the northern African region and works closely with European countries, the U.S., and members of the GCC on security issues and counter-terrorism operations. The security dilemmas facing this region are abundant. There is a growing influence – albeit weakened – of Daesh (one of the terrorist organizations affiliated with the Islamic State group) and other terrorist organizations. There have been connections to North African terrorists who have carried out attacks within Europe. The region continues to be plagued by Libya's collapsing economy and local militias competing for power. Algeria is viewed as a threat to Morocco's stability as it is not governing its western and southern borders and is destabilizing the Sahel and sub-Saharan region. Therefore, U.S., European countries, and the GCC have a strong interest in understanding security threats that emanate from North Africa and in working with North African countries to address them. In particular, Morocco's relative political stability, economic development, and regional integration in Africa and the Middle East has made the country one of Europe and U.S.' key security partners in the region.[58]

Morocco is also working with NATO, as part of the "Mediterranean Dialogue," to explore cooperation in cyber defense, notably through the exchange of expertise and training,[59] and it participates in several exercises with international partners, including the Mediterranean Naval Exercise called "Phoenix Express." This exercise is designed to improve regional cooperation, increase maritime domain awareness, information-sharing practices, and operational capabilities in order to enhance efforts to promote safety and security in the Mediterranean Sea. Moreover, Morocco has been hosting the annual joint military exercise "African Lion" since at least 2005. This is the largest (land) regional exercise in the area and in 2018 it involved 15 countries, including Burkina Faso, Canada, Chad, Egypt, France, Germany, Italy, Mali, Mauritania, Senegal, Spain, Tunisia, the U.K., and the U.S. This exercise was designed to improve the interoperability and mutual understanding of each nation's tactics, techniques, and procedures, and it plans to incorporate cyber security injects and planning in future iterations.

Although Morocco has developed several cyber-related capabilities, there is no evidence that it has formalized the military or the intelligence services' cyber security mission in a policy or decree. The Royal Moroccan Armed Forces (FAR) is responsible for overseeing the development of cyber security and cyber defense capabilities and for ensuring the resilience and availability of the country's military operational networks (i.e., air defense, air surveillance, ground surveillance, and special communications). It is also responsible for securing the networks and exchange of data among the three military components (i.e., army, navy, and air force). While its top mission is border security — tracking sub-Saharan illegal immigrants, terrorist movement, and drug movement, it is unclear whether the FAR has a broader cyber mandate for the country or if it would be mobilized to restore services if Morocco faced a digital national crisis. FAR reports directly to the King — its Supreme Commander and Chief of General Staff — and views its responsibilities and capabilities as distinctive from those of DGSSI.

The FAR recently created a Cyber Center of Excellence. It reports to the FAR's Communications and Information Systems Protection Entity and is responsible for multiple initiatives. It designs and executes at least two cyber defense exercises annually and provides technical support and incident response services. It is also charged with R&D and is currently working on the development of new applications that will support the SOCs.

*The Royal Moroccan Armed Forces (FAR) is responsible for overseeing the development of cyber security and cyber defense capabilities and for ensuring the resilience and availability of the country's military operational networks.*

The Royal Military Education College of Morocco (CREMS) — Morocco's higher education institute for its military officers — has started to include lectures on cyber security and cyber defense in their curricula. CREMS is also working to incorporate cyber exercises into their Joint Theatre Level Simulation (JTLS). Currently, their cyber education is limited to tactical level planning and has yet to expand to broader cyber defense/security issues at the strategic and operational levels.

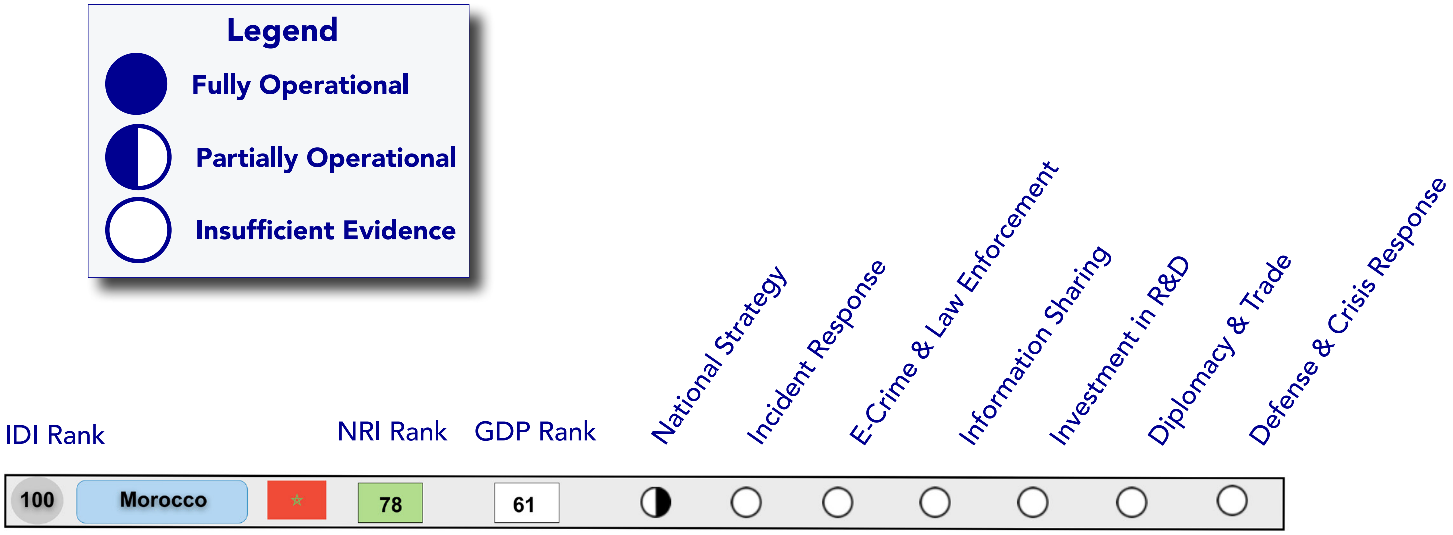
It is difficult to determine the level of funding dedicated to further developing cyber capabilities within Morocco's military or intelligence services because the budget is not publicly available. However, the country is credited with operating a tight and effective security program through an extensive network of security officials, informants, and advanced signal intelligence including preemptive digital surveillance techniques and monitoring of digital platforms for signs of radicalization and terrorism. For example, the DGSSI is responsible for securing and monitoring cyber traffic and web activities.[60] In November 2017, Morocco became the first

North African country to launch a high-resolution surveillance satellite (named after King Mohammed VI) that is capable of providing multi-purpose images.[61] In November 2018, Morocco launched a second satellite (named Mohammed VI B) that aims to provide Morocco with a more robust capability to gather intelligence, monitor its borders, map land and survey activities, prevent and manage natural disasters, and monitor environmental changes and desertification.[62]

## CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, Morocco is still in the early stages of developing a path toward cyber resilience and cyber readiness, and is currently partially operational only in one of the seven CRI essential elements. The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As Morocco continues to implement its Digital Agenda 2020, empowers DGSSI to address the nation's security, and aligns its national economic vision with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path toward a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. The CRI 2.0 methodology is available in Arabic, Chinese, English, French, Russian, and Spanish. The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.*



**Legend**

● Fully Operational

◐ Partially Operational

○ Insufficient Evidence

| IDI Rank | | | NRI Rank | GDP Rank | National Strategy | Incident Response | E-Crime & Law Enforcement | Information Sharing | Investment in R&D | Diplomacy & Trade | Defense & Crisis Response |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 100 | Morocco | 🟥 | 78 | 61 | ◐ | ○ | ○ | ○ | ○ | ○ | ○ |

## ENDNOTES

1. USAID, "USAID Leland Initiative," *https://web.archive.org/web/20011109164754/http:/www.usaid.gov/leland/*.

2. MTDS, "About MTDS," *https://www.mtds.com/about-us/*.

3. Rachid Amaoui, "L'opérateur Maroc Telecom," *https://www.tic-maroc.com/p/maroc-telecom.html*.

4. World Bank, "Individuals using the Internet (% of population)," 2016, *https://data.worldbank.org/indicator/IT.NET.USER.ZS*.

5. World Bank, "Kingdom of Morocco: Governing Towards Efficiency, Equity, Education and Endurance," June 2018: 20.

6. Oxford Business Group, "New plan and updated legislation provide a boost for Morocco's IT sector," *https://oxfordbusinessgroup.com/overview/building-new-plan-and-updated-legislation-have-provided-boost-0*.

7. Ibid.

8. Kingdom of Morocco, "Digital Morocco 2013," *https://www.ccdcoe.org/sites/default/files/strategy/Maroc_Cyber security_2013_ENG.pdf*.

9. Ibid.

10. Maroc Cour des Comptes, "Assessment of 'Digital Morocco 2013' Strategy," February 2014, *http://www.courdescomptes.ma/upload/MoDUle_20/File_20_418.pdf*.

11. Ministry of Industry, Trade, Investment and of the Digital Economy, "Stratégie Maroc Digital 2020," UNESCO, *https://en.unesco.org/creativity/periodic-reports/measures/strategie-maroc-digital-2020*.

12. "The Development of Morocco's IT Sector," *Info Mineo*, 27 February 2017, *https://infomineo.com/the-development-of-moroccos-it-sector-2/*.

13. Ibid.

14. Chris Kelly, "Orange launches cyber security centre in Morocco," *Total Telecom*, 29 October 2018, *https://www.totaltele.com/501453/Orange-launches-cyber-security-centre-in-Morocco*.

15. McKinsey Global Institute, "Lions go digital: The Internet's transformative potential in Africa," (November 2013): 4, 22, *https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/Lions%20go%20digital%20The%20Internets%20transformative%20potential%20in%20Africa/MGI_Lions_go_digital_Full_report_Nov2013.ashx*.

16. "Casanearshore," Med Sourcing, *https://www.medz-sourcing.com/en/our-parks/casanearshore-park-outsourcing-offshoring-casablanca-morocco.html*.

17. "Rabat Technopolis," Med Sourcing, *https://www.medz-sourcing.com/en/our-parks/technopolis-rabat-offshore-activities-morooco.html*.

18. "Morocco to launch Chinese industrial city in Tangiers," *Afri-*

*ca News*, 21 March 2017, *http://www.africanews.com/2017/03/21/morocco-to-launch-chinese-industrial-city-in-tangiers//*.

19. Kingdom of Morocco, "Digital Morocco 2013."

20. Kingdom of Morocco, General Directorate of Information Systems, "Stratégie nationale en matière de cybersécurité," 5 December 2012, *https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf*.

21. Kingdom of Morocco, General Directorate of Information Systems, "Directive Nationale de la Sécurité des Systèmes d'Information," *https://www.dgssi.gov.ma/fr/node/33.html*.

22. Ibid.

23. Sophia Akhmisse, "Le Maroc déjoue des cyberattaques di régime Algérien," *Le 360*, 12 November 2013, *http://fr.le360.ma/politique/le-maroc-dejoue-des-cyberattaques-du-regime-algerien-5787*.

24. Youssef Bentaleb, "Fighting Cybercrime in Morocco: Achievements and Some Challenges," Moroccan Centre for Polytechnic Research and Innovation, 9 January 2017, *https://observatoire-fic.com/en/fighting-cybercrime-in-morocco-achievements-and-some-challenges-by-prof-youssef-bentaleb-moroccan-centre-for-polytechnic-research-and-innovation/*.

25. "Morocco's Tanger-Med port running at full steam," *News 24*, 4 April 2018, *https://www.news24.com/Africa/News/moroccos-tanger-med-port-running-at-full-speed-20180404*.

26. Kingdom of Morocco, "Stratégie nationale en matière de cybersécurité," 3.

27. Kingdom of Morocco, "Directive Nationale de la Sécurité des Systèmes d'Information."

28. Ibid.

29. Interview with Maj. Chergaoui Mouhssine, Forces Armées Royales (FAR), 7 December 2018.

30. Phoebe Parke and Chris Giles, "Morocco's megawatt solar plant powers up," 17 May 2018, *https://www.cnn.com/2016/02/08/africa/ouarzazate-morocco-solar-plant/index.html*.

31. Kingdom of Morocco, "Digital Morocco 2013," 86.

32. Interview with Marco Obiso, International Telecommunication Union, Head of ICT Applications and Cybersecurity Division, 19 November 2018.

33. Anthony Dworking and Fatim-Zohra El Malki, "The Southern front line: EU counter-terrorism cooperation with Tunisia and Morocco," *European Council on Foreign Relations*, 15 February 2018, *https://www.ecfr.eu/publications/summary/the_southern_front_line_eu_counter_terrorism_cooperation*.

34. Kingdom of Morocco, General Directorate of Information Systems,

"Directive Nationale de la Sécurité des Systèmes d'Information."

35. In addition to the specific security standards and requirements established by DGSSI that the financial sector must meet, the Central Bank of Morocco (Bank Al Maghreb) has regulatory power over other banks in regards to different aspects including cyber security.

36. Kingdom of Morocco, General Directorate of Information Systems, "Directive fixant les règles de sécurité et les modalités de déclaration des systèmes d'information sensibles et des incidents de sécurité applicables aux infrastructures d'importance vitale," *https://www.dgssi.gov.ma/fr/node/32.html*.

37. Ibid.

38. "State of Privacy Morocco," *Privacy International*, January 2018, *https://privacyinternational.org/state-privacy/1007/state-privacy-morocco*.

39. Council of Europe Deputy Secretary General, "Morocco joins the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism," Council of Europe, 29 June 2018, *https://www.coe.int/en/web/deputy-secretary-general/-/morocco-joins-the-budapest-convention-on-cybercrime-and-its-protocol-on-xenophobia-and-racism*.

40. Morocco's Law No 09-08 relating to the protection of individuals with regard to the processing of personal data and its implementation, Decree n° 2-09-165 of 21 May 2009.

41. Sextortion is defined as a form of sexual exploitation wherein its perpetrators, usually through non-physical forms of coercion such as the Internet, extort money from their victims by threatening to share their intimate photos and videos if they do not pay up. Thousands of 'sextortionists' are believed to be living and operating out of the city of Oued Zem, which has at least fifty money transfer agencies.

42. "State of Privacy Morocco," *Privacy International*.

43. Anthony Dworking and Fatim-Zohra El Malki, "The Southern front line: EU counter-terrorism cooperation with Tunisia and Morocco."

44. OIC-CERT, *https://www.oic-cert.org/en/index.html*.

45. "EDU-CERT," *https://www.educert.ma/index.php/*.

46. Kingdom of Morocco, "Digital Morocco 2013."

47. Ministry of Industry, Trade, Investment and of the Digital Economy, "Stratégie Maroc Digital 2020."

48. McKinsey Global Institute, "Lions go digital: The Internet's transformative potential in Africa," 64.

49. Oxford Business Group, "New plan and updated legislation provide a boost for Morocco's IT sector."

50. "Morocco – Pioneering Economic Growth," *Foreign Affairs*, November-December 2015: 11.

51. HPS, "Enabling Innovative Payments," *https://www.hps-worldwide.com*.

52. Chris Kelly, "Orange launches cyber security centre in Morocco," *Total Telecom*, 29 October 2018, *https://www.totaltele.com/501453/Orange-launches-cyber-security-centre-in-Morocco*.

53. Mohamed Chtatou, "A Moroccan success story tainted with some shortcoming," UNESCO (2015), *http://unesdoc.unesco.org/images/0023/002324/232463e.pdf*.

54. INPT, "Mastère Spécialisé en Technologies du Web et Cyber Sécurité," *https://www.inpt.ac.ma/fr/technologies-du-web-et-cyber-sécurité*.

55. OFPPT, "Offre de formation: Technologies de l'Information," *http://www.ofppt.ma/index.php/offre-de-formation2/secteurs-de-formation/27-technologies-de-l-information*.

56. Ministry of Industry, Trade, Investment and of the Digital Economy, "Cyber Security: National Campaign to Fight Cybercrime," *http://www.mcinet.gov.ma/en/content/cyber-security-national-campaign-fight-cybercrime*.

57. David Hernádez Martínez, "Morocco and the GCC: between Saudi Arabia and Qatar," *The London School of Economics and Political Science*, 25 September 2017, *http://blogs.lse.ac.uk/mec/2017/09/25/morocco-inside-the-gcc-between-saudi-arabia-and-qatar/*.

58. Anthony Dworking and Fatim-Zohra El Malki, "The Souther front line: EU counter-terrorism cooperation with Tunisia and Morocco," *European Council on Foreign Relations*.

59. "Morocco, NATO to Cooperate in Countering Cyber Security Risks," *The North Africa Post*, May 18, 2017, *http://northafricapost.com/17912-morocco-nato-cooperate-countering-cyber-security-risks.html*.

60. Kingdom of Morocco, General Directorate of Information Systems, "Stratégie nationale en matière de cybersécurité" (2013).

61. Ghalia Kadiri, "Satellite marocain en orbite: un lancement secret qui inquiète", *Le Monde*, 19 November 2017, *http://www.lemonde.fr/afrique/article/2017/11/19/satellite-marocain-en-orbite-un-lancement-secret-qui-inquiete_5217299_3212.html*.

62. "Morocco to foster Earth observation capabilities with second satellite," *The North Africa Post*, 26 September 2018, *http://northafricapost.com/25552-morocco-to-foster-earth-observation-capabilities-with-second-satellite.html*.

# ABOUT THE AUTHORS

**Melissa Hathaway** is a leading expert in cyberspace policy and cyber security. She served in two US presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. Today, she is a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies. She is also a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, a Distinguished Fellow at the Centre for International Governance Innovation in Canada, a non-resident Research Fellow at the Kosciuszko Institute in Poland, and she is President of Hathaway Global Strategies LLC, her own consultancy. Melissa developed a unique methodology for evaluating and measuring national levels of preparedness for certain cyber security risks, known as the Cyber Readiness Index (CRI). The CRI methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is being applied to 125 countries. The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index*. Having served on the board of directors for two public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field. She publishes regularly on cyber security matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html*.

**Francesca Spidalieri** Francesca Spidalieri is the co-principal investigator on the Cyber Readiness Index Project at the Potomac Institute for Policy Studies. She is also an Associate for Hathaway Global Strategies LLC, and serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, as a cyber security subject-matter expert for the UN International Telecommunications Union (ITU), and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, comparative organization analysis, and cyber security workforce development. In 2015, she published a report, entitled State of the States on Cybersecurity, that applied the Cyber Readiness Index 1.0 at the US state level. All her additional studies and academic articles can be found at the following link: *http://pellcenter.org/cyber-leadership/*.

*For more information or to provide data to the CRI 2.0 methodology, please contact:*

*CyberReadinessIndex2.0@potomacinstitute.org*

*The CRI 2.0 methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is currently being applied to 125 countries.*

*The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States can be found at the following link:*

*http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.*

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
*www.potomacinstitute.org*