euromesco
Policy Study

N. 22

GREAT EXPECTATIONS: DEFINING A TRANS-MEDITERRANEAN CYBERSECURITY AGENDA

Patryk Pawlak
Coordinator

Adel Abdel-Sadek

Samuele Dominioni

Alexandra Marion Youmna Laban

IEMed.
European Institute of the Mediterranean

euromesco
Policy Study

N. 22

GREAT EXPECTATIONS: DEFINING A TRANS-MEDITERRANEAN CYBERSECURITY AGENDA

Patryk Pawlak
Coordinator

Adel Abdel-Sadek

Samuele Dominioni

Alexandra Marion Youmna Laban

IEMed.
European Institute of the Mediterranean

euromesco
research dialogue advocacy

EuroMeSCo has become a benchmark for policy-oriented research on issues related to Euro-Mediterranean cooperation, in particular economic development, security and migration. With 104 affiliated think tanks and institutions and about 500 experts from 29 different countries, the network has developed impactful tools for the benefit of its members and a larger community of stakeholders in the Euro-Mediterranean region.

Through a wide range of publications, surveys, events, training activities, audio-visual materials and a strong footprint on social media, the network reaches thousands of experts, think tankers, researchers, policy-makers and civil society and business stakeholders every year. While doing so, EuroMeSCo is strongly engaged in streamlining genuine joint research involving both European and Southern Mediterranean experts, encouraging exchanges between them and ultimately promoting Euro-Mediterranean integration. All the activities share an overall commitment to fostering youth participation and ensuring gender equality in the Euro-Mediterranean experts' community.

EuroMesCo: Connecting the Dots is a project co-funded by the European Union (EU) and the European Institute of the Mediterranean (IEMed) that is implemented in the framework of the EuroMeSCo network.

As part of this project, five Joint Study Groups are assembled each year to carry out evidence-based and policy-oriented research. The topics of the five study groups are defined through a thorough process of policy consultations designed to identify policy-relevant themes. Each Study Group involves a Coordinator and a team of authors who work towards the publication of a Policy Study which is printed, disseminated through different channels and events, and accompanied by audio-visual materials.

POLICY STUDY

Published by the European Institute of the Mediterranean

Peer Review
Academic Peer Reviewer: anonymous

Editing
Karina Melkonian

Design layout Maurin.studio
Proofreading Neil Charlton
Layout Núria Esparza
Print ISSN 2462-4500
Digital ISSN 2462-4519
July 2021
Arabic version available

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union or the European Institute of the Mediterranean.

IEMed.
European Institute of the Mediterranean

The **European Institute of the Mediterranean** (IEMed), founded in 1989, is a think and do tank specialised in Euro-Mediterranean relations. It provides policy-oriented and evidence-based research underpinned by a genuine Euromed multidimensional and inclusive approach.

The aim of the IEMed, in accordance with the principles of the Euro-Mediterranean Partnership (EMP), the European Neighbourhood Policy (ENP) and the Union for the Mediterranean (UfM), is to stimulate reflection and action that contribute to mutual understanding, exchange and cooperation between the different Mediterranean countries, societies and cultures, and to promote the progressive construction of a space of peace and stability, shared prosperity and dialogue between cultures and civilisations in the Mediterranean.

The IEMed is a consortium comprising the Catalan Government, the Spanish Ministry of Foreign Affairs, European Union and Cooperation, the European Union and Barcelona City Council. It also incorporates civil society through its Board of Trustees and its Advisory Council.

euromesco
Policy Study

Content

Executive Summary

European Union (EU) cooperation on cybersecurity with the Middle East and North Africa (MENA) region is conditioned by two competing claims. Due to the geographical proximity and broad security implications for the EU, the MENA region is one of the priorities of the EU's external relations. Over the past two decades, and especially after the Arab Spring, the EU has invested significant resources to support the reforms in the region and align its policies with its own. At the same time, however, this ambition to cooperate closely with the region is often made more complicated by the situation on the ground. This is particularly the case of cyber resilience cooperation, where even despite overlapping interests – like the fight against cybercrime or improving the overall level of cybersecurity – the EU needs to exercise enhanced due diligence in order to avoid undermining the already fragile human rights protection in some of those countries. Reconciling these two elements – the willingness to engage in closer cooperation and the need for a cautious approach to cybersecurity cooperation – remains the key challenge.

Against this background, the study aims to address two questions. First, to what extent are different initiatives and policies implemented across the region compatible with the EU's own interests and values? Second, who are the key multipliers on cybersecurity in the region that could potentially align with the EU in certain aspects and help it achieve its policy objectives? Which of these relationships are mature enough or require further work in order to turn into concrete cooperation initiatives? These two sets of questions guide the discussion in each of the chapters.

Alexandra M. Y. Laban addresses the issue of **digital economy and cybercrime.** Cyberattacks, intellectual property theft facilitated by digitisation, online fraud, and financial manipulation pose a threat to the digital economy and require an agile and speedy response from public authorities. The challenge for the MENA region is not only to carve out a place for itself in this new global economy but also to modernise its public institutions to face the new threats in cyberspace. In addition to presenting general trends, the first chapter scrutinises the involvement of the MENA countries in the regional and global debates about the international cooperation against cybercrime (e.g., the Budapest Convention, the United Nations [UN], regional initiatives) as well as offering recommendations for the EU's engagement with the MENA region. The chapter looks in particular at the situation in Algeria, Lebanon and Morocco.

Samuele Dominioni looks at the challenge of cyber resilience more from the societal perspective and analyses the link between a **double challenge of digital and democratic transition** across the region. His chapter addresses how the Internet Governance model has an impact on regime transition/consolidation in the MENA region. The second chapter argues that the lack of a shared understanding and common principles for the governance of cyberspace allows countries to adopt different policies at the domestic level. In particular, the chapter analyses how and to what extent policies aimed at curbing disinformation are used for crushing political dissent and limiting external influence in cyberspace. The chapter looks at different solutions adopted in Egypt, Morocco and Jordan.

Finally, Patryk Pawlak looks at the broader question of **preventing conflict and promoting responsible state behaviour in cyberspace.** The last chapter analyses how the increasing geopolitical competition in cyberspace impacts the region's stability. Countries like Israel, Iran and Turkey regularly use cyber operations in support of their political objectives. In addition, the involvement of the military forces of the United States of America (USA) and the expanding presence of actors like China and Russia in the region complicates the situation further. If anything, cyber-related developments in the region illustrate very well that cyberspace is just one additional domain for pursuing political and economic objectives, in particular in the context of a pre-existing conflict. Yet, with the exception of Egypt and Iran, the majority of countries in the region are rather absent from the international debates aimed at strengthening the stability of cyberspace.

Consequently, the analysis presented in this study leads to four main observations:

- **Tension between state and societal resilience.** While building state and societal resilience is one of the EU's objectives, in the MENA region these two concepts often clash: resilient society is perceived by some governments as a threat to their rule rather than an empowering element. For the EU to engage in a meaningful partnership with the region on cyber and digital policies, this tension needs to be better understood and addressed through adequate risk mitigation strategies.

- **International cooperation against cybercrime.** Cybercrime is one of the key priorities for the international cooperation highlighted in the *EU 2020-*

2025 Security Union Strategy. In addition, cybercrime is also one of the threats to trust in digital society and economy, which the EU puts as one of the priorities for its growth. Similar concerns are present in the MENA region; hence there is a solid basis for dialogue on those issues. However, the lack of proper human rights protection mechanisms and checks and balances in some of the countries in the region is still a serious impediment to closer cooperation.

- **Stability and responsible behaviour in cyberspace.** Through activities at the UN and in other regional organisations, the EU has advanced norms of state behaviour in cyberspace, the adherence to the existing international law, and the confidence-building measures (CBMs) in cyberspace. However, the engagement on these topics with the MENA region is to a large extent non-existent and should be strengthened to promote the EU's vision of cyberspace.

- **Role of non-state actors in strengthening cyber resilience.** Participation of non-state actors – civil society and the private sector – is critical for the effective and sustainable digital transition. Although strengthening multistakeholder engagement on cyber issues across the region could ultimately help to bridge the differences between societal and state resilience across the region, MENA countries have been reluctant to engage in such cooperation and access to the policy-making process has been limited.

The study makes a number of policy recommendations for strengthening cooperation between the EU and its partners across the Mediterranean along two main axes: policies and cooperation mechanisms.

Policies

- Enhance cyber hygiene and cyber awareness policies in the region through campaigns, exercises, cyber drills, and cybersecurity competitions.

- Pursue a more robust political dialogue between the EU and partners in the region regarding their positions on key cyber diplomacy issues, in particular the application of the existing international law on cyberspace and norms of responsible state behaviour.

- Define what type of resilience to promote in the region while remaining mindful of a possible trade-off between regime and societal resilience.

- Minimise the risk of cyber capacity-building projects being used for increased surveillance, censorship, and other information control capabilities.

- Strengthen cooperation between regional organisations to develop and implement region-specific CBMs with the aim of creating a demilitarised cyber-zone.

Cooperation mechanisms

- Create mechanisms for better data collection to assess the risks of cybercrime across the region, including by building on the already existing projects.

- Foster inclusive participation of the private sector and civil society in cyber policy formulation and monitoring. In that sense, the EU needs to play particularly close attention to creating opportunities and channels for a more inclusive multistakeholder participation.

- Reinforce MENA capacities through existing networks across the whole range of issues by building on the existing channels of communication to mutualise and enhance intra-regional know-how and replicate the efforts.

- Strengthen collaborations with countries that are still hesitant about their policy preferences regarding international cyberspace norms.

Introduction

Patryk Pawlak
Brussels Executive Officer, European
Union Institute for Security Studies (EUISS)

Strengthening state and societal resilience is one of the key objectives of the European Union (EU) Global Strategy that is reflected in the EU's thematic and regional policies. This also includes cooperation on issues such as cybersecurity and cybercrime with countries in the Middle East and North Africa (MENA) region. As an increasing number of the partner countries embark on or continue with the process of digital transition, the EU's collective experience in this domain – both at the EU and member state level – can be of value for countries that often struggle with similar challenges and policy choices.

Acknowledging different levels of economic development and taking into account their respective institutional, regulatory or societal make-up, the EU can be a valuable partner for the countries in the MENA region and offer the necessary support in the process of transitioning towards becoming **cyber resilient, rules- and rights-based digital societies.** At the same time, cooperation with MENA countries on cyber resilience, cybercrime, digital economy and responsible behaviour in cyberspace is critical for achieving the common objective of free, open, secure and stable cyberspace. A new Agenda for the Mediterranean unveiled in February 2021 aims for a "green, digital, resilient and just recovery" based on the assumption that "sustainable prosperity and resilience can only be built in strong partnership across the Mediterranean."

The region is torn by disparities when it comes to the degree of digitalisation and connectivity (World Bank, 2014). According to the Global System for Mobile Communications (GSMA)'s Global Mobile Connectivity Index, the highest scoring countries in the region are Israel, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates. Several other countries in the Southern Mediterranean also experienced high growth in connectivity between 2014 and 2018, including Tunisia, Morocco and Turkey (GSMA, 2019). The reasons for the region falling behind in the development of broadband networks, Internet access and use, and creation of digital content have for a long time been partly structural (i.e., infrastructure, cost, regulation) and partly political: political elites across the region feared that democratising Internet access will undermine state control over information (HRW, 1999). This tendency has been reversed in the past decade following the push from the business and research communities that stressed the value of digital transformation for their countries' economic growth, competitiveness and democratic transition. As connectivity across the region is improving, governments invest in building their capacities, and several countries actively participate in the ongoing international debates on responsible behaviour in cyberspace (e.g., Egypt, Jordan, Morocco, Tunisia) or the future of international cybercrime cooperation (e.g., Jordan, Lebanon, Morocco, Tunisia).

These processes, however, are vulnerable to the same forces as the rest of the world: cybercrime, attacks on the critical infrastructure (CI), malicious activities by state and non-state actors, as well as potential abuses of civil liberties and human rights as a consequence of ill-designed state policies. However, **the situation in the region is particularly sensitive given the still fragile nature of the transition processes that these countries undergo: digital, economic, political**

and societal. A failure of governance in and of cyberspace in the MENA region could potentially undermine these efforts and contribute to further instability. The lack of adequate legislation and robust institutions to ensure safe and secure operation of the CI might result in their failure, slow down the economic transition, further accentuate governing challenges, strengthen anti-government sentiments and consequently lead to social unrest. Even a perceived effort to manipulate or influence electoral processes in the region or government policies imposing limitations on citizens' rights online might undermine the legitimacy of such processes and fuel discontent. Finally, the strategic interest in the Southern Mediterranean exhibited by other regional and external players – through increasing their economic presence, investment in infrastructure or even state-sponsored cyber operations – adds to this complexity. Consequently, the EU's engagement with the MENA countries needs to be constructed by recognising these different realities and dynamics.

References

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSMA). (2019). Mobile Internet connectivity 2019. *Middle East and North Africa factsheet.* Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/09/Mobile-Internet-Connectivity-MENA-Fact-Sheet.pdf

HUMAN RIGHTS WATCH (HRW). (1999). The Internet in the Middle East and North Africa: a cautious start. In *The Internet in the Mideast and North Africa: free expression and censorship.* Retrieved from https://www.hrw.org/legacy/advocacy/internet/mena/int-mena.htm

WORLD BANK. (2014). *Broadband networks in the Middle East and North Africa: key facts.* Retrieved from https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/MNA_Broadband_Key_Facts_English.pdf

Digital Economy and Cybercrime

Alexandra Marion Youmna Laban
Project Manager, Société Française de
Réalisation, d'Etudes et de Conseil (SOFRECO)

Introduction

Access to the digital economy – both in terms of infrastructure and policy instruments – is a prerequisite to reaping its economic and developmental benefits. The Middle East and North Africa (MENA) region is well positioned to become a digital economy powerhouse (UNESCWA, 2019a) due to its 400 million inhabitants, the educated and young workforce, access to natural resources, a relatively homogeneous language, and a privileged geographical position. As of April 2019, the Internet penetration in the MENA was 67.2% (Statista, 2019) – more than double compared to just a decade ago. In addition, the digital economy and the Fourth Industrial Revolution in the MENA region brought a leap in productivity with the expanding use of advanced robotics and manufacturing techniques.

However, the reliance of a non-negligible portion of the economy on Internet-based platforms is accompanied by new types of criminal activity that have pervaded this new economic segment. Although there is no universally agreed definition of cybercrime, for the purpose of this chapter cybercrime refers to criminal activities where computers and information systems are involved either as a primary tool or as a primary target (EU Cyber Direct, 2020). It impedes online economic growth, costing about €530 billion globally (Latici, 2019), while threatening the security of citizens, businesses and states and breeding distrust in digital services. By nature, cybercrime is a cross-border challenge, which requires international cooperation to contain the uncontrolled criminal activity growth, as well as robust domestic legislation and enhanced capacities to identify and prosecute cyber criminals (EU Cyber Direct, 2020).

This chapter looks at the evolution and impact of cybercrime in the MENA region, which has adapted impressively to new technologies and, at the same time, has become exposed to new crimes in the same way as other parts of the world. Despite the diversity across the region regarding the exposure to cybercrime and maturity to deal with this challenge, this chapter offers some conclusions regarding past and ongoing cooperation activities in the field of cybercrime in the MENA region funded by the European Union (EU), in particular the European Neighbourhood and Partnership Instrument (V. Spidiron, C-PROC, personal communication, November 20, 2020; M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020). While the primary focus of the chapter is on Algeria, Lebanon and Morocco, other MENA countries are also actively engaged in the fight against cybercrime, including Jordan, Tunisia and the Gulf Cooperation Council (GCC) countries. Four policy recommendations targeted at national and EU policy-makers conclude the chapter and inform on the next steps of EU-MENA cybercrime cooperation. The conclusions of this chapter are based on interviews with experts conducted between November 2020 and February 2021.

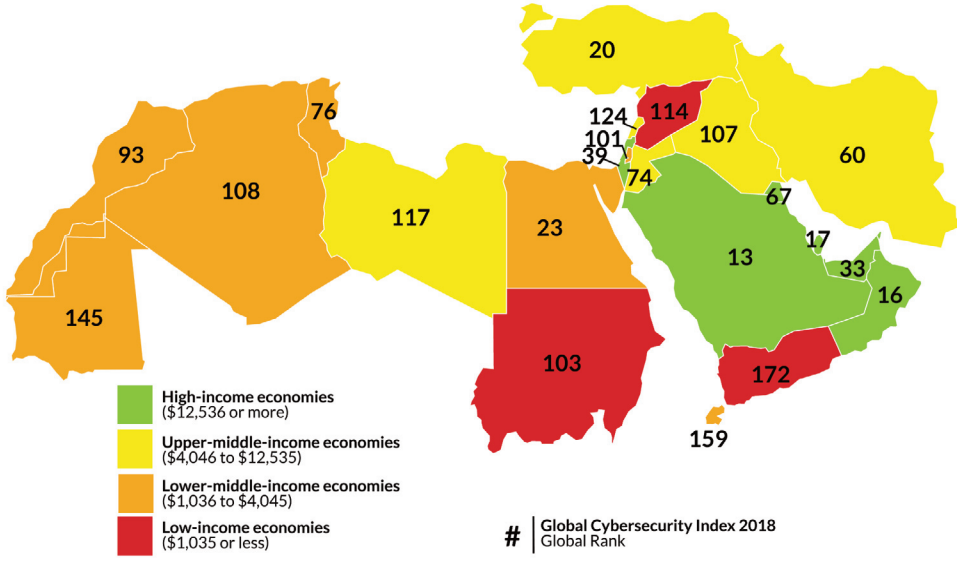
Cybercrime: impediment to growth, threat to stability

Economic development is generally defined as the process that promotes the improvement of a region's economic well-being and quality of life by

providing high living standards and high-quality employment. Developing the MENA region's economy is one of the key conditions for its stability. It brings highly heterogeneous countries in economic and cybersecurity terms (see figure 1 below) and has, for decades, suffered from a high proportion of autocratic regimes, high youth and women's unemployment rates, high levels of government employment and inflated subsidy systems, and heavy reliance on volatile rent revenues (oil and gas commodities, as well as tourism and diasporic remittances) (Gaub, 2019; Belhaj, 2021). This bleak socio-economic situation is complemented by a chronic state of social unrest and violence, epitomised by ongoing conflicts, sectarianism, irregular migration, radicalisation, large weapon purchases, geopolitical rivalries, and overreliance on state repression (Youssef et al., 2020). Besides, regional stability is weakened by the absence of security structures, which, in turn, threatens to make the MENA region prone to perennial conflict, including in cyberspace.

Regional stability is weakened by the absence of security structures, which, in turn, threatens to make the MENA region prone to perennial conflict, including in cyberspace

Figure 1. Selected Economic Indicators



Sources: World Bank (2019); ITU (2018).

In 2017, the unclassified version of the Euro-Mediterranean Police Threat Assessment (EMTA) placed cybercrime as a rising threat in its analysis of serious organised crime and terrorist activities in the Euro-Mediterranean region (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020). Historically, the MENA region has also been a target of sophisticated attacks, illustrated by the Iran-attributed Shamoon cyberespionage that attacked Saudi Aramco in August 2012 (Shires & Hakmeh, 2020). State-

sponsored cyber operations could be considered criminal activities, blurring the lines between law enforcement and intelligence responses in cyberspace. Examples of cybercrime are numerous in the region. EMTA refers to the Moroccan Islamic Union-Mail (CIVIPOL & Euromed Police IV, 2017) active until March 2018 as an example of the terrorist organisation's use of information and communication technologies (ICT) to conduct cyberattacks (TRAC, n.d.). An example of a hacktivist organisation is the Tunisian Fallaga Team, which defaced 33,605 websites around the world, especially in France, where they have defaced many ministries' websites (Zone-H, n.d.). Another illustration of an intricate cybercriminal activity in the MENA region is a major cyberespionage campaign, dubbed Dark Caracal, which is also covered in Pawlak's chapter in this study. It targeted thousands of individuals across 21 countries and was operating out of a Lebanese intelligence agency building since January 2012 (SMEX, 2018). Consequently, addressing the threat of crime as a multiplier of conflict and instability is paramount in the MENA region.

The crime-conflict nexus vividly extends to cyberspace. Instability creates space and opportunity for criminal activities to flourish (illegal trade of natural resources, fees and bribes, illegal drug trafficking, looting and selling antiquities), while organised crime also sustains conflict by offering lucrative means to wage longer conflicts (Steenkamp, 2017). These linkages are even easier to make as access to ICT expands and amplifies a transborder nature of crime. As such, cyber tools are used by criminals to communicate, collect funds and coordinate illicit activities in an easier, faster, safer and anonymous way. This connection has become particularly clear in the context of the terrorist use of the Internet. The region's key political features, i.e., transitioning regimes, civil conflicts and sectarianism, set favourable grounds for both domestic and transnational terrorism, "making this region the epicentre of global terrorism" (Kim & Sandler, 2020). Even though not entirely new as a phenomenon (UNODC, 2013), terrorist organisations in the MENA region use the online strategies and tactics of cybercriminals and hacktivists to inspire, communicate, recruit, train and share news of success, failure and calls to actions (Vacca, 2020, p. 54). The latter also rely on numerous sources of income and use a range of electronic methods to fundraise, such as social media, crowdfunding platforms and virtual currencies, among others (FATF, 2015). This became a particularly burning challenge in the aftermath of the conflict in Syria when the Islamic State of Iraq and Syria turned social media and cyberspace as one of its main channels of activity with well-developed communication outlets (Berton & Pawlak, 2015).

Furthermore, these cyber tools enable sabotage and espionage activities to be upscaled in the region, where a complex web of actors – ranging from hostile states to organised crime networks, terrorist organisations, and non-state actors – make way in this new domain to destabilise and discredit public and private organisations (see also Pawlak's chapter and Abdel-Sadek's Annex of this study). The activities range from illegal access to data, illegal interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and copyright and neighbouring rights (CIVIPOL & Eu-

romed Police IV, 2017). A rather low level of cyber hygiene across the region contributes to the high vulnerability of the region to cybercrime (CIVIPOL & Euromed Police IV, 2017). Common methods used in cyberattacks involve the exploitation of information to perpetrate crimes, such as spying, impersonating people to obtain merchandise services, money or communicate with other people, committing medical fraud, theft and monetisation of sensitive corporate, government or healthcare data (Vacca, 2020, p. 21). But there is more. Cash-out services can be used to buy mobile phones illegally, thus circumventing the laws obliging SIM card users to provide identification upon registration. These unregistered mobile phones are the gateway to cybercrime. Regional hacktivists are active in the region and commit low impact crimes, such as defacements. Malware-as-a-service is the most prevalent criminal activity in the region in terms of flagged cybercrime. Phishing is also a powerful vector for fraud across the region, as the common language enables criminals to reach out to victims across national borders. There are many types of phishing activities, such as financial fraud, theft of personal data, illegal online marketing, romance scam, man-in-the-middle attacks, and sexual extortion (CIVIPOL & Euromed Police IV, 2017).

Domestic efforts to fight cybercrime

The MENA countries are targeted with 6% more cyberattacks than the rest of the world and the region is "one of the world's most targeted areas of cybercrime and data loss" (Gonçalves, 2019). For instance, the United Arab Emirates (UAE) is reported as the second most targeted country in the world for cybercrime, costing the country an estimated €1.15 billion per year, while cybercriminals also exploited the COVID-19 crisis to their advantage (UNODC, 2020). Mimecast Threat Intelligence Center reports a 751% increase in unsafe clicks during the first three months of 2020 in the MENA region (Bell, 2020). While statistical information about cybercrime across the region still remains a challenge, there are some efforts to address this gap. Since 2018, the Tunisian National Agency for Computer Security has published the Tunisian cyberspace's statistics, which demonstrate a year-on-year hike in detected cybersecurity breaches, per type (ANSI, 2020).

These trends are correlated with an increasing number of investigations related to cybercrime across the MENA countries, demonstrating the involvement of regional policy-makers in finding adequate solutions to this new threat (CIVIPOL & Euromed Police IV, 2017). The objective for national policy-makers is to set up or update their existing cyber governance framework to account for and prosecute these new crimes accordingly. In the past five years, detection and disruption of cybercrime rose in the policy agenda, partly due to the creation of specific law enforcement structures.

An effective fight against cybercrime involves a multitude of mandates and requires constant adaptation to the evolving threat landscape by policy-makers and Law Enforcement Agencies (LEAs). But no government can do it alone, which makes cooperation with the private sector and non-governmental organizations (NGOs) a key component in successful imple-

The MENA countries are targeted with 6% more cyberattacks than the rest of the world and the region is "one of the world's most targeted areas of cybercrime and data loss"

mentation of any cybercrime strategy. Such cooperation also helps avoid duplications and redundancies by focusing efforts and ensuring wide consultation of all stakeholders: judicial personnel, ICT, defence, and police administrators, economics teams, NGOs and the private sector.

At the same time, a whole-of-society approach to cybersecurity also helps to strengthen a human-centric approach to it by minimising the risks of potential human rights abuses and strengthening the rule of law. This is particularly important given that monitoring and controlling of social media content has become a key aspect of MENA cybersecurity policy, sometimes to the detriment of freedom of expression online, as is further elaborated in Abdel-Sadek's Annex of this study. Under the cover of controlling the spread of online radical propaganda, several MENA governments have been restricting online civil liberties and free speech. **This chapter argues that cyber policies must contribute as much to human rights, rule of law, democratic governance and human development, as to guaranteeing security, confidence and trust in ICT.**

Algeria

Algeria has seen a substantial level of institutionalisation when it comes to fighting cybercrime. There is a progressive concentration of the competence within the Ministry of National Defence (MND). Previously, the Department of Intelligence and Security was tasked with electronic surveillance through the Network Control Group. In addition, the National Body for the Prevention and Fight against ICT Crimes (ONPLCILTIC) was under the Ministry of Justice until July 2019, when it was transferred to the MND. Nonetheless, the monitoring and reporting of cybercrime is under the responsibility of the Centre for the Prevention and Fight against Computer Crime and Cybercrime (CPLCIC), dependent on the National Gendarmerie Command, or by the cybersecurity cells of the General Directorate of National Security (DGSN). According to official statistics, these two structures handled more than 3,000 cybersecurity-related cases in 2018 (Kahlane, 2019, p. 13).

However, experts agree on three shortcomings of the existing system. First, the normative and organisational system is not complete and the establishment of bodies for the monitoring of cybercrime provided for in the texts is slow to take place. Second, there is a lack of logistical and human resources to optimise this new institutional framework. Third, the tendency to over-centralise the cybercrime response hinders the integration of the private sector and civil society, which would nonetheless provide resources and support to the administration on these issues (S. Bechiri, Realistic Security, personal communication, December 8, 2020).

Algeria has gradually acquired the means to fight cybercrime since 1997 and, according to the Council of Europe (CoE), the legal arsenal in place makes it possible to combat most of the computer crimes mentioned in the Budapest Convention on Cybercrime. Weaknesses remain in the areas of procedural law and international cooperation. There is currently no national body responsible for protecting information systems and raising awareness on this matter, even though the lack of information technology security

is a major problem for the country. A presidential decree dated 20 January 2020 aims to address some of the previously identified shortcomings by setting up a national information systems security framework, which provides for the creation of three organisations to develop the national information systems security strategy and coordinate its implementation. This institutional structure will consist of new entities, under the supervision of the MND: the National Council for the Security of Information Systems; the Agency for the Security of Computer Systems; the first national Computer Emergency Response Team (CERT), i.e., the National Operational Centre for Computer Security. It also foresees that all public and private entities must appoint a Chief Information Security Officer (Bechiri, 2020).

The first Working Groups responsible for implementing this institutional reform have started their work but their progress is hampered by COVID-19-related restrictions. Once in place, this structure will contribute to providing more clarity on cyber governance in Algeria, bringing together numerous actors under a single umbrella, while being the key government stakeholders to engage with in the field of cybercrime.

Lebanon

Lebanon scores rather low in international indexes concerning the levels of connectivity and cybersecurity (see figure 1 above). The key policy stakeholder in the fight against cybercrime is the controversial Cyber Crime and Intellectual Property Rights Bureau of the Judicial Police, within the Internal Security Forces, which was established in 2006 to strengthen online security and combat cybercrime. It focuses on addressing identity theft, money laundering, child pornography, as well as online defamation, libel and slander complaints. It has the dual role of investigating complaints, cybersecurity breaches, and technology-related crimes under the supervision of judicial authorities, while providing basic awareness to public and educational institutions on the latest cyber threats. The Cybercrime Bureau has been used as a coercion tool to regulate and remove unfavourable discourse from social media (Quino, 2015). Other state institutions and agencies, namely the Army, the General Security and State Security, have also strengthened their investigative capabilities to prevent threats to national security, including cyberattacks and cyberespionage.

In July 2019 the National Cyber Security Committee concluded that the one crucial step to set in motion the Lebanese Cyber Security Strategy is to create a National Cyber Security Information System Agency (NCISA) to assess vulnerabilities, recommend preventive measures, identify threats, respond promptly and efficiently to attacks, and maintain security (Araz, 2019). It is expected that NCISA will facilitate coordination among different actors and proactive approach to managing cybersecurity issues, while tracking the growth and diversity of cyberthreats, and addressing their sophistication. The NCISA will report directly to the Prime Minister and will be attached to the Higher Council of Defence's General Secretariat. The Cyber Security Strategy also posits the creation of the Cyber Security Incidents Response Team (CSIRT) as the central repository of cyber incidents to support in remediation, defence and prevention against the notified attacks.

There is currently no national CERT (N. Alkhatib, Bank Audi, personal communication, February 12, 2021; S. Araz, Middle East Institute, personal communication, February 12, 2021).

Morocco

Morocco has achieved legal and technical excellence in the fight against cybercrime. However, the regulatory arsenal is still limited to vital organisations and leaves out most of the private sector (DATAPROTECT & AUSIM, 2018). Bill 05-20 relating to cybersecurity was adopted by the Moroccan Parliament on 14 July 2020. The law is a significant step towards strengthening national capacities in the field of cybersecurity, broadening the scope of information systems security by integrating other active categories, such as public telecommunications network operators, cybersecurity service providers, and digital service providers. It also aims to set up a framework for cooperation data exchange between the national cybersecurity authority and the competent services for combating cybercrime and the misuse of personal data. Finally, it provides legal ground for international cooperation in the field of cybersecurity (Moroccan Parliament, 2020).

These efforts have notably been recognised by the CoE, which relies on Morocco to support the deployment of an updated legal arsenal capable of tackling cybercrime in the MENA region in the framework of its two projects: GLACY+ and CyberSouth. Currently, in Morocco, the filing of a complaint against an act of cybercrime can be made to the Moroccan Computer Emergency Response Team (maCERT), the centre for detection and reaction to computer attacks, which is part of the National Defence Administration, and the Directorate General of Information Systems Security. The maCERT Helpdesk enables any citizen to report an incident online by completing an incident report form and sending it by email or fax. maCERT also has a hotline. Morocco is, however, lagging behind with regards to its organisational structures, the inexistence of an updated cybersecurity strategy and the failure to monitor statistical indicators, which are major flaws in the system for efficiently combating cybercrime. Moreover, the study's Annex by Abel-Sadek also reviews Morocco's bleak developments from the perspective of Internet openness and freedom of speech and access.

Regional process for fighting cybercrime

Concurrently to the national efforts, countries across the region have also taken steps to strengthen their cooperation against cybercrime at regional level. The African Union Convention on Cyber Security and Personal Data Protection – also known as the Malabo Convention (MC) – of 27 June 2014 is the most comprehensive effort in this respect. However, the Convention has not gained broad support and faces problems with ratification among the African Union (AU) Commission member states (O. Daas, AFRIPOL, personal communication, November 18, 2020). In the MENA region, only two countries have signed it: Mauritania in February 2015, and Tunisia in April 2019. The Malabo Convention focuses on the technical aspects of cybersecurity, while the issue of electronic evidence in legal cases remains unsolved. An amendment is necessary to create an evidence-management gateway and lay

the groundwork for operationalisation in the area of cybercrime, based on inter-African cooperation as a principle.

The African Police Cooperation Organisation (AFRIPOL), launched in 2015, has also been active in the field of cybercrime cooperation. In 2018, a Working Group on Cybercrime began to meet biannually with the objective of developing a regional strategy to fight cybercrime. The aim of this document is to establish a regional framework for the tools in use (equipment and procedures), the training of police experts, and the legal and legislative framework to develop a convention. The need for a regional strategy to combat cybercrime stems from the observation that the African continent is disparate in terms of progress, as well as standards and tools. In preparation for the strategy, a census was conducted in the 55 countries and North Africa is among the most developed ones. In fact, Algeria will be called upon to train cybercrime experts from the AU member states. The next steps are the ongoing validation of the strategy, the provision of tools by one or more sponsors for under-equipped police forces, training in the regional centres of excellence (Rwanda, South Africa and Senegal), and capitalisation on INTERPOL Support Programme for the AU in Relation to AFRIPOL (ISPA), which was launched on 28 April 2020, especially with regards to operational capacity-building in the field of cybercrime. Other partnership projects are currently under development, in particular with the EU Agency for Law Enforcement Cooperation (EUROPOL) and the EU Agency for Law Enforcement Training (CEPOL), and cybercrime is one of the topics addressed.

Other regional instruments in the MENA region include the Arab Convention on Combating Information Technology Offences by the League of Arab States (2010), the Arab Strategy for Scientific Research and Innovation by the Arab League Educational, Cultural and Scientific Organisation (ALECSO, 2014), the Arab Regional initiative on confidence and security in use of telecommunications and ICT and the International Telecommunication Union Centre of Excellence Network in the Arab Region, from 2015 to 2018 (UNESCWA, 2019a).

MENA and international cooperation against cybercrime

The MENA countries are also engaged in international efforts to fight cybercrime: both through the existing global instruments, such as the Budapest Convention on Cybercrime, and the ongoing efforts undertaken at the United Nations (UN) through the United Nations Office on Drugs and Crime (UNODC) in Vienna and in the Third Committee at the UN Headquarters in New York.

The 2001 Budapest Convention was the most relevant international treaty seeking to address cybercrime by harmonising national laws, improving investigative techniques, and increasing transnational cooperation. The Budapest Convention is the only legally binding instrument that provides a framework for international cooperation in the fight against cybercrime, and has served as a benchmark for setting international standards in this field (Pawlak, 2017). The Budapest Convention has set out the prioritisation of cybercrime in international cooperation.

The Budapest Convention is the only legally binding instrument that provides a framework for international cooperation in the fight against cybercrime

It entered into force in July 2004, and has 65 parties and nine states in the process of accession at the moment of writing. The process of adhesion requires the CoE and the Cybercrime Convention Committee (T-CY) to conduct an assessment, which leads to the harmonisation and upgrade of the necessary legislation, after which the country is invited to become a member. The main advantage of ratifying the Budapest Convention is that it allows local institutions to interface with other countries more smoothly. Thanks to its early involvement in cybercrime cooperation, Morocco became a full party to the treaty on 26 June 2018.

Tunisia was also invited to adhere to the Budapest Convention on 13 February 2018 but has yet to become a full party, as the draft law to align the national legislation with the provision of the Budapest Convention is still pending approval. The Tunisian authorities have capacities in place to fight cybercrime and deal with electronic evidence and the CyberSouth project is assisting them further in the area of judicial training and guidelines for handling electronic evidence (V. Spiridon, C-PROC, personal communication, November 20, 2020).

Regarding the additional international legislation on cybercrime, T-CY has published 11 Guidance Notes, which serve as a follow-up mechanism to better explain the Budapest Convention to parties and provide complementary definitions (T-CY, 2012). The Second Additional Protocol to the Budapest Convention is currently under preparation by T-CY. The additional elements include enhanced international cooperation between public authorities and the private sector, new investigative powers to access data, and discussion of EU electronic evidence (T-CY, 2020).

Even though accession to the Budapest Convention is open to all countries, the Convention has not gained global recognition as a universally binding instrument. It has faced a particularly strong opposition from some countries, in particular Russia, which is the main proponent of a new international treaty on cybercrime under the auspices of the UN (Hakmeh & Peters, 2020). In 2019, a Russia-sponsored resolution proposed the establishment of an Ad Hoc Expert Committee to work towards a new UN treaty. Several countries in the MENA region such as Algeria, Iran, Libya, Sudan and Syria co-sponsored the resolution, with another 15 voting in favour, only one against (Israel) and six abstaining (Bahrain, Djibouti, Morocco, Saudi Arabia, Tunisia and Turkey) (UN, 2019). The organisational session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes convened from 10 to 12 May 2021. During the postponement debate, MENA countries were actively involved, with Saudi Arabia and Syria demonstrating a close watch over the process, and Egypt submitting views. At the meeting, Ambassador Faouzia Boumaiza Mebarki from Algeria was elected the Chair of the Group and Ambassador Mohamed Hamdy El-Molla from Egypt became one of 13 Vice-Chairs. Experts point out a strategic political discrepancy between politicians who take their decisions based on ideological alignment, and practitioners (such as LEAs), which continue to be direct beneficiaries of EU-funded support in tackling cybercrime (V. Spidiron, C-

PROC, personal communication, November 20, 2020; M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020).

Finally, on 12 November 2018, the Paris Call for Trust and Safety in Cyberspace was supported by states, local governments, companies and civil society organizations (CSOs). Its ninth principle is to promote the wide acceptance and implementation of international standards of responsible behaviour and confidence-building measures in cyberspace through the facilitation of information exchange on cybercrime. Several MENA countries have supported the Paris Call and they are Kuwait, Lebanon, Morocco, Qatar, Tunisia, and the UAE (Paris Call, 2018).

The EU's role in supporting the MENA countries

The *EU 2020-2025 Security Union Strategy* identified cybersecurity as an issue of strategic importance. Online dependency, the rise of cybercrime, and cyber theft of trade secrets are described as rationale for acting. The EU 2013 Cybersecurity Strategy lists "drastically reducing cybercrime" as one of its five priorities. In that respect, the EU's external priorities include promoting a truly multi-stakeholder dialogue between the EU and the partner countries, reinforcing ties with like-minded partners on cybercrime, and leveraging European expertise on cyber-related matters.

Although MENA as a region is not mentioned explicitly, the EU has been a key partner in supporting the region in its fight against cybercrime and has therefore funded several actions in this respect. The underlying reason for its involvement is to support Southern Neighbourhood (SN) partners in their efforts to join the multi-stakeholder dialogue on cybercrime through capitalising on EU know-how. Even though cybercrime is not officially stated in the Multiannual Action Programmes and the Annual Action Programmes with the European Neighbourhood Policy (ENP)-South countries, some activities in cybersecurity capacity-building are taking place under national Technical Assistance projects and Association Agreements or are supported by other EU global initiatives funded by the EU.

Euromed Police IV Project

According to the expert consulted, regional cooperation on cybercrime between the EU and the MENA region started in the Euromed Police IV Project, which is part of the Euro-Mediterranean Partnership (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020). Euromed Police IV was funded by the European Commission's Directorate-General for Neighbourhood and Enlargement Negotiations, and was implemented from February 2016 to January 2020 by a public-private consortium involving seven EU member states, namely: France, Germany, Italy, the Netherlands, Romania and Slovenia. Its aim was to support the LEAs (police, gendarmerie) of the EU's SN countries: Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Palestine and Tunisia. Libya and Syria were excluded for security reasons. Five crime areas were identified following a consultation between the EU and beneficiaries and a detailed matrix of the crime phenomena in the region was developed. These were: terrorism; cybercrime; trafficking in human beings, sexual exploitation, im-

Regional cooperation on cybercrime between the EU and the MENA region started in the Euromed Police IV Project, which is part of the Euro-Mediterranean Partnership

migration; drugs; and weapons and explosives.

Cybercrime was high on the agenda, with three sub-priorities and their derived activities. The first was to reinforce the capacity of security and investigation forces in their use of online networks, and Internet access providers. As an illustration of a successful activity, an initial meeting between access providers and investigation services was held at AFRIPOL, in Algiers, in the presence of Internet Service Providers (Facebook, Google, among others) and counter-terrorism and investigation officers from the region. The objective was to initiate an instantaneous reaction mechanism upon the occurrence of a cyber threat on the networks, to facilitate automatic contact sharing and enhance the authorities' feedback to the perpetrator. This mechanism is already used in Europe, and not yet in place in the MENA (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020).

The second priority area was to strengthen the capacity in the fight against financial cybercrime, and the fight against online child pornography. The SN security services were ill-equipped to tackle these new threats. Several training workshops were conducted in Tunisia and Morocco on investigative tools on the dark web for police officers, police investigation services, intelligence, and counter-terrorism operatives.

The third priority area was to strengthen police and judicial cooperation on cybercrime issues in collaboration with the Euro-Mediterranean Justice Project by developing all the prerequisites for criminal investigations. This resulted in a joint publication entitled *The Digital Evidence Handbook* in 2017, which was subsequently taken up and disseminated worldwide (M. Quillé, Euromed Police IV Project, personal communication, November 13, 2020).

Overall, the project had a positive impact on the region's capability to fight cybercrime. It provided a platform for face-to-face contacts between the private sector and LEAs to support cooperation in the region, improved understanding of key challenges of cybercrime through workshops on the dark web and other topics, and publication of *The Digital Evidence Handbook*. The project also resulted in the successful creation of two networks for LEAs, which are still active to date, even though there is currently little feedback on cybercrime activities: the Analysis Network, whereby each SN country feeds strategic and non-operational information to EUROPOL through a Euro-Mediterranean database; and the Capacity-Building Specialist Network that deals with existing crime.

In comparison to other priorities of the project, cybercrime cooperation was the area that most marked cooperation between the EU and MENA countries. An encouraging axis of cooperation has been to strengthen the links between the public and private actors on cybercrime by contributing to the development of standardised investigation methods in the fight against child pornography. Future action is needed, as some activities carried out may not be fully institutionalised, and the Ministries of the Interior's relevant units now have relatively strong regional networks.

The Euro-Mediterranean Police V Project was launched in October 2020, with CEPOL as the lead implementer. CEPOL has been involved in setting up

the Euro-Mediterranean Knowledge Base with the aim of centralising the cooperation actions carried out in the fight against crime, in particular cybercrime.

GLACY, GLACY+ and CyberSouth

In addition, the EU has provided support to other cybercrime focused projects that are global in scope but include the MENA countries among their beneficiaries. In cooperation with the CoE, since 2014 the EU has supported the Global Action on Cybercrime (GLACY) and currently its successor the GLACY Extended (GLACY+) Project (V. Spidiron, C-PROC, personal communication, November 20, 2020). The objective of GLACY+ is to strengthen the capacities of 15 priority countries, including Morocco, to apply legislation on cybercrime and electronic evidence. GLACY+ supports these countries in becoming regional hubs carrying out the implementation of activities and sharing their lessons learnt. Morocco was the earliest of ENP-South countries to take up cybercrime actions individually. As a testimony for its long involvement in international cooperation on cybercrime, Moroccan magistrates are leading training workshops in other countries (V. Spidiron, C-PROC, personal communication, November 20, 2020).

The CyberSouth Project – another joint action of the EU and the CoE that started in 2017 – has similar objectives but targets the MENA region specifically: Algeria, Jordan, Morocco, Lebanon and Tunisia. The objective is to reinforce criminal justice authorities' capacities on cybercrime and support the legislation through institutional training, and interagency and international cooperation (CoE, 2021). The important regional advantage is to capitalise on Morocco's experience in fighting cybercrime, as the country is more advanced regionally. Working with an experienced partner that has already gone through the process will enable other partners to make use of the same methodology to develop capacities and best practices, while the more advanced partner can continue to receive support. Models and best practices in cybersecurity legislation and electronic evidence exist; however, regional ambitions ought to be navigated wisely, as the question of who has the leading role is sensitive (V. Spidiron, C-PROC, personal communication, November 20, 2020).

The main activities are the law enforcement and judicial trainings carried out in these countries in computer forensics and open-source intelligence in a train-the-trainer perspective, where trained magistrates conduct trainings for newcomers. Guidelines to secure, collect and analyse electronic evidence is currently not in line or harmonised with international best practices and support was provided in this respect. Since the first workshops that have taken place to benefit structures in each country, major progress was registered and some of the countries developed their domestic guidelines on handling electronic evidence. A joint effort to develop the national training material on cybercrime in all five target countries (including the curricula for judicial training institutes) is currently being put together by Domestic Working Groups. The CyberSouth Judicial Network Secretariat also facilitates dialogues between magistrates in the region on

the topics of cybercrime and electronic evidence, and is an informal channel to enhance international cooperation.

Conclusions and recommendations

In sum, the MENA region is gradually integrating into the global digital economy, although a mindset shift is needed to foster the development of a truly competitive private sector, the rationalisation of public sector employment and the diversification of the economy to other growth-generating economic sectors apart from oil and gas.

In the MENA region a shift is underway from passive technology consumption to localisation and technological appropriation

A promising sign of economic diversification in the MENA region is the appetite for technology and innovation that is beginning to emerge. Indeed, a shift is underway from passive technology consumption to localisation and technological appropriation (UNESCWA, 2019b). Endemic ride-hailing applications and a regional music streaming platform are examples of technological appropriation. Nevertheless, more efforts are needed to move towards the endogenous production and technological innovation levels that are required in the digital economy.

One of the hidden facets of this optimistic horizon is the extreme vulnerability and poor cyber hygiene of the region in the face of the new risks, and in particular the new criminal trends. Many actors, from competing states, to non-state actors, terrorist groups and political oppositions, are converging on the web, exploiting its easy, fast and anonymous access to conduct illicit activities. This is all the more true in a polarised and war-prone region, such as the MENA.

Cybercrime has rapidly emerged as one of the most serious societal threats and a key challenge for the LEAs in the region. The national piloting of a cybersecurity strategy is a crucial step in creating a common framework for responding to this exponential problem.

Efforts have been made in this direction in the MENA region and this chapter has focused on presenting the administrative and legal remedies available to citizens who are victims of cyberattacks in three countries, Algeria, Lebanon and Morocco, being particularly active in cooperating with the EU in this field.

As cybercrime is a cross-border issue by nature, it requires international cooperation to strengthen and increase convergence of national legislations in order to trace and prosecute cybercriminal networks across borders. Ongoing negotiations at the UN regarding the possible adoption of a new cybercrime treaty divide the world, and the MENA region is no exception, with a majority of MENA countries supporting this process with the expectation that it would provide more clarity on the rules applicable to cyberspace.

In line with its objective of promoting a multi-stakeholder dialogue on cybersecurity, the EU has been working since 2014 to support the countries of the SN in their efforts to upgrade their administrations and legislative frameworks in the fight against cybercrime. Several EU-funded initiatives, described in this chapter, coexist to, among other things, support countries wishing to adopt the Budapest Convention and improve their capacity to respond to cyberattacks. This chapter also argues that the EU is a legitimate

partner to support the MENA region in its anti-cybercrime efforts due to its early involvement in the process and continued eagerness to support, demonstrated by several ongoing EU-funded projects.

Four concrete measures are suggested as the way forward for MENA national policy-makers to advance the much-needed anti-cybercrime reform with the support of committed partners, such as the EU.

1. **Data collection is a necessary step to evaluate the risk of cybercrime.** Policy-makers should prioritise sizing up cybercrime's costs, numbers and types of cyberattacks, and the most hit industries and administrations. The information gathered will highlight the extent of cybercrime and will help determine proper threat levels. The EU and MENA countries' policy-makers must take advantage of the new phase of the MEDSTAT regional programme presently at a tender stage, whose objective is the harmonisation of statistics in the ENP-South countries, by adding cybersecurity statistics to the current targeted fields.

2. **Fostering inclusive participation of the private sector and civil society in cyber policy formulation and monitoring.** Experts consulted agree that a way to enhance cooperation in tackling cybercrime is to engage with the private sector and develop new cooperation schemes, i.e., the hybridisation of cybersecurity provision and widening dependency between public and private actors. Public-private partnerships in the fight against cybercrime are an indispensable element. This area of cooperation is to be developed and, although contacts were initiated, they are yet to be institutionalised. The new phase of the Euro-Med Police V Project, which was recently launched, provides a suitable framework to introduce private sector participation and wider consultation.

3. **Reinforcing MENA capacities through existing networks.** This chapter presented regional projects that have built networks and Centres of Excellence, within which state personnel (LEAs, prosecutors and magistrates) from across the MENA region interact and share best practices. This effort is bearing fruits, especially as it offers a channel of communication to mutualise and enhance intra-regional know-how and replicate efforts. This is especially relevant in this region's context of relative linguistic homogeneity.

4. **Enhancing cyber hygiene in the MENA region.** One crucial element in preventing cybercrime is to educate Internet users about the risks that they are taking online. This awareness-raising effort is already taking place in the form of multiple campaigns, from organising cyber drills and cybersecurity competitions, participating in Safer Internet Day, and public awareness events, such as regional cybersecurity week and other thematic workshops. These domestic efforts must be sustained, and systematised, with regional organisations (UNESCWA, AFRIPOL, League of Arab States) playing a unifying role. In addition to policy-makers' capacity-building efforts, CyberSouth and Euromed Police Projects, as well as others, could also implement activities reinforcing school curricula in cyber hygiene.

References

AGENCE NATIONALE DE LA SECURITE INFORMATIQUE (ANSI). (2020). *Statistiques sur le cyberespace tunisien.* Retrieved from https://www.ansi.tn/statistics

ARAZ, S. (2019). *Lebanon's cybersecurity strategy emerges.* Retrieved from https://mei.edu/publications/lebanons-cybersecurity-strategy-emerges

BECHIRI, S. (2020). *Nouvelle organisation de la SSI en Algérie.* Retrieved from https://www.realistic-security.com/nouvelle-organisation-de-la-ssi-en-algerie/

BELHAJ, F. (2021). *MENA unbound: ten years after the Arab Spring, avoiding another lost decade.* Retrieved from https://www.worldbank.org/en/news/ opinion/2021/01/14/mena-unbound-ten-years-after-the-arab-spring-avoiding-another-lost-decade

BELL, J. (2020). *Coronavirus: Cybercrime rockets in Middle East as fraudsters exploit COVID-19.* Retrieved from https://english.alarabiya.net/News/middle-east/2020/12/07/Coronavirus-Coronavirus-Cybercrime-rockets-in-Middle-East-as-fraudsters-exploit-COVID-19

BERTON, B., & PAWLAK, P. (2015). *Cyber Jihadists and their Web.* Retrieved from https://www.iss.europa.eu/content/cyber-jihadists-and-their-web

CIVIPOL & EUROMED POLICE IV. (2017). *Euromed police threat assessment.*

COUNCIL OF EUROPE (CoE). (2021). *CyberSouth.* Retrieved from https://www.coe.int/en/web/cybercrime/cybersouth

CYBERCRIME CONVENTION COMMITTEE (T-CY). (2012). *Guidance notes.* Retrieved from https://www.coe.int/en/web/cybercrime/guidance-notes

CYBERCRIME CONVENTION COMMITTEE (T-CY). (2020). *Protocol negotiations.* Retrieved from https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

DATAPROTECT & AUSIM. (2018). *Les enjeux de la cybersécurité au Maroc - Livre Blanc.* Rabat: Bibliothèque Nationale du Royaume du Maroc.

EU CYBER DIRECT. (2020). *Cybercrime at the United Nations Background Note.* Retrieved from https://eucyberdirect.eu/wp-content/uploads/2020/06/backgroundnote.pdf

FINANCIAL ACTION TASK FORCE (FATF). (2015). *FATF Report. Emerging terrorist financing risks.* Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

GAUB, F. (2019). *Chaillot Paper 154 - Arab futures 2.0 the road to 2030.* Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/ Chaillot_154%20Arab%20Futures.pdf

GONÇALVES, P. (2019). *Middle East is the biggest target for cybercrime.* Retrieved from https://www.internationalinvestment.net/news/4001693/middle-east-biggest-target-cybercrime

HAKMEH, J., & PETERS, A. (2020). *A new UN cybercrime Treaty? the way forward for supporters of an open, free, and secure Internet.* Retrieved from https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet

INTERNATIONAL TELECOMMUNICATION UNION (ITU). (2018). *Global Cybersecurity Index.* Retrieved from https://www.itu.int/pub/D-STR-GCI.01-2018

KAHLANE, A. (2019). La problématique de la concurrence dans le contexte de l'économie numérique. Retrieved from http://www.conseil-concurrence.dz/wp-content/uploads/2019/10/Mr-Kahlane.pdf

KIM, W., & SANDLER, T. (2020). Middle East and North Africa: terrorism and conflicts. *Global Policy, 11*(4), 424-38.

LATICI, T. (2019). *Cyber: how big is the threat?* Retrieved from https://www.europarl.europa.eu/ RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

MOROCCAN PARLIAMENT. (2020). *La Chambre des Représentants adopte 6 projets de loi relatifs à la défense nationale, à la sécurité informatique et au secteur financier et bancaire.* Retrieved from https://www.chambredesrepresentants.ma/fr/actualites/la-chambre-des-representants-adopte-6-projets-de-loi-relatifs-la-defense-nationale-la

PARIS CALL. (2018). *Paris Call for trust in cyberspace.* Retrieved from https://pariscall.international/en/call

PAWLAK, P. (2017). *A wild wild web? laws, norms, crime and politics in cyberspace.* Retrieved from https://www.iss.europa.eu/content/wild-wild-web-law-norms-crime-and-politics-cyberspace

QUINO, Z. (2015). *#HackingTeam leaks: Lebanon's cybercrime bureau exploited angry birds to surveil citizens' mobile devices.* Retrieved from https://smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

SHIRES, J., & HAKMEH, J. (2020). *Briefing - is the GCC cyber resilient?* Retrieved from https://www.chathamhouse.org/2020/03/gcc-cyber-resilient

SMEX. (2018). *Beirut-based global cyber-espionage campaign a threat to local freedoms.* Retrieved from https://smex.org/beirut-based-global-cyber-espionage-campaign-a-threat-to-local-freedoms/

STATISTA RESEARCH DEPARTMENT. (2019). *Internet penetration rate in the Middle East and globally 2009-2019.* Retrieved from https://www.statista.com/statistics/265171/comparison-of-global-and-middle-eastern-internet-penetration-rate/

STEENKAMP, C. (2017). The crime-conflict nexus and the civil war in Syria. *Stability: International Journal of Security & Development, 1*, 1-18.

TERRORISM RESEARCH AND ANALYSIS CONSORTIUM (TRAC). (n.d.). *Moroccan Islamic Union-Mail.* Retrieved from https://www.trackingterrorism.org/group/moroc%C2%ADcan-islamic-union-mail

UNITED NATIONS ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (UNESCWA). (2019a). *Arab horizon 2030 - digital technologies for development.* Retrieved from https://www.unescwa.org/publications/arab-horizon-2030-digital-technologies-development

UNITED NATIONS ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (UNESCWA). (2019b). *Fourth industrial revolution - impact of the fourth industrial revolution on development in the arab region.* Retrieved from https://www.unescwa.org/sites/www.unescwa.org/files/publications/files/impact-fourth-industrial-revolution-development-arab-region-english.pdf

UNITED NATIONS (UN). (2019). *Countering the use of information and communications technologies for criminal purposes: resolution adopted by the General Assembly.* Retrieved from https://digitallibrary.un.org/record/3841023?ln=en

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). (2013). *Comprehensive study on cybercrime.* Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). (2020). *COVID-19 cyber threat analysis UNODC MENA assessment & actions.* Retrieved from https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf

VACCA, J. (Ed.). (2020). *Online terrorist propaganda, recruitment, and radialization.* Boca Raton, FL, United States: Taylor & Francis Group.

WORLD BANK. (2019). *World Bank data.* Retrieved from https://datahelpdesk.worldbank.org /knowledgebase/articles/906519-world-bank-country-and-lending-groups

YOUSSEF, T. M., ABOUELDAHAB, N., ABDEL GHAFAR, A., ZOUBIR, Y., FATHOLLAH-NEJAD, A., & KABBANI, N. (2020). *Op-Ed The Middle East and North Africa over the next decade: Key challenges and policy options.* Retrieved from https://www.brookings.edu/opinions/the-middle-east-and-north-africa-over-the-next-decade-key-challenges-and-policy-options/

ZONE-H. (n.d.). Unrestricted information. Retrieved from http://www.zone-h.org/archive/notifier=Fallaga%20Team/page=50

Stability, Internet Governance and Disinformation

Samuele Dominioni
Research Fellow, Italian Institute for International Political Studies (ISPI)

Introduction

The spread of information and communication technologies (ICT) has revolutionary effects on contemporary societies. Luciano Floridi described this new age of reliance on digital technologies as "hyperhistory" (Floridi, 2012). These great transformations also affect politics, where both positive and negative implications of digital technologies are already widespread. For example, social media can help people to have their voices heard and share episodes of political frauds or malpractices. At the same time, ICT amplify the effects of fake news and disinformation campaigns. There has been a growing number of studies investigating the effects of digital technologies on politics both in liberal democracies (Deibert, 2019; Bartlett, 2018; Kavanagh & Rich, 2018; Nemitz, 2018) and non-democratic regimes (Dominioni, 2020a; Keremoğlu & Weidmann, 2020; Xu, 2020; Rød & Weidmann, 2015; Deibert et al., 2008; Kalathil & Boas, 2003). Nevertheless, as Jaclyn Kerr (2018) points out, what has not received much attention to date is how Internet control may impact broader developments of political regimes.

This chapter aims to address this gap by looking into three countries in particular: Egypt, Jordan and Morocco. In the last decade, all these countries experienced constitutional change or reforms driven by a revolution in Egypt or by elite concessions in Jordan and Morocco (Bank & Edel, 2015). All these countries also enjoy a relatively high share of young population (around one third of the entire population[1]) and have high levels of literacy.[2] In addition, they are or were in the past members of international fora addressing norms of responsible state behaviour in cyberspace such as the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE) and the United Nations Open-Ended Working Group on Developments in the Field of ICT in the Context of International Security (UN OEWG). All are also part of the European Neighborhood Policy (ENP), which since 2017 specifically included cybersecurity among its actions (Lannon, 2019). Finally, none of them can be described as a democratic regime. According to the Democracy Index 2019, Egypt and Jordan are both "authoritarian regimes", whereas Morocco is a "hybrid regime". These categorisations are important insofar as they permit the study of Internet governance models in non-Western liberal democracies. This, in turn, raises relevant questions concerning the impact of the Internet on the stability of these regimes.

The argument herein is that different policies and practices around Internet governance, and in particular those regarding content regulation and disinformation, may actually play an important role in regime developments. Since the digital domain became a tool for contesting the existing power structures and rulers (Bunce & Wolchik, 2010; Eltantawy & Wiest, 2011) or even a "liberation technology" (Plattner & Diamond, 2012), it seems justified to include national regulation of cyberspace as a variable in-

[1] Egypt 33.6%; Jordan 33.1%; Morocco 27% (CIA World Factbook, 2020).

[2] Egypt 93.29%; Jordan 99.23%; Morocco 95.07% (World Data Atlas, 2015).

fluencing the state's organisational capacity defined as "the scope and cohesion of state and governing-party structures" (Levitsky & Way, 2010) or "a powerful coercive apparatus and/or party organization" (Levitsky & Way, 2010, p. 25). A strong organisational capacity is thus key to counter both institutional and informational uncertainties, which – as Andreas Schedler (2013) claims – are the two main variables that play a substantial role in authoritarian stability. Therefore, mass protest and election contestations often fail in regimes with fewer information gaps, as happened for example with countries that joined late during the Arab Spring (Bank & Edel, 2015). With the advent of digital technologies, non-democratic regimes had to develop capabilities in order to contrast threats and challenges from cyberspace (Deibert et al., 2010).

Beyond authoritarian control to curb civil and political dissent, many countries around the world undertook efforts to create legislation on digital media in order to counter challenging phenomena related to disinformation, such as radicalisation (for example, in the context of the Islamic State of Iraq and Syria [ISIS]) and information operations to influence elections (such as the 2016 United States presidential election). These cases triggered, especially in liberal democracies, the debate regarding the conditions under which freedom of speech could and should be limited. The outbreak of the COVID-19 pandemic has resulted in a sharp increase in the level of political attention to disinformation as a global phenomenon, which aggravated the necessity to counter the informational disorder, and prompted the UN to declare an "infodemic".

With many governments around the world adopting policies to curb disinformation, including in the European Union (EU) and across the Middle East and North Africa (MENA) region, the study of a triangular relationship between a legitimate security concern, protection of human rights online and regime stability needs to become a priority. What is the effect of these policies on freedom and societal resilience and regime stability? How can these sometimes conflicting objectives be reconciled and provide fruitful ground for EU cooperation with countries in the MENA region?

This chapter discusses the Internet governance models in Morocco, Jordan and Egypt in order to draw conclusions about how various models can abuse policies of information control. In order to assess opportunities for cooperation between the EU and countries in the region, the chapter compares the EU's response to fake news, disinformation and other informational threats in its member states with those in the region. The analysis presented in this chapter builds on semi-structured interviews with subject experts, the analysis of the UN voting patterns and the analysis of secondary sources such as reports and studies regarding freedoms online. Given the particular attention that the EU attaches to cyber capacity-building programmes, the chapter concludes with recommendations on how to make better use of good practices in these programmes across the region.

Open, free and secure? Internet governance in the MENA region

Non-democratic regimes often take different approaches to cyberspace than liberal democracies, including in the international fora defining norms

Countries undertake content control at the domestic level, through a mix of formal and informal measures

and state behaviours in cyberspace. This pattern can be traced back to the late 1990s when Russia raised the issue of countering threats from cyberspace at the UN. The request to open up an international debate about informational threats provoked a drift between two fronts, which predictably mirrored geopolitical stances (Dominioni & Rugge, 2020). All those states that wanted to preserve the founding principles of cyberspace belonged to the first front, called "globalised". The founding principles are based on the underpinning paradigm of an "unfragmented space", without boundaries and with free flow of information (Mueller, 2017). The second front brought together countries that conceptualised cyberspace, and thus Internet, as just another medium like TV or radio and consequently it had to be ruled, in particular with regards to content. This second approach is referred to as "alignment" (Mueller, 2017).[3] These two conflicting reasons are also the main factor in the two processes that drove the discussions at the UN, namely the UN GGE and the UN OEWG. Presumably, the success and failure of one depends on developments in the other (Broeders, 2019). The next sections shed light on models of Internet governance adopted in Egypt, Jordan and Morocco. Overall, it is possible to claim that in terms of Internet governance models, the three countries under analysis are implementing policy choices and practices that are more in keeping with the aligned model approach. This is particularly evident in Egypt, where there is consistency between domestic policies/practices and the behaviour at the UN General Assembly regarding cyber-related issues. Both Morocco and Jordan's domestic and international behaviours are less consistent. On the one side, the countries undertake content control at the domestic level, through a mix of formal and informal measures. On the other, at the international level, they sustain the processes of both the United States of America (USA) and Russia to set state behaviour norms in cyberspace. It could be hypothesised that the inconsistency at the domestic and international level is led by their preference to non-align themselves with any sides on Internet governance solutions.

Egypt

Egypt invested in the ICT sector to foster economic development (Saleh, 2012). The government opted for a centralised approach (Wheeler, 2003) and released a national strategy on Internet during the MENA Economic Summit in 1994. The plan aimed for a socioeconomic transition, which revolved around the idea of passing from an industrial-based to a knowledge-based economy. In the following years, the government led by President Hosni Mubarak undertook a series of initiatives to spread ICT among the population. These efforts produced relevant results as in less than two decades Internet users went from 438,208 (2000) to 48 million (2019) according to the Internet Live Stats (www.internetlivestats.com) data compiled by the International Telecommunication Union (ITU), World Bank, and UN Population Division, with a penetration rate of 55.7% (Arab Republic of Egypt, 2020).

[3] This dichotomy does not find a consistent preference among Western countries. For example, "hard-core European data protection advocates who want to border information flows, many cyber-warriors in the U.S. military […] are all partisan of alignment" (Mueller, 2017, p. 35).

Moroever, there are more than 200 accredited Internet service providers (ISPs). The centralised model is also reflected in the government's power over ICT matters and authorities. For example, the National Telecommunication Regulatory Authority (NTRA), which regulates all ICT and ISP activities, does not enjoy formal independence from the government (Article 19, 2015). Overall, the government maintains "considerable control over Internet infrastructure and has restricted connectivity" (Freedom House, 2019a).

Government regulation and control over the online content have increased over the years. In the first phase, prior to the 2011 Revolution, a report from the OpenNet Initiative stated there was "no evidence of Internet filtering in Egypt, although a small group of politically sensitive websites have been blocked in the past" (OpenNet Initiative, 2009). Amidst the Revolution, in January 2011, national authorities managed to shut down the Internet on several occasions. Beyond the brief political parenthesis of Mohamed Morsi, with the advent of Abdel Fattah Al-Sisi authorities began to engage significantly more in online surveillance, arbitrary censorship, and website shutdowns. Facebook in particular is under scrutiny and targeted with requests to close down certain pages (Freedom House, 2020a). In 2018 the government even decided to launch, without success, its own version of Facebook, a social platform called Egypt Face.

In terms of international stances, Egypt is a very active player and takes part in key global initiatives, including those sponsored by EU countries and "like-minded" states. For example, Egypt and France were the initiators of a proposal submitted to the Chair of the UN OEWG to establish a Programme of Action that is now sponsored by another 47 UN member states. The proposals call for concrete steps in order to achieve practical outcomes on international cybersecurity. Nevertheless, Egypt's stances at the UN have often reflected those of the "aligned" countries, such as Russia (Dominioni, 2020b). This is particularly evident in Egypt's UN voting patterns on some of the key resolutions, including on the establishment of all UN GGE or the UN OEWG. In these fora, Egypt expressed its desire for the "operationalization of the existing rules and norms previously endorsed by the UN General Assembly through upgrading their status and making them more binding for all States" (UN OEWG, 2020).

Jordan

Jordan also pursues the development of ICT as a means to foster economic diversity and trigger growth (Ein-Dor et al., 2005). In particular, since the early 2000s, King Abdullah II expressed full faith and support for the diffusion of ICT in the country (Al-Jaghouob & Westrup, 2003). Multiple initiatives, which attracted the participation of international public and private donors (such as the World Bank and Microsoft), spread new technologies among the population along with education efforts (Al-Jaghouob & Westrup, 2003). The percentage of Internet users among the Jordanian population passed from being 2.6% in 2000 to 66.8% in 2017 (World Bank, 2020). The government of Jordan opted for a public-private approach for ICT development. The main strategy was outlined in the REACH initiative, which presents a national approach and outlines a clear action plan for Jordan to develop a competitive model for ICT,

such as that adopted in Ireland and Singapore (Al-Jaghouob & Westrup, 2003). However, the state maintains some control on Internet infrastructures (Freedom House, 2020b). Currently there are five main ISPs in Jordan, namely Zain, Orange, Umniah, TE Data and Damamax. The Telecommunications Regulatory Commission (TRC) regulates the ISP market. TRC is an independent body yet accountable to the Ministry of Digital Economy and Entrepreneurship (MoDEE).

Jordan's policies on Internet content control and censorship have evolved over the years. During the 2000s, authorities were keen to avoid Internet blockages, including of social platforms such as Facebook, Twitter and YouTube. In addition, in terms of censorship or content limitation, Jordanian authorities in those years appeared uncertain about Internet freedom and how best to regulate it (Freedom House, 2011). In January 2010, a substantial shift was imposed by the ruling of the Court of Cassation, which affirmed that websites and electronic media must comply with the Press and Publications Law (PPL) (Freedom House, 2011). Moreover, in the years after the Arab Spring, Jordan passed several laws that posed burdensome restrictions on Internet freedom, including amendments to the PPL law, which declared that any website or platform that publishes news had to register with the government.

At the international level, especially regarding the UN General Assembly votes about the UN GGE and UN OEWG, Jordan took a milder approach than Egypt, welcoming both the Russian and USA initiatives. However, Jordan has been rather silent in making its positions clear: domestically it seems to sustain information control, whereas at the international level it is more cautious about taking a side and clearly stating its stances. This approach is in line with both that of the so-called non-aligned countries and with Amman's intentional strategy that "allows Jordan to pose [with a special eye on Western donor countries] as a modern and relatively progressive polity" (Yom, 2009, p. 152).

Morocco

Morocco started to liberalise the telecommunications sector in the late 1990s. This process was managed by the National Telecommunications Regulatory Agency (ANRT). Nevertheless, the entire ICT infrastructure is still owned by the state. Nowadays there are three leading ISPs in Morocco: Maroc Telecom, Orange Morocco, and INWI. Over the years, the government has never imposed any connectivity restrictions and does not exercise technical or legal control over the Internet infrastructure for this purpose (Freedom House, 2019b).

Internet access in Morocco is, for the most part, open and unrestricted. ANRT also manages the top-level country domain (.ma) in a most indiscriminate manner. Nevertheless, the odds for potential systemic control over content are high as the Internet backbone is very centralised (Freedom House, 2019b). In this regard, Morocco's censorship and filtering policies are very surgical and focused (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020). These policies are enforced by limiting access to specific websites, social media monitoring, and limiting the use of torrents (Internet Censorship Map, 2017). Moreover, when they have to intervene, the authorities directly target individuals by contacting the user and asking her/him to take down the content (Z. Bouziane, University of Shar-

jah, personal communication, October 28, 2020). In terms of content, authorities are particularly active in curbing all online content that is deemed "prejudicial to Islam, the monarchy, territorial integrity, or public order" (Reporters Without Borders, 2016). The law is particularly prejudicial to investigative journalism, but the effects spread to the Internet community as a whole. Nevertheless, Freedom House has signalled a positive trend in that it has not reported any Internet blocking by the government since 2013, and no general or local Internet shutdowns so far.

At the international level, Morocco seems to be following the Non-Aligned Movement (NAM) approach, which implies an open policy toward any kind of initiatives regardless of their initiator, including binding documents, such as the Budapest Convention on Cybercrime (ratified in 2018). In particular, as stated in the *NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,* a "multilaterally-agreed, and consensus-based process within the UN System represents the best way to ensure that arrangements in this field address the concerns of all States, and are thus equitable, comprehensive and effectively implemented" (NAM, 2020).

Tackling disinformation

Since 2013, the World Economic Forum has reported on the global risk of massive digital disinformation[4] campaigns at the core of technological and geopolitical risks (Zollo, 2019). This phenomenon became even more problematic during the COVID-19 pandemic. Public actors, such as governments and international organisations, private actors, newspapers and social media platforms, took measures to fight the spread of disinformation online. Yet, it is hypothesised that in some particular contexts public policies aimed at tackling disinformation could be used to curb opposition movements, civil society groups, and Internet freedom as a whole. In all the countries under analysis there are precedents of countering disinformation policies and practices, which were developed prior to the outbreak of the COVID-19 pandemic. Indeed, Egypt, Morocco and Jordan equipped themselves with laws aimed at countering radicalisation propaganda and terrorist content online. Abuses of these laws have already been observed on multiple occasions.[5] In terms of countering COVID-19-related disinformation, in some cases the authorities used the legal tools already in place; in others they developed brand new policies to target the infodemic. Nevertheless, the research conducted so far did not report on any specific definition of disinformation/misinformation/fake news used by the authorities in the selected countries.

The following sections investigate the approaches adopted in Egypt, Morocco and Jordan to counter disinformation practices. The cases under analysis portray three different behaviours regarding the adoption and

[4] In this chapter, disinformation is used as a catchall concept, which includes misinformation, fake news and other related information disorder typologies.

[5] See, for example, the *EuroMed Rights Report* available at: https://euromedrights.org/wp-content/uploads/2018/03/EuroMed-Rights-Report-on-Counter-terrorism-and-Human-Rights.pdf

mis/use of counter-disinformation policies regarding COVID-19. In Egypt, where Internet freedom is already very limited (26/100 according to Freedom House, 2020a), the authorities did not need to adopt further specific restraints to Internet freedom to tackle disinformation. In this case, the authorities were using existing laws to curb any possible alternative narratives on pandemic management, in particular those from authoritative sources (such as doctors and medical staff). In Morocco, where Internet freedom is more tolerated (52/100 according to Freedom House, 2020c) the regime tried to pass a new and more restrictive law against content control online but it was harshly criticised by a lively civil society and therefore suspended. Jordan has a similar level of Internet freedom (49/100 according to Freedom House, 2020b), yet the authorities, even though there was already a legal framework against disinformation, decided to implement tougher policies to fight this phenomenon and resorted to misusing it to curb political dissent, as happened for the "teachers' protests".

Internet is considered by the Jordanian authorities to be a source of instability in the regime

These three different behaviours are also emblematic in terms of the state of the regime, or organisational power, in each country under analysis. Morocco is a stable hybrid regime that has found a sustainable equilibrium between rulers and ruled since the important constitutional reforms in 2011. Law 22.20 could have generated an imbalance and was thus suspended. Anecdotal evidence suggests that the regime does not conceive Internet freedom as a threat to its stability (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020). Egypt is a stable authoritarian regime which since the aftermath of the Arab Spring revolution, and in particular since the instauration of the Al-Sisi administration, has implemented important policies to limit Internet freedom, which are now making another Internet-based revolution practically impossible (Researcher, AFTEEGYPT, personal communication, November 10, 2020; J. Shea, TIMEP, personal communication, November 11, 2020). In light of this background, the regime was well equipped to curb disinformation regarding COVID-19. Jordan is also an authoritarian regime but it portrays less stable organisational power. As a matter of fact, people have lost trust in public institutions (IRI, 2018). This was a long process of disillusionment that started in the mid-90s (M. Torki, Yarmouk University, personal communication, October 30, 2020). In this context, Internet is considered by the Jordanian authorities to be a source of instability in the regime (M. Torki, Yarmouk University, personal communication, October 30, 2020; R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). Therefore, as shown by the analysis above, there are observed cases of misuse of policies to tackle disinformation about COVID-19. The overall impact on Internet freedom could be relevant for the country.

Egypt

The infodemic hit Egypt at the very beginning of the pandemic. In March 2020 there were three main statements, from the Prime Minister, the Public Prosecutor, and the Head of Supreme Media Council aimed at preventing the population from sharing disinformation about COVID-19. Among the major sources of concern were social media platforms (Researcher, AFTEEGYPT, personal communication, November 9, 2020), which are widely used by Egyptians, as other

types of media are already under full state control. The authorities did not pass particular laws or regulations to curb disinformation but relied on the pre-existing laws such as Law No. 175 of 2018 on Anti-Cybercrime, Law No. 180 of 2018 on Regulating the Press and Media, and Law No. 58 of 1937 and its amendments on the Penal Code. These laws give authorities sufficient powers to intervene against any publications, newspapers, media outlets, or advertising materials containing information deemed to threaten national security; disturb the public peace; or promote discrimination, violence, racism, hatred or intolerance (Law 180, art. 4, 2018). In such cases, Law 180 grants the Supreme Media Council authority to ban or suspend the distribution, broadcast or operation of any media outlets or to suspend or block any personal website, blog or social media account that has more than 5,000 followers.

The authorities, after a first period of positive initiatives, such as debunking COVID-19-related fake news efforts undertaken by the Egyptian Cabinet's Media Center (a public institute), turned into a more widespread campaign to curb any type of dissent and to silence criticisms on how the Egyptian government was managing the pandemic (AFTEEGYPT, 2020). As a matter of fact, the government did not want alternative narratives to circulate (J. Shea, TIMEP, personal communication, November 11, 2020). Medical doctors, nurses and other medical employees were particularly scrutinised by authorities, which resorted to controlling their behaviour online. Between April and June 2020, six doctors were arrested with the charge of expressing their views on social media (AFTEEGYPT, 2020). According to the *Quarterly Report on the State of Freedom of Expression in Egypt,* between April and June 2020 the violation rate of the right to freedom of expression online increased by 500% (AFTEEGYPT, 2020).

Jordan

With the unfolding of the pandemic in the country, in mid-March 2020 King Abdullah II issued a royal decree that allowed the government to take extraordinary measures. One of them was the Defence Order 8, published on 15 April 2020, which prohibited "publishing, re-publishing, or circulating any news about the epidemic in order to terrify people or cause panic among them via media, telecommunications, or social media." Contraveners could risk up to three years in prison. The country is not new to this type of restriction regarding freedom of speech, as there are other laws that criminalised criticisms against the King, the royal family and other public institutions (M. Torki, Yarmouk University, personal communication, October 30, 2020). Moreover, in February 2019 the parliament approved an amended law on cybercrime that included an ambiguous definition of "hate speech" as "every writing and every speech or action intended to provoke sectarian or racial sedition, advocate violence or foster conflict between followers of different religions and various components of the nation" (Accessnow, 2019). Similarly, the text of the Defence Order 8 is vague about what is considered to be disinformation (R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). As a matter of fact, although Prime Minister Omar Razzaz affirmed that the law would be applied to the "narro-

west extent" (Freedom House, 2020b), there have been multiple contested cases regarding its application even prior to its entering into force (HRW, 2020a).

Since the beginning of the pandemic there have been numerous cases of prosecutions against individuals that shared or posted something on social media, which were initiated on the basis of the cybercrime law or the Defence Order 8. Among the episodes observed by human rights organisations is the cracking down on online posts regarding the so-called "teachers' protest", which took place in summer 2020 (HRW, 2020b). Yet, there have not been observed cases of conviction for the same charges (Q. Suwan, Jordan Open Source, personal communication, November 9, 2020). It could be argued that it is an additional "card" that the regime can play to deter further discontent (R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). The identification of users works through an effective system of surveillance and relies on simple mechanisms, such as monitoring public social media posts (R. Sharbain, Jordan Open Source, personal communication, November 9, 2020). Once a user is identified, the authorities have several ways to intervene: they reach out directly to the author of the post and ask them to shut it down; proceed to start a prosecution against them; or they go directly to the residence of the authors and pick them up from there, sometimes in plain clothes (M. Torki, Yarmouk University, personal communication, October 30, 2020; R. Sharbain, Jordan Open Source, personal communication, November 9, 2020).

Morocco

The combination of a widespread use of ICT and still high level of illiteracy is a pulling factor for disinformation, which is an endemic and long-lasting problem affecting the country. Yet, the Moroccan authority did not have a social media policy till the very beginning of the pandemic. The antiterrorism law adopted in 2003 has not been used to curb media since 2013, when Moroccan authorities blocked the websites of the investigative news outlet Lakome for allegedly condoning terrorism (Freedom House, 2020c). In mid-March the government passed Law 22.20, which was soon after dubbed "*la loi bavette*".[6] According to this new legal provision, "anyone who deliberately uses social networks, open broadcast networks, or similar networks to publish or promote electronic content containing false information shall be punished by imprisonment for three months to two years and a fine of 1,000 to 5,000 dirham [$105 to $525], or either of these two penalties alone" (Law 22.20, Article 16, 2020). This new law shocked the Moroccan population as until that moment Morocco enjoyed a relatively positive Internet freedom of expression policy (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020). In response, multiple civil society organizations (CSOs) harshly contested the law with some success as, in May 2020, it was put on hold until the health crisis is over. Notwithstanding the suspension of the law, Moroccan authorities have other tools for tackling disinformation such as the penal code, the antiterrorism law, and the press code.

[6] "the gag law" (author's translation).

In light of this legal framework, in the months following the outbreak of the pandemic several people have been arrested for sharing fake news on social media platforms. The first one was a relatively famous local influencer, "Mi Naima", who, on a video published on YouTube, claimed that COVID-19 did not exist. Other cases followed, and at least another 12 people were arrested for the same charges (Mebtoul, 2020). The General Directorate of National Security is closely monitoring social media platforms to fight COVID-19 disinformation episodes, and it has very sophisticated surveillance programmes (Freedom House, 2020c). The authorities prefer not to close down pages or request the blocking of a post but to address the users directly, and there have been no reports of misuse of anti-disinformation policies to target people for other reasons than spreading false news about COVID-19 (Z. Bouziane, University of Sharjah, personal communication, October 28, 2020).

EU support to counter disinformation in the MENA region

The EU's approach to disinformation has evolved in the past five years from one focused especially on targeted disinformation campaigns such as the Kremlin-inspired disinformation campaigns (addressed by the European External Action Service's East StratCom Task Force [ESCTF]) or on confronting the phenomenon of radicalisation in the Arab world, especially to counter ISIS narratives (addressed by the ESCTF), to more inward-looking policies following the interference in the United States Presidential elections in 2016. The domestic efforts to strengthen the EU's own resilience against disinformation are also an important aspect of the EU's engagement to fight disinformation as they can serve as a source of inspiration for both institutional and regulatory solutions, including the Code of Practice on Disinformation (EC, 2018a), the Action Plan against Disinformation (December 2018), the Rapid Alert System (March 2019), the European Democracy Action Plan (2020), the Digital Market Acts (DMA) and the Digital Service Act (DSA, 2020).

In light of the EU's commitment to an open, global and resilient Internet worldwide (EC, 2020), cyber capacity-building constitutes a building block of the EU's cyber diplomacy, including development cooperation programmes, to promote and protect human rights, gender digital equality, the rule of law, and security. The main guiding principles are reflected in the conclusion of the Council of the EU meeting in June 2018. This document integrates internal lessons and best practices from member states and the different initiatives undertaken at the EU level. The Council of the EU conclusion also welcomes the development of "operational guidelines" by the Commission on the EU Cyber Capacity Building in third countries (Council of the EU, 2018). The EU is actively looking for greater coordination at the international level to foster a harmonised approach to cybersecurity and cyber resilience. In this sense, cyber capacity-building plays a key role in strengthening cooperation with other countries.

So far, the EU has funded 37 projects worldwide related to cyber capacity-building (Cybil Portal, n.d.). For example, in terms of the countries under analysis, the EU co-funded the Cyber-

The EU's approach to disinformation has evolved in the past five years from one focused especially on targeted disinformation campaigns to more inward-looking policies

South project with the Council of Europe (CoE, n.d.). This project aims to strengthen legislation and institutional capacities on cybercrime and other electronic offences in line with human rights and rule of law requirements in Algeria, Jordan, Lebanon, Morocco and Tunisia. Yet, disinformation can be addressed through other initiatives. From an ENP standpoint, the EU is actively engaged in many different projects that involve actors that are key to counter disinformation and fake news. Some of them aim to support media in the region, such as "Developing knowledge-based European journalism relating to Europe's Neighbors" (2018-2019), "SouthMed WiA" (2017-2019), and "Open Media Hub" (2016-2019); other projects aim to enhance youth digital skills and awareness, such as "D-Jil" (2018-2022), "Generation What? – Arabic" (2017-2018), and "NET-MED Youth" (2014-2018). Nevertheless, this analysis did not find empirical evidence about former or current EU funded projects or programmes directly aimed at sharing best practices, guidelines or assistance to tackle disinformation in the MENA region. It could be argued that the lack of direct projects to counter disinformation (beyond radicalisation) in the region was determined by two main factors. First, the EU itself has only recently developed a specific and structured set of policies and guidelines to tackle phenomena such as disinformation and fake news in a systematic and structured way. Second, the disinformation issue has only scaled up in the Brussels political agenda in the last few years. In this regard, the topic of disinformation was absent in the Commission's European Agenda on Security 2015-2020, whereas it features as a security threat in the new *EU 2020-2025 Security Union Strategy*.

Conclusions and recommendations

This chapter investigated how Internet governance and in particular policies tackling disinformation during the COVID-19 pandemic could play a role in non-democratic regime strengthening. The results of the study are twofold. First, countries analysed in this chapter seem to prefer the Internet governance approach that resembles the "alignment" model that posits great attention on content control and censorship. Second, the analysis revealed that the regimes' reactions to disinformation on COVID-19 were calibrated to their organisational capacity (the cohesion of the state or governing apparatus) and to the perceived threat that freedom of expression online can pose to the regime. This second argument accounts for the nuances between the countries under analysis, which are all adopting the "alignment" approach. In Morocco, the contested Law 22.20 is suspended, but could be re-activated once the health emergency is over. In Egypt the pre-existing laws have been applied with particular focus on medical personnel, including doctors and nurses. In Jordan, the new Defence Order 8 has also been applied indiscriminately for purposes other than fighting COVID-19 disinformation.

In this context, the EU is missing in action. Yet, during the last few years Brussels has equipped itself with very important policies, which proved to be effective to counter disinformation campaigns in the run up to the European Parliament elections in 2019, and proved to be sufficient to tackle the COVID-19 infodemic. At the same time the EU has included it in its ENP cybersecurity and cyber capacity-build-

ing programmes. Nevertheless, so far, the official cooperation with the MENA region concerning the topic of disinformation, fake news and other informational disorders has been very limited and indirect. As previously mentioned, this lack of action could be related to two reasons. First, because the EU was equipping itself with the right strategy and tools to counter these new challenges. Second, the perceived threats of these phenomena have been recognised officially only recently by the new *EU 2020-2025 Security Union Strategy*.

Nevertheless, because of the growing relevance and, at the same time, increasing threats from cyberspace, finding an agreement at the international level is key. On this, the EU as well as the other international actors should also strengthen their efforts to build up principles, benchmarks and guidelines for managing the Internet at the domestic level. Otherwise, as is currently the case, each state can author its own digital policies, including those violating human rights. Indeed, content control policies could be disguised as policies against fake news, disinformation or other online threats including radicalisation, when, in practice, they could be used to curb opposition movements or civil society groups.

The EU could play an important role in this context as it has defined detailed programmes to tackle disinformation, which have been successful and consistent with the principles of Internet freedom and human rights. In light of this, it is important for future EU actions to contemplate the following recommendations:

1. **The EU should define what type of resilience it would promote in these countries, as there is a possible trade-off between regime resilience and societal resilience.** Given the "aligned" model that these countries are pursuing (in different degrees) to cyberspace governance, the capacity for a state to tackle disinformation is dependent on policies and practices that are against the principle of Internet freedom. For example, it is recommended to support the creation of a network of experts (fact checkers) that can work against disinformation in the selected countries. The model for this could be the "Social Observatory for Disinformation and Social Media Analysis (SOMA)" project. Moreover, the EU is launching the "European Digital Media Observatory (EDMO)" with a focus on four main areas of intervention: fact checking, research, media literacy, policy research and analysis. The overarching idea is to create multiple national observatories in EU member states to act harmoniously against disinformation. The creation of a similar structure in the MENA region could help to counter informational disorders.

2. **The EU needs to exercise caution to avoid its cyber capacity-building projects being used for increased surveillance, censorship and other information control capabilities.** The odds of this possibility are higher in countries where the Internet is considered to be a source of instability. Therefore, when proposing and implementing actions and projects, the EU must consider the cross-cutting issue of a human rights-based approach to cyber capacity-building (EC, 2020b). In addition, it is important that the EU monitors other initia-

tives (legal, technical and informal) undertaken by the beneficiary government that might be contrary to the EU's values or interests.

3. **Government-to-government cooperation is important but the EU should also consider the involvement of other non-state actors, in line with the multi-stakeholders approach to cyberspace.** These should include: CSOs that are working as watchdogs; social media platforms, such as Facebook or Twitter, to also expand their engagement in curbing disinformation in third countries; other donors and international organisations (such as the ITU, the Organisation of Security and Cooperation in Europe [OSCE], and the North Atlantic Treaty Organization [NATO]) that are working on cyber-related issues.

4. From a broader perspective, **it could be useful to strengthen collaborations in the field of cyber and information security with those countries that are still hesitant about their policy preferences regarding international cyberspace norms** or those that consider themselves as part of the NAM. By building up closer cooperation, for example by including more references to cyber- and information-related issues in the ENP partnership priorities, the EU could achieve the so-called "entanglement" (Nye, 2017), which could result in exerting stronger dissuasion for alternative visions on digital topics, including disinformation.

References

ACCESSNOW. (2019). *Cybercrime law in Jordan: pushing back on new amendments that could harm free expression and violate privacy.* Retrieved from https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/

AL-JAGHOUOB, S., & WESTRUP, C. (2003). *Jordan and ICT-led development: towards a competition state? Information, Technology & People,* 16(1), 93-110.

ARAB REPUBLIC OF EGYPT. (2020). *ICT indicators in brief . Ministry of Communication and Information Technology.* Retrieved from http://www.mcit.gov.eg /Upcont/ Documents/Publications_19102020000_ICT _Indicators_in_Brief_ July_2020_EN.pdf

ARTICLE 19. (2015, April). *Egypt: Telecommunication Regulation Law.* Retrieved from https://www.article19.org/data/files/medialibrary/37966/Egypt-telecoms-report—-English.pdf)

ASSOCIATION FOR FREEDOM OF THOUGHT AND EXPRESSION IN EGYPT (AFTEEGYPT). (2020). *Information blockade in the time of social distancing. Quarterly Report on the state of freedom of expression in Egypt second quarter.* Retrieved from https://afteegypt.org/en/breaking_news-2/2020/10/07/20093-afteegypt.html

BANK, A., & EDEL, M. (2015). Authoritarian regime learning: comparative insights from the Arab uprisings (*GIGA Working Paper 274*). GIGA.

BARTLETT, J. (2018). *The people vs. tech: how the Internet is killing democracy (and how we save it).* New York: Penguin Random House.

BROEDERS, D. (2019). Mutually assured diplomacy: governance, 'unpeace' and diplomacy in cyberspace. Observer Research Foundation. Retrieved from https://www.orfonline.org/expert-speak/mutually-assured-diplomacy-governance-unpeace-diplomacy-cyberspace-56800/

BROEDERS, D., & CRISTIANO, F. (2020). Cyber norms and the United Nations: between strategic ambiguity and rules of the road. In S. Dominioni & F. Rugge (Eds.), *Fragmenting the Internet: states' policies in the digital arena.* ISPI Dossier. Retrieved from https://www.ispionline.it/it/pubblicazione/fragmenting-internet-states-policies-digital-arena-25416

BUNCE, V., & WOLCHIK, S. (2011). *Defeating authoritarian leaders in post-communist countries.* Cambridge: Cambridge University Press.

COUNCIL OF EUROPE (COE). (n.d.). *CyberSouth activities.* Retrieved from https://www.coe.int/en/web/cybercrime/cybersouth-activities

COUNCIL OF THE EUROPEAN UNION (COUNCIL OF THE EU). (2018). *EU external cyber capacity building guidelines - Council conclusions.* Retrieved from https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

CYBIL PORTAL. (n.d.). *The knowledge portal for cyber capacity building.* Retrieved February 15, 2021, from www.Cybilportal.org

DE LA CHAPELLE, B., & FEHLINGER, P. (2016). *Jurisdiction on the Internet: from legal arms race to transnational cooperation* (Paper Series 28). Centre for International Governance Innovation and Chatham House.

DEIBERT, J. (2019). The road to digital unfreedom: three painful truths about social media. *Journal of Democracy, 30*(1), 25-39.

DEIBERT, J., PALFREY, J., ROHOZINSKI, R., & ZITTRAIN, J. (Eds.). (2010). Access controlled. *The shaping of power, rights, and rule in cyberspace.* Cambridge: The MIT Press.

DEIBERT, J., PALFREY, J., ROHOZINSKI, R., & ZITTRAIN, J. (Eds.). (2008). *Access denied: the practice and policy of global Internet filtering.* Cambridge: The MIT Press.

DOMINIONI, S. (2020a). Panopticon 2.0? Why and how authoritarian regimes use AI surveillance. In F. Rugge (Ed.), *AI in the age of cyber disorder* (pp. 65-85). Milan: ISPI-Brookings.

DOMINIONI, S. (2020b). Does a North African Internet governance model exist? Evidence from Egypt and Morocco. In V. Talbot (Ed.), *MED Report 2020* (pp. 102-105). Milan: ISPI.

DOMINIONI, S., & RUGGE F. (Eds.) (2020). *Fragmenting the Internet: states' policies in the digital arena.* ISPI Dossier. Retrieved from https://www.ispionline.it/it/pubblicazione/fragmenting-internet-states-policies-digital-arena-25416

EIN-DOR, P., GOODMAN, S., & WOLCOTT, P. (2005). *The global diffusion of the Internet project: The Hashemite Kingdom of Jordan.* The MOSAIC Group. Retrieved from http://mosaic.unomaha.edu/Jordan_1999.pdf

ELTANTAWY, N., & WIEST, J. B. (2011). Social media in the Egyptian revolution: reconsidering resource mobilization theory. *International Journal of Communication,* 5, 1207-24.

EUROPEAN COMMISSION (EC). (2018a). *Code of practice on disinformation.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

EUROPEAN COMMISSION (EC). (2018b). *Operational guidance for the EU's international cooperation on cyber capacity building.* Retrieved from https://www.iss.europa.eu/content/operational-guidance-eu's-international-cooperation-cyber-capacity-building

EUROPEAN COMMISSION (EC). (2020). *The EU's cybersecurity strategy in the digital decade.* Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

FLORIDI, L. (2012). Hyperhistory and the philosophy of information policies. *Philosophy & Technology,* 25, 129-31.

FREEDOM HOUSE. (2011). *Freedom on the Net – Jordan.* Retrieved from https://www.refworld.org/docid/4dad51b627.html

FREEDOM HOUSE. (2019a). *Freedom on the Net – Egypt.* Retrieved from https://freedomhouse.org/country/egypt/freedom-net/2019

FREEDOM HOUSE. (2019b). *Freedom on the Net – Morocco.* Retrieved from https://freedomhouse.org/country/morocco/freedom-net/2019

FREEDOM HOUSE. (2020a). *Freedom on the Net – Egypt.* Retrieved from https://freedomhouse.org/country/egypt/freedom-net/2020

FREEDOM HOUSE. (2020b). *Freedom on the Net – Jordan.* Retrieved from https://freedomhouse.org/country/jordan/freedom-net/2020

FREEDOM HOUSE. (2020c). *Freedom on the Net – Morocco.* Retrieved from https://freedomhouse.org/country/morocco/freedom-net/2020

HUMAN RIGHTS WATCH (HRW). (2020a). *Jordan: free speech threats under Covid-19 response.* Retrieved from https://www.hrw.org/news/2020/05/05/jordan-free-speech-threats-under-covid-19-response

HUMAN RIGHTS WATCH (HRW). (2020b). *Jordan: arrests, forced dispersal at teacher protests.* Retrieved from https://www.hrw.org/news/2020/08/27/ jordan-arrests-forced-dispersal-teacher-protests

INTERNATIONAL REPUBLICAN INSTITUTE (IRI). (2018). *Public opinion survey: residents of Jordan.* Center for Insights in Survey Research. Retrieved from https://www.iri.org/sites/default/files/2018.11.6_jordan_poll_presentation.pdf

INTERNET CENSORSHIP MAP. (2017). Retrieved from https://www.whoishostingthis.com/blog/2017/02/27/internet-censorship/#africa

KALATHIL, S., & BOAS, T. C. (2003). *Open networks, closed regimes: the impact of the Internet on authoritarian rule.* Washington D.C.: Carnegie Endowment for International Peace.

KAVANAGH, J., & RICH, M. D. (2018). T*ruth decay: an initial exploration of the diminishing role of facts and analysis in American public life.* Santa Monica: RAND Corporation.

KEREMOĞLU, E., & WEIDMANN, N. B. (2020). How dictators control the Internet: a review essay. *Comparative Political Studies,* 53(10-11), 1690-703.

KERR, J. (2018). Information, security, and authoritarian stability: Internet policy diffusion and coordination in the former Soviet region. *International Journal of Communication,* 12, 3814-34.

LANNON, E. (2019). EU cybersecurity capacity building in the Mediterranean and the Middle East. Strategic sectors security & politics. *IEMed Mediterranean Yearbook.* Retrieved from https://biblio.ugent.be/publication/8651360/file/8651361.pdf

LEVITSKY, S., & WAY, L. (2010). *Competitive authoritarianism. Hybrid regimes after the Cold War.* Cambridge: Cambridge University Press.

MEBTOUL, T. (2020, July 28). Moroccan court convicts woman who claimed COVID-19 is fake news. *Morocco World News.* Retrieved from https://www.moroccoworldnews.com/2020/07/312804/moroccan-court-convicts-woman-who-claimed-covid-19-is-fake-news/

MUELLER, M. (2017). *Will the Internet fragment?* Cambridge: Polity Press.

NEMITZ, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions Royal Society A*, 376(9).

NON-ALIGNED MOVEMENT (NAM). (2020). *NAM working paper for the second substantive session of the UN OEWG.* Retrieved from https://front.unarm.org/wp-content/uploads/2020/04/nam-wp-to-the-oewg-final.pdf

NYE, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security,* 41(3), 44-71.

OPENNET INITIATIVE. (2009). *Egypt.* Retrieved from https://opennet.net/research/profiles/egypt

PLATTNER, F. M., & DIAMOND, L. (Eds). (2012). *Liberation technology: social media and the struggle for democracy.* Baltimore: John Hopkins University Press.

REPORTERS WITHOUT BORDERS. (2016). *The new press code retains prison sentences for press offences.* Retrieved from https://rsf.org/en/news/new-press-code-retains-prison-sentences-press-offences

RØD, E. G., & WEIDMANN, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research,* 5(3), 338-51.

SALEH, N. (2012). *Egypt's digital activism and the dictator's dilemma: an evaluation.* Telecommunications Policy, 36, 476-83.

SCHEDLER, A. (2013). *The politics of uncertainty. sustaining and subverting electoral authoritarianism.* Oxford: Oxford University Press.

STOLTON S., & GRÜLL, P. (2021). *Lawmakers call for tougher EU disinformation laws in wake of US riots. Euractive.* Retrieved from https://www.euractiv.com/section/digital/news/lawmakers-call-for-tougher-eu-disinformation-laws-in-wake-of-us-riots/

UNITED NATIONS OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF ICT IN THE CONTEXT OF INTERNATIONAL SECURITY (UN OEWG). (2020). *Comments by Member States on the initial pre-draft of the OEWG report.* Retrieved from https://reachingcriticalwill.org/disarmament-fora/ict/oewg/documents

UNITED NATIONS OPEN-ENDED WORKING GROUP ON DEVELOPMENTS IN THE FIELD OF ICT IN THE CONTEXT OF INTERNATIONAL SECURITY (UN OEWG). (2020). *Informal multi-stakeholder cyber dialogue summary report* (04-10 December 2020). Retrieved from https://eu-iss.s3.eu-central-1.amazonaws.com/horizon/assets/X5Hf8NIU/informal-ms-dialogue-series_summary-report_final.pdf

WEIDMANN, N. B., & RØD, E. G. (2019). *The Internet and political protest in autocracies.* Oxford: Oxford University Press.

WHEELER, D. L. (2003). Egypt: building an information society for international development. *Review of African Political Economy,* 30(98), 627-42.

WORLD BANK. (2020). *Individuals using the Internet (% of population) – Jordan*. Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=JO

XU, X. (2020). To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science*, 65(2), 309-25.

YOM, S. L. (2009). Jordan: ten more years of autocracy. *Journal of Democracy,* 20(4), 151-66.

ZOLLO, F. (2019). *Polarization in the online public debate.* ISPI Commentary. Retrieved from https://www.ispionline.it/it/pubblicazione/polarization-online-public-debate-23150

Preventing Cyber Conflicts and Instability

Patryk Pawlak
Brussels Executive Officer, European Union Institute for Security Studies (EUISS)[1]

[1] The views expressed in this chapter are those of the author and do not necessarily reflect the official position of the EUISS.

Introduction

The European Union (EU)'s security partnership with the Southern Mediterranean partners has developed along a triple nexus: humanitarian aid, development cooperation, and peace-building. Despite a quarter-century old commitment to turning the Mediterranean basin into an area of dialogue, exchange and cooperation, guaranteeing peace, stability and prosperity, the region continues to be plagued by conflicts that undermine political stability and sustainable development across the region. The increasing reliance by governments and non-state actors on cyber tools adds to this already complex picture and further exposes political, economic and societal causes of vulnerability across the region. Consequently, joint efforts between the EU and its partners in the Southern Mediterranean aimed at preventing and resolving cyber-enabled or cyber-facilitated conflicts and addressing the root causes of conflict offer a valuable avenue for inter-regional cooperation. Together with the commitment to respect for international law and rules-based order, these elements are key pillars of a framework for promoting responsible state behaviour in cyberspace.

The EU has expressed its commitment to this framework on numerous occasions and is uniquely placed to bring together international and regional partners as well as relevant stakeholders to promote it across the region. This objective seems particularly important **given the fragile security situation in the region and the fact that many countries therein rely on cyber tools to build up their security posture. This also implies that the use of offensive and defensive cyber tools in interstate and intrastate relations in the Middle East and North Africa (MENA) context is a question of "when" rather than "if".** In the MENA region, "geopolitics is at a critical inflection point where the cyber domain is becoming a principal frontline" (Kausch, 2017).

Until now, however, the EU's engagement with the countries across the Mediterranean has remained relatively limited. Concerned about potential human rights abuses by military, law enforcement or intelligence agencies, on the one hand, and still weak checks-and-balances system across the region, on the other, the EU has been walking on eggshells when it comes to cyber capacity-building initiatives in the region. Reputational political risks resulting from any potential power abuse as a result of the EU's support are often judged too high. The requests for closer cooperation on cybersecurity from Egypt and Lebanon, for instance, have fallen on deaf ears in light of the ambivalent role of the intelligence agencies as security providers.

The purpose of this chapter is to analyse the increasing importance of cyberspace as an arena of geopolitical competition, the potential impact this might have on the region's stability, and the role it plays in shaping this environment. The efforts across the region to develop adequate legislative frameworks or institutions to strengthen the overall level of cyber resilience go hand in hand with the deployment of offensive cyber operations and tools in the ongoing political or military conflicts. Public reports have previously implicated Israel, Iran and Turkey, for instance, in the use of cyber operations in support of their political objectives. In

addition, the military involvement of the United States of America (USA) and the expanding presence of actors like China and Russia in the region complicate the situation further. **If anything, cyber-related developments in the region illustrate that cyberspace is just one additional domain for pursuing political and economic objectives, in particular in the context of pre-existing intra- or interstate conflicts.** This chapter is based on the analysis of primary sources such as the United Nations (UN) voting patterns of 18 countries in the region and the speeches and positions presented during the meetings of the Open-Ended Working Group in the Field of ICT in the Context of International Security (UN OEWG) in 2020 and 2021. Policy recommendations presented at the end are aimed at supporting the design and implementation of the EU's engagement with the region, including the regional organisations.

Cyber tensions in the MENA region

The history of the MENA region is one of instability, with cyberspace being yet another theatre for pre-existing conflicts – both domestic and regional. Since the first publicly debated offensive cyber operation with the use of Stuxnet malware (which continues to raise questions until this day), the region has become a laboratory for different uses of cyber tools by governments and non-state actors. Over time, the **MENA region has evolved to become one of the most cyber-militarised parts of the world whereby "cyber weapons" are used by states to resolve their ongoing political, economic or military tensions or by governments as an instrument of oppression targeting their own population.** The increased state activism in cyberspace has influenced the way in which many states defined emerging threats in cyberspace (as also discussed in the previous chapters of this study). For instance, Iran defined them as a threat or use of force in terms of the information and communication technologies (ICT) environment, interference and ICT abuse, unilateral coercive and other measures in the ICT environment, threats arising from "content", hostile image-building and fabricated attribution in the ICT environment, imbalance between the role and responsibility of states and those of the private sector, abuse of emerging technologies, and abuse of the ICT supply chain.

According to the Cyber Conflict Portal (EU Cyber Direct, 2020), **most military cyber operations across the region have a dyadic relationship and build on pre-existing political tensions between states, including from outside of the region** (e.g., between Iran and the USA and its allies). However, over time, the picture became more complex with the emergence of new players – both state and non-state – with different capabilities and motivations. In 2017, media reports suggested the involvement of the United Arab Emirates (UAE) in the attacks against the Qatar News Agency, branded by the government as a violation of international law (DeYoung, 2017). The attack was inscribed into a broader conflict between the Emirates, along with Saudi Arabia, Bahrain and Egypt, who accused Doha of supporting terrorist groups and allying with regional foe Iran. Additional reports released in February 2021 suggest that Saudi Arabia and the UAE have reportedly used spyware created by an Israeli company to hack into phones and

devices of journalists working for Al Jazeera (Middle East Monitor, 2021). In one of the latest episodes, the UAE became a target of cyberattacks after it decided to normalise relations with Israel and break with decades-long Arab solidarity on that issue.

One of the most complex challenges is that of the existing links and mechanisms of control between the official government agencies and non-state actors acting as proxies

One of the most complex challenges is that of the existing links and mechanisms of control between the official government agencies and non-state actors acting as proxies (Mauer, 2018). State responsibility for the actions of these actors is often difficult to establish, which complicates the task of making the perpetrators accountable for malicious cyber activities. Iran is among the countries suspected of conducting cyber operations in the region and beyond. In October 2020, the Iranian Advanced Persistent Threat (APT) actor APT35 was identified as responsible for attacks on over 100 high-profile potential attendees of the Munich Security Conference and the Think 20 Summit in Saudi Arabia. In 2018, another report by the Electronic Frontier Foundation (EFF, 2018) and mobile security company Lookout uncovered a new APT actor called Dark Caracal, which was responsible for a cyberespionage campaign against targets in more than 20 countries. The authors trace back the threat to a building belonging to the Lebanese General Security Directorate in Beirut (Electronic Frontier Foundation, 2018). In that respect, the role of cyber proxies across the region poses a significant challenge to stability and undermines de-escalatory and conflict prevention efforts undertaken by various actors (Kavanagh & Cornish, 2020).

The region is also fertile ground for operations mounted by politically-motivated non-state actors. The Gaza Cyber Gang, for instance, is a politically-motivated Arab group operating in the MENA region targeting mainly Egypt, the UAE and Yemen. Bahamut is another group running cyberespionage campaigns against various political, economic and social sectors in the Middle East. In 2000, the Bahamut group was suspected of being behind attacks against Saudi diplomats, Sikh separatists, and others in the MENA region. In other words, when it comes to the use of cyber tools by states against each other, the MENA region has seen higher intensity of malicious activities within the region than any other part of the world. But, as some authors observe, this mostly inner-Gulf confrontation could develop into a larger block confrontation as many regional powers expand their relations with China, Japan, India and Russia to hedge against uncertainty surrounding continued engagement by the USA and Europe (Kausch, 2017).

In addition, the intrastate conflicts have been exacerbated by the wide use of **cyber surveillance and armies of bots by repressive governments against their own societies, human rights defenders or political opponents.** The past decade has seen a general trend of states increasing control over their populations in cyberspace[2] in response to a growing role of social media platforms (of which the Arab Spring is the most vivid example) and the use of the Internet by terrorist organisations. While the two are not related, governments across the region have approached both as a national security threat that needs to be countered through a decisive response that came in many forms. The control

[2] See also chapters by Dominioni and Laban.

over online activities is one of them. Blurring the lines between freedom of political or religious expression and national security, some countries engaged in cyber espionage against journalists, human rights defenders or activists. In Morocco, the Hirak protest leaders in Morocco were victims of social engineering campaigns aimed at gaining access to their mobile phones (Sayadi, 2019). Such measures are often taken on the basis of recently adopted cybercrime laws that give broad powers to national security agencies without simultaneously strengthening the rule of law mechanisms and independent judiciary. The 2018 cybercrime law adopted in Egypt, for instance, compels Internet service providers to store user data for its hypothetical request by security agencies (Švedkauskas, 2019). The region is an important client for Russian and Chinese technologies for communications interception and surveillance or active private companies such as NSO or Black Cube with licences granted by some of the EU member states under the dual-use export regime (Goslinga & Tokmetzis, 2017). The "rise of digital authoritarianism" across the region is well-documented by Freedom House.[3]

Development-security paradox

One of the main drivers of the EU's involvement in the Mediterranean is the assumption that there cannot be security without development, or development without security. This mantra has served as justification for the EU's economic and political commitment to the region. But the understanding of this causal link when it comes to governance of cyberspace is not always present in the EU policies towards the region or shared between the EU and its partners. In that respect, the apparent development-security paradox reflects broader political issues and insecurities felt by the governments across the region.

First, the growth of the digital sector and closing the digital gap are generally believed to stimulate innovation, promote growth and strengthen freedoms. In principle, governments recognise the benefits of ICT for the social and economic development of their countries. In an effort to stimulate that growth, they often stress that "access to new information and communications science, technologies and techniques should be available to all countries" and object to any unilateral measures that restrict such access.[4] This concern is not only characteristic of countries like Iran, whose access to such technologies is already severely limited due to the USA-imposed sanctions, but also others that are on the receiving end of potential export controls or sanctions.

Second, like Iran, governments across the region also stress that "the development-related dimension and the security-related concerns of ICT shall be addressed in a balanced manner" (UNODA, 2019). Such a cautious approach is primarily linked to the per-

[3] See the Freedom on the Net reports published regularly at: https://freedomhouse.org/report/freedom-net

[4] Unless indicated otherwise, this paper is primarily based on the positions expressed by the mentioned countries in the debates of the UN OEWG, available here: https://www.un.org/disarmament/open-ended-working-group/

ceived need to exercise a certain degree of digital sovereignty that allows governments to make independent decisions about policies that reflect values and cultures of individual societies – even though they may not entirely correspond to those of others. For some countries, referencing development has simultaneously become a way of calling for more security. In one of its submissions to the UN OEWG, Iran recalled that it is "the sovereign right of all UN member states to invoke their rights and responsibilities to increase incredible benefits and advantages of ICT and mitigate destabilising impacts emanating from their malicious use" (UNODA, 2019). However, the persisting disagreements on what may constitute a malicious use or destabilising impact – especially in countries with questionable human rights standards – results in tensions over a governmental abuse of ICT tools.

The discussion about the emerging threats has provided an insight into what states consider to constitute acceptable behaviour in cyberspace

Third, the discussion about the emerging threats has provided an insight into what states consider to constitute acceptable behaviour in cyberspace and their different approaches to the linkages between security and development. Egypt, for instance, considered a failure to use ICT peacefully as a serious threat to security and stability as well as economic development and prosperity of the nations. This view is particularly pronounced in the debate about critical infrastructure (CI) protection, such as water, energy or transportation networks, which should be interpreted as a basic developmental issue given the reliance of the civilian population. Consequently, Egypt calls for legally binding obligations that would prohibit the use of ICT against CI facilities providing services to the public or measures to address the threats of stockpiling vulnerabilities which could be used for attacks against such infrastructure.[5] This, however, is not necessarily the position put forward by Israel, which in its most recent comments on the draft zero of the UN OEWG report requested to delete references to medical facilities, energy, water, transportation and sanitation. Given that Israel has been accused of conducting the first offensive cyber operation, Stuxnet, against Iran's nuclear facilities (Zetter, 2014) and attacks against Syria's Air Defence Systems in 2007 (Weinberger, 2007) – both of which could be argued to be CI – such a request might be interpreted as an attempt to avoid potential responsibility. At the same time, a request to make a less explicit causal link between disruption, damage or destruction of CI and critical information infrastructure as a threat to economic development and livelihoods, and ultimately the safety and wellbeing of individuals, indicates that in Israel's view in some cases such infrastructure represents a legitimate security target.

In that respect, the security-development nexus is often instrumentalised by the governments in the region to pursue two objectives. The calls to limit the proliferation of offensive cyber tools and prevent over-militarisation of cyberspace are in reality meant to constrain technologically advanced countries rather than promote a development-oriented cyber agenda. At the same time, the arguments for a balanced approach in reconciling se-

[5] This is a clear reference to the vulnerability of stockpiling that has led to WannaCry and NotPetya attacks, which had significant economic consequences around the globe, leading, for instance, to the adoption of cyber sanctions by the EU.

curity and development objectives serve to justify governments' control over cyberspace (including through surveillance and content control measures) or to object to any potential external interference in pursuit of "illegitimate geopolitical goals."

Conflict prevention and responsible state behaviour in cyberspace

The framework of responsible state behaviour in cyberspace is composed of four main pillars as developed in the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE) reports: application of international law in cyberspace; norms, rules and principles; confidence-building measures (CBMs), and capacity-building. Against a deteriorating cybersecurity environment and potential for conflict and escalation in the region, as described earlier, it is surprising that only a handful of the MENA countries have been actively contributing to defining these policies and shaping the international debate. Among rather muted voices from the region, Egypt's and Iran's are clearly the loudest. What is not clear, however, is to what extent their views reflect a broader consensus across the region or maybe are meant to contribute to shaping such a consensus. In other words, are Iran and Egypt speaking *for* or *to* the region?

At the same time, while countries like Turkey or Israel, whose capabilities have been recognised as significant, have not participated extensively in the ongoing diplomatic processes, their actions speak louder than words. Israel, for instance, has been engaged in strengthening bilateral cybersecurity cooperation in the region, including with the EU member states like Cyprus or Greece. In April 2021, Israel appeared to admit its involvement in a cyberattack on Iran's nuclear facility in Natanz – one of the main components of Iran's nuclear programme. But Israel itself is also a frequent target of malicious cyber activities. In May 2021, several Israeli companies claimed to be victims of cyberattacks that were linked to Iran. Turkey, on the other hand, has relied more on hacktivist groups or cyber patriots who used malicious cyber activities to express their discontent with any views critical of Ankara's policies. In December 2020, the European Court of Human Rights was hit by a large-scale cyberattack after it published a ruling critical of Turkey. A hacker group, Phoenix Warriors Team (Anka Neferler Timi) has claimed responsibility for this and earlier attacks against targets in Greece.

The following sections of this chapter focus on the positions expressed by governments in the official UN-led processes.

Regional powers: a silent majority

Despite their membership of the UN GGE and the role they might potentially play in shaping the cyber stability debate across the MENA and the Gulf, countries like **Jordan, Algeria, Morocco, Oman, Lebanon, Israel and Turkey** have been rather absent. This is particularly disappointing in the case of Jordan and Morocco, which as members of the UN GGE that presented its final report in June 2021 (UN, 2021), and other countries that could potentially play an important role in bringing different parties together.

Oman, for instance, played an instrumental role in the evolution of the Iran nuclear deal and in providing support during the Yemeni crisis (Winder, 2020). Oman's relatively low profile and foreign policy built around neutrality has allowed it to exercise considerable influence behind the scenes and act as a broker between competing regional powers such as Iran, Israel and Saudi Arabia (Bodetti, 2020). But it does remain silent on critical issues in the cyber stability debate. The following sections provide a limited account of the views and positions expressed by those countries regarding their priorities.

In one of the rare interventions at the UN OEWG, **Jordan** has called for focusing the discussion on two issues in particular: development of norms to counter threats and challenges for the international community and clearly denoting those norms that facilitate international cooperation as well as identification of mutual threats and challenges. It further stressed the key role of UN agencies and regional organisations in building digital inclusion and strengthening cyber resilience in all sectors: food, water, health, education, and economic development.

Algeria stressed that benefits from ICT cannot be taken for granted and also highlighted threats emanating from the use of digital technologies: manipulation of information with malicious intent; cyberattacks on CI, such as hospitals and electrical grids; and militarisation and weaponisation of cyberspace through the development of cyber offensive capabilities and the risks of turning cyberspace into a theatre of military operations. In that respect, Algeria underscored the importance of ensuring the full respect for the purposes and principles of the UN Charter in the use of such technologies; namely, the principles of sovereign equality, non-interference in internal affairs, refraining from the use of force in international relations, respect for human rights, and peaceful coexistence among states.

The role of **Israel, Lebanon and Turkey** is more nuanced given their involvement in conducting cyber operations and de facto setting the rules of the game on the ground. For instance, while Israel may have been a rather muted participant in the UN OEWG, its actions usually speak quite loudly. Israel is commonly acknowledged to set standards for what does and does not constitute acceptable behaviour in cyberspace. "Lethal Arrow", a large-scale military exercise conducted by the Israel Defense Forces in October 2020, included a cyber component involving the targeting of infrastructure and personnel of Hezbollah (Gross, 2020). Israeli company Circles, affiliated with the Israeli software broker NSO Group, was also singled out in a report by the Citizens Lab exposing suppliers of surveillance technologies around the globe (Marczak et al., 2020). Submissions by **Turkey** have focused on two dimensions in particular: CBMs and capacity-building. Regarding the former, the Turkish position stressed the importance of establishing communication channels among countries for emergency situations with a view to countering cyber threats and sharing information and resources through those channels. Such mechanisms across the region are currently lacking.

Despite these limited interventions, there are a number of commonalities in the positions adopted across the region, albeit not always aligned with

the EU (see table 1 below). With regard to responsible state behaviour in cyberspace, most countries in the region have preferred not to choose between the positions presented by the USA and likeminded countries or Russia, China and their supporters. The MENA countries have supported both resolutions contributing to a duopoly of initiatives at the UN level within the UN GGE and UN OEWG. Regarding the fight against cybercrime, the region has departed from the position adopted by the EU and voted in support of the Russia-sponsored resolution calling for the establishment of a new Ad Hoc Committee on Cybercrime with an international binding instrument as a possible outcome.

Table 1. Voting patterns in the UN General Assembly on key cyber-related resolutions

	Cybercrime	International security & ICT		Responsible behaviour	
	2019	2019	2020	2019	2020
	A/RES/74/247	A/RES/74/29	A/RES/75/240	A/RES/74/28	A/RES/75/32
Algeria	Y	Y	Y	Y	Y
Bahrain	A	Y	Y	Y	Y
Egypt	Y	Y	Y	N	A
Iran	Y	Y	Y	N	N
Israel	N	N	N	Y	Y
Jordan	Y	Y	Y	Y	Y
Kuwait	Y	Y	Y	Y	Y
Lebanon	Y	Y	Y	A	A
Libya	Y	Y	A	Y	Y
Morocco	A	Y	Y	Y	Y
Oman	Y	Y	Y	Y	Y
Qatar	Y	Y	Y	Y	Y

Saudi Arabia	A	Y	Y	Y	Y
Syria	Y	Y	Y	N	N
Tunisia	A	Y	Y	Y	Y
Turkey	A	A	N	Y	Y
UAE	Y	Y	Y	Y	Y
Yemen	Y	Y	Y	Y	Y
EU	N	A	N	Y	Y

Source: Author's compilation based on data from the UNGA (2019 a-c & 2020 a-b).

Note: Light blue stands for the same vote by the EU and a third country, dark blue stands for the opposite vote and white stands for no conflict in the expressed positions.

One of the items where there seems to be an overarching agreement across the region is the support for new international treaties. According to Algeria, a new treaty that takes into account "the concerns and interests of all states" would contribute to constraining actions that may lead to destabilisation and be "fully dedicated to international cooperation on safeguarding peaceful uses of ICT."[6] The Syrian delegation to the UN OEWG was more outspoken on the topic, claiming that "some states believe that absence of such an instrument allows other states to behave irresponsibly and develop cyber capacities that can be used against other states." Similarly, there seems to be a convergence of views across the region when it comes to fighting cybercrime with many countries flagging combating "cyber terrorism" and the "terrorist use of ICT" as a serious threat. However, the lack of a universally accepted definition of terrorism – or of cybercrime for that matter – in the region and a rather broad scope of definitions adopted at the national level make cooperation on this topic rather difficult. This also translated into views on cybersecurity capacity-building which, as expressed among others by Turkey, "should be realised without conditionality" (UNODA, 2021b).

Egypt and Iran: systemic challengers

There is no doubt that both Iran and Egypt have a clear interest in making their voices heard. And even though their ultimate goal of diminishing the Western influence over the governance of cyberspace and its resources (e.g., in terms of infrastructure, regulation and "monopoly of power") seems to overlap, they each pursue this objective with a different approach. **While Egypt has opted to pursue the path of moderate contestation by acknowledging the progress achieved to date and stress-**

[6] Quotations from an intervention by Algeria at the UN OEWG during the informal inter-sessional meeting in September 2019. Available at: https://media.un.org/en/asset/k1x/k1xubugkf4

ing the need for further work, Iran has contested the past progress and adopted a more revisionist approach. According to Iran, for instance, the 2015 UN GGE report endorsed by the UN General Assembly cannot be read as a consensus document given that it was drafted and agreed upon by a small number of countries. Nevertheless, a significant degree of convergence in their positions (see table 2) needs to be acknowledged and addressed, especially given the impact they have in shaping the positions of the country-members of the Non-Aligned Movement.

Iran's approach is not too surprising given that it is often singled out as a "rogue state" in cyberspace due to its extensive malicious cyber operations. Iran's alleged interference in the United States presidential elections in 2020 is just one example. The United States Department of Justice seized 92 domains used in Iranian global disinformation and the United States Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued an alert warning against Iranian state-sponsored cyber operations against several state and election-related websites. In September, Twitter had already announced the removal of 130 Iranian Twitter accounts amplifying conversations on politically sensitive topics, including Black Lives Matter, the murder of George Floyd, and other issues of racial and social justice in the USA. Ultimately, the United States Department of Treasury sanctioned five Iranian entities: Islamic Revolutionary Guard Corps (IRGC), IRGC-Qods Force (IRGC-QF), Bayan Rasaneh Gostar Institute (Bayan Gostar) as well as the Iranian Islamic Radio and Television Union (IRTVU) and the International Union of Virtual Media (IUVM) owned or controlled by the IRGC-QF.

Table 2. Comparison of positions addressed in the UN OEWG submissions

Issue/Positions	Iran	Egypt
Binding international instrument	Yes	Yes
Instrumentalisation of international law	Yes	No
New norms	Yes	Yes
De-militarisation of cyberspace	Yes	Yes
Limits on stockpiling vulnerabilities	Yes	Yes
Common but differentiated responsibilities (CBDR)	Yes	Yes
De-monopolisation of resources	Yes	No
Support for UN OEWG	Yes	Yes
Support for the Programme of Action	No	Yes
Utility of CBMs	No	Yes
Degree of contestation	High	Moderate

Source: Author's compilation based on positions expressed during the UN OEWG (2019-2021).

In response, Iran pursues a coherent approach built on two pillars: (1) undermining the West's claim of higher moral ground when it comes to cyberspace by exposing its cyber operations and stressing progressing militarisation of cyberspace to which it contributes, and (2) proposing alternative interpretations of the existing principles of international law and norms of responsible behaviour in cyberspace. The ultimate objective of both is to weaken the Western narrative about Iran's offensive and irresponsible actions in cyberspace and consequently challenge the credibility of the sanctions system – "coercive unilateral measures" – that was put in place and which over the past years has significantly limited Iran's access to new technologies. This narrative is skilfully sold under the guise of the need for more cyber capacity-building in order to support developmental progress and growth.

One of the mechanisms to achieve this has been Iran's active role in shaping the conversation about the application of existing **international law** to cyberspace by stressing that "the applicability of existing international law in cyber-related areas is still an unclear domain" and the need for a new "legal multilateral and inclusive framework for the peaceful ICT environment." Iran makes an interesting argument that the envisaged international law as "common heritage of mankind" would encompass non-appropriation and shared governance, its integrity and states' intrinsic right to access and commitment to transfer of technology. Furthermore, the new cyber specific body of law should not be open to "manipulation and biased interpretation by those who have dominance in ICT environment, especially states with offensive cyber strategies and capabilities" (UNODA, 2020b).

Iran has been particularly outspoken regarding all forms of interference through cyber-related ways and means directly or indirectly and for any reason in the internal or external affairs of other states

Regarding specific norms and principles of international law, Iran's arguments – and to some extent those presented by Egypt and other countries in the region, as discussed earlier – have aimed at curbing potential cyber operations by the West against targets in the region. This approach stems directly from the way in which the region perceives major threats in cyberspace. On the top of the list are the cyberattacks against the critical civilian infrastructure and associated information systems. Recognising the fact that the lines between civilian and military information infrastructure are often blurred, any cyberattack might ultimately have negative consequences for the civilian population. Therefore, the "stockpiling vulnerabilities", security of supply chain and risks associated with malicious uses of "mass computing technologies" or "autonomous cyberattacks" provided a context for making concrete claims about international law.

Iran has been particularly outspoken regarding all forms of interference through cyber-related ways and means directly or indirectly and for any reason in the internal or external affairs of other states. In its submissions it stressed the need to strengthen the role of states as bearing the primary responsibility for maintaining "a secure, safe and trustable ICT environment," in particular by strengthening state sovereignty "without affecting the rights of the states in making their choice of development, governance and legislation models […]" (UNODA, 2020a). This is linked directly to a concern expressed regularly by Iran about unilateral coercive measures. Accordingly,

Iran has tabled a new norm whereby "states should take steps in a way to balance their security and development of nations" including states' right to the "supply chain including ICT-related research and development as well as manufacturing, utilising and transferring ICT products and services" (UNODA, 2019). Furthermore, Iran has also emphasised the need for states to meet their obligations regarding internationally wrongful acts, although it added that such acts should be attributable beyond a reasonable doubt and that an indication that an ICT activity was launched or otherwise originated from the territory or objects of the ICT infrastructure of state may be insufficient in itself to attribute this activity to that state. Iran described "hostile image-building and fabricated attribution" as one of the emerging threats in cyberspace (UNODA, 2020a). Finally, Iran has also expressed concerns when it comes to focusing on elements such as the "right to self-defence" under article 51 of the UN Charter and the applicability of the rules of engagement in military conflicts in the ICT context. In its view, such discussions may intentionally or unintentionally legitimise or encourage turning the ICT environment into an arena of conflict. An exaggerated focus on these specific aspects and their associated legal controversies and attribution challenges might divert attention from addressing the right questions on how to cooperate to prevent such conflicts from occurring in the first place.

Egypt, on the other hand, has assumed a more active role regarding **norms and principles of responsible state behaviour.** The main argument presented by Egypt is that there is a need to step up international efforts to develop rules on ICT security consistent with international law, in order to sustain an open, secure, stable, and peaceful ICT environment in the long term. Consequently, Egypt insisted that the UN OEWG should focus on "transforming and upgrading" the existing voluntary recommendations that have already been endorsed into more operational and binding commitments that specifically address the most relevant conflict scenarios in the ICT environment, pending the conclusion of appropriate multilateral legally binding obligations. According to Egypt, the most appropriate way forward would be a conclusion of a Political Declaration that reflects the commitment of the member states to adhere to the 11 recommendations in the 2015 UN GGE report and to step up their implementation, in particular regarding refraining from: (1) knowingly or intentionally damaging or otherwise impairing the use and operation of critical civilian infrastructure under any circumstances; (2) limiting the access of other states to the Internet; (3) stockpiling ICT-related vulnerabilities; and (4) harming the information systems of the authorised emergency response teams of other states. In terms of positive obligations, Egypt's position focused in particular on states' obligations to address potential vulnerabilities in the national infrastructure and information systems resulting from the use of harmful hidden functions and compromising the integrity of the ICT products' supply chain. It also called for states to take coordinated measures towards the voluntary exchange of relevant information including on best practices and possible threats and vulnerabilities. Iran's contribution to the discussion about norms was more upsetting for the commonly accepted status quo as expressed in the UN

GGE reports. According to Iran, although states have a prerogative to implement, if they wish, the envisaged norms, it is "premature" for the UN to speak about norm implementation and guidelines. Instead, the UN OEWG should, in their view, "accelerate its work to finalise a balanced and comprehensive list of norms while working on a set of agreed terminologies" (UNODA, 2020a). But, ultimately, Iran and Egypt converge in their view that without a legally binding instrument regulating behaviour of state and non-state actors in cyberspace, implementation of voluntary norms will not be a silver bullet for the states' actions in cyberspace.

Another aspect particularly relevant for the MENA region is the development and implementation of the **CBMs.** As described earlier, the levels of mistrust between countries are relatively high and therefore measures aimed at reducing risks of escalation of conflict should be considered a priority. This, however, is not the case. In an effort to remedy the situation, Egypt has called in the UN OEWG for states to reach an agreed common definition of what constitutes "CI", with a view to agreeing, as appropriate, on prohibiting any act that knowingly or intentionally utilises offensive ICT capabilities to damage or otherwise impair the use and operation of CI. Such suggestions are indeed a very important development given that attacks against energy or water infrastructure might be the most prone to escalation. In Egypt's words, "the voluntary sharing of information on various aspects of national and transnational threats and vulnerabilities, as well as best practices for ICT security, are powerful tools that should be utilised, as appropriate, in a more systematic and harmonised manner in the context of a multilateral inclusive specialised forum" (UNODA, 2020c). Iran, on the other hand, has presented the opposite view arguing that the origins of CBMs are linked to weaponry and military history and as such should not be applied in cyberspace. Instead, Iran argues that CBMs in cyberspace should be tailored to the unique features of cyberspace and address what it sees as the main sources of mistrust in the ICT environment: the monopoly in Internet governance, anonymity, offensive cyber strategies, hostile image-building and xenophobia, and lack of responsibility of private companies and platforms (UNODA, 2020a). The reference to fairer Internet governance is not surprising given Iran's dependence on Internet infrastructure that is primarily managed by Western private companies.

Finally, regarding **cyber capacity-building**, the positions of Egypt and Iran point to two distinct aspects that so far have been largely neglected but do shape views in this policy area. Egypt in its interventions has stressed the importance of the **principle of common but differentiated responsibilities** (CBDR) when it comes to cybersecurity. Although well-established in international environmental law and formalised in international law at the 1992 UN Conference on Environment and Development in Rio de Janeiro, the CBDR principle has not been discussed in the context of cyberspace governance (Epstein, 2021). This proposal is not surprising, however, given that the common thread through most of the interventions made by representatives of the developing countries points to a clear difference in the level of technological advancement and the uses of cyberspace. In general, states acknowledge that they have a shared

responsibility for the development of cyberspace and that not all states have capabilities to deliver what is expected of them. The application of the CBDR principle to cybersecurity would depart from the common understanding that all states should reach a similar level of cyber maturity accepted globally. Instead, it requires the international community to accept that the applicability of standards that are valid for the most advanced countries "may be inappropriate and of unwarranted social cost for the developing countries."[7] As such, the CBRD principle calls for accepting that each state has a different set of capabilities that they can contribute to this project. This also corresponds to the argument presented by Egypt that "the provision of assistance and cooperation should be demand-driven and made upon request by the recipient state, taking into account its specific needs and particularities."

A similar position has also been presented by Iran. However, Iran's focus on **de-monopolisation of Internet resources** through capacity-building also played to a different audience that is very sensitive towards new ideas such as "tech colonialism" (Arnold, 2005) or "digital colonialism" (Hicks, 2019). Iran argues that the benefits of ICT cannot be fully realised "unless technological, infrastructural and informational needs are met, including through de-monopolisation and facilitation of access to and transfer of new ICT-related science and technologies." As in the case of CBMs, cyber capacity-building should therefore serve to disarm what it calls "unilateral digital sanctions" which affect investment in ICT infrastructures as well as access to digital technologies, digital resources (e.g., Internet Protocol addresses and the Domain Name System and networks). As a consequence, Iran sees any such measures as having an overall negative impact on economic growth and development of whole populations. At the same time, it also notes that capacity-building "shall not disturb states' national security and interests, social ethics, and public order."

States acknowledge that they have a shared responsibility for the development of cyberspace and that not all states have capabilities to deliver what is expected of them

Conclusions and recommendations

Advancing responsible state behaviour in cyberspace is a cornerstone of the EU's cyber diplomacy and is deeply rooted in the EU's ambition to act as a security provider, especially in its neighbourhood. Through activities at the UN and in other regional organisations, the EU has promoted adherence to the existing international law, norms and principles, and the CBMs in cyberspace. However, engagement on these topics with the MENA region is to a large extent non-existent. This is surprising given that the EU has committed significant resources towards cyber-related capacity-building, including in the Southern Neighbourhood.

With digital transition now at the centre of the EU's engagement with partner countries, it is important to **strengthen convergence between the EU and countries in the MENA**

[7] See, for instance, the discourse presented during the UN Conference on the Environment in Stockholm in 1972: https://www.un.org/en/conferences/environment/stockholm1972

region regarding a double objective of building more resilient states and societies as well as reducing the risks of conflicts resulting from the potential malicious use of ICT. This requires an unequivocal recognition that digital transition is not just a technological process but also a political one. Consequently, this chapter makes four concrete recommendations for the EU's engagement with the region.

1. The EU needs to aim for a **more robust political dialogue with its partners in the region regarding their positions on key cyber-related issues,** in particular the application of the existing international law in cyberspace and norms of responsible state behaviour. A new Agenda for the Mediterranean presented in February 2021 provides a good opportunity for embedding these issues in a broader context of strengthening resilience and digital transition. In an effort to promote its norms and principles for free, open, stable and secure cyberspace, the EU should not shy away from openly expressing its expectations of partners in the region. At the same time, the EU should pursue a double strategy in the region based on deepening its dialogue with Egypt and Iran in order to better understand their respective positions while at the same time encouraging other players – in particular Tunisia, Morocco and Jordan – to play a more active role. This also requires rethinking the EU's approach to capacity-building initiatives in the region, in particular through better mapping of key stakeholders and their needs.

2. The EU's engagement with the region should aim to **strengthen a multi-stakeholder approach across the region based on the fact that state resilience does not always go hand-in-hand with societal resilience.** Against the general trends of democratic backsliding and human rights abuses, the EU needs to ensure that cyber capacity-building undertaken in the region is driven by a rights-based and human-centric approach. This is particularly relevant in the context of the fight against cybercrime whereas strengthening the capacities of law enforcement and criminal justice bodies needs to be directly linked to building capacities and creating the right environment for non-governmental actors to operate. Some of the concrete ideas for operational cooperation might include exchange programmes for cyber experts and training platforms, international exercises in order to enhance national cyber incident preparedness levels and response capacities, as well as exchanges of good practices to ensure the security of new technologies, including 5G Toolbox and the General Data Protection Regulation. Political dialogue could also serve to improve mutual understanding concerning the application of common but differentiated responsibility that countries in the region advocate as also relevant in the context of cyberspace.

3. **The EU and regional organisations** – in particular the League of Arab States and the Gulf Cooperation Council (GCC) – **should strengthen their cooperation to develop and implement region-**

specific CBMs. Such dialogue could focus on exploring mechanisms to implement a set of CBMs already proposed in the 2015 UN GGE report and developing a regional platform dedicated to exchange of information on vulnerabilities and best practices, fostering international cooperation and capacity-building. Ultimately, the objective of such cooperation could be a demilitarised cyber-zone with states making a binding commitment to refrain from using cyber tools against each other. The Union for the Mediterranean (UfM) could also serve as a useful outlet for the development of such a project.

References

ARNOLD, D. (2005). Europe, technology, and colonialism in the 20th century. *History and Technology,* 21(1), 85-106.

BODETTI, A. (2020, January 7). Oman strives for neutrality in the Middle East. *Yale Global Online.* Retrieved from https://archive-yaleglobal.yale.edu/content/ oman-strives-neutrality-middle-east

DEYOUNG, K. (2017, July 21). Qatar's investigation of cyberattack stops just short of naming suspects. *Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/qatars-investigation-of-cyberattack-stops-just-short-of-naming-suspects/2017/07/20/de721b26-6d8a-11e7-96ab-5f38140b38cc_story.html

ELECTRONIC FRONTIER FOUNDATION (EFF). (2018). *EFF and Lookout uncover new malware espionage campaign infecting thousands around the world.* Retrieved from https://www.eff.org/nl/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around

EPSTEIN, C. (2021). Common but differentiated responsibilities. *Encyclopedia Britannica.* Retrieved from https://www.britannica.com/topic/common-but-differentiated-responsibilities

EU CYBER DIRECT. (2020). *Cyber conflict portal.* Retrieved from https://eucyberdirect.eu/content_research/cyber-conflict-portal/

GOSLINGA, M., & TOKMETZIS, D. (2017, February 23). The surveillance industry still sells to repressive regimes. Here's what Europe can do about it. *The Correspondent.* Retrieved from https://thecorrespondent.com/6249/the-surveillance-industry-still-sells-to-repressive-regimes-heres-what-europe-can-do-about-it/679999251459-591290a5

GROSS, J. A. (2020, October 29). With massive exercise in north, IDF prepares for war on multiple fronts. *Times of Israel*. Retrieved from https://www.timesofisrael.com/with-massive-exercise-in-north-idf-prepares-for-war-on-multiple-fronts/

HICKS, J. (2019, September 26). "Digital colonialism": why some countries want to take control of their people's data from Big Tech. *The Conversation.* Retrieved from https://theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048

KAUSCH, K. (2017). Cheap havoc: how cyber-geopolitics will destabilize the Middle East (GMF *Policy Brief*, 35). German Marshall Fund of the United States.

KAVANAGH, C., & CORNISH, P. (2020). Cyber operations and inter-state competition and conflict: the persisting value of preventive diplomacy. *EU Cyber Direct.* Retrieved from https://eucyberdirect.eu/content_research/cyber-operations-and-inter-state-competition-and-conflict-the-persisting-value-of-preventive-diplomacy/

MARCZAK, B., SCOTT-RAILTON, J., RAO, S. P., ANSTIS, S., & DEIBERT, R. (2020). Running in circles uncovering the clients of cyberespionage firm circles. *The Citizen Lab.* Retrieved from https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

MAUER, T. (2018). *Cyber mercenaries: the state, hackers, and power.* Cambridge: Cambridge University Press.

MIDDLE EAST MONITOR. (2021). *New York Times: UAE hired NSA hackers to spy on Qatar.* Retrieved from https://www.middleeastmonitor.com/20210207-new-york-times-uae-hired-nsa-hackers-to-spy-on-qatar/

SAYADI, E. (2019, April 8). Morocco's Hirak movement has gone quiet, but the crackdown on independent media continues. *Access Now.* Retrieved from https://www.accessnow.org/moroccos-hirak-movement-has-gone-quiet-but-the-crackdown-on-independent-media-continues/

UNITED NATIONS (UN). (2021). R*eport of the UN OEWG* (Final report - advanced copy).

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2019a). *Countering the use of information and communications technologies for criminal purposes. Statement of financial implications (A/74/610), A/RES/74/247.* Retrieved from https://www.un.org/en/ga/74/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2019b). *Advancing responsible state behavior in cyberspace in the context of international security, A/RES/74/28.* Retrieved from https://www.un.org/en/ga/74/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2019c). *Developments in the field of information and telecommunications in the context of international security, A/RES/74/29.* Retrieved from https://www.un.org/en/ga/74/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2020a). *Developments in the field of information and telecommunications in the context of international security. Statement of financial implications (A/75/674), A/RES/75/240.* Retrieved from https://www.un.org/en/ga/75/resolutions.shtml

UNITED NATIONS GENERAL ASSEMBLY (UNGA). (2020b). *Advancing responsible state behaviour in cyberspace in the context of international security, A/RES/75/32.* Retrieved from https://www.un.org/en/ga/75/resolutions.shtml

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2019). *Submission by the Islamic Republic of Iran to the UN OEWG.* Retrieved from https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/iran-submission-oewg-sep-2019.pdf

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2020a). *Second submission by the Islamic Republic of Iran to the UN OEWG,* February 2020.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2020b) *Intervention by delegation of the Islamic Republic of Iran on International Law, 1 October 2020.* Retrieved from https://front.un-arm.org/wp-content/uploads/2020/10/iran-intervention-1-october-2020.pdf

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA).(2020c). *Working Paper submitted by the Delegation of Egypt to the UN OEWG.* Retrieved from https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/Egypt-Working-Paper-OEWG-ICTs1.pdf

UNITED NATIONS OFFICE FOR DISARAMAMENT AFFAIRS (UNODA). (2021a). *UN OEWG Final Substantive Report.* A/AC.290/2021/CRP.2.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). (2021b). *Statement by Turkey at the informal meeting of the UN OEWG.* Retrieved from : https://front.un-arm.org/wp-content/uploads/2021/02/Turkey-statement_OEWG-informal-meeting_February-2021.pdf

WEINBERGER, S. (2007, April 10). *How Israel spoofed Syria's air defense system. Wired.* Retrieved from https://www.wired.com/2007/10/how-israel-spoo/

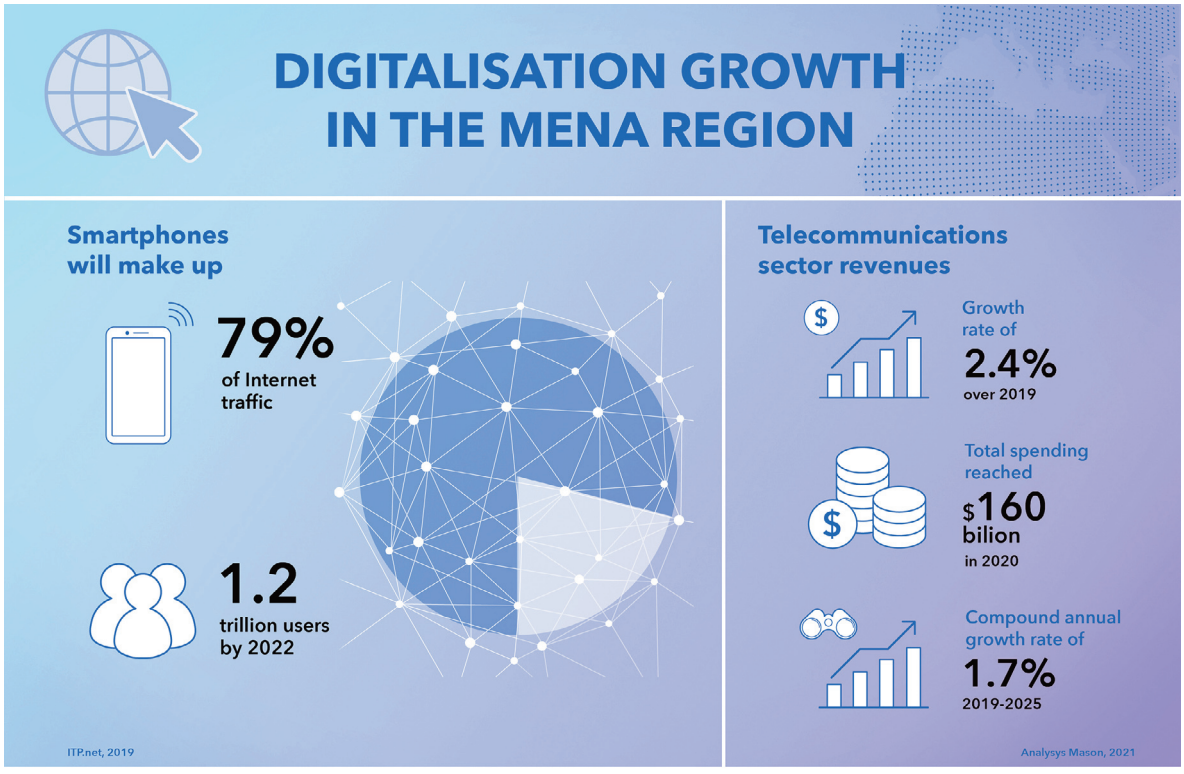
WINDER, B. (2020). Oman's regional role in a time of challenge and change. *Middle East Institute.* Retrieved fromhttps://www.mei.edu/publications/omans-regional-role-time-challenge-and-change

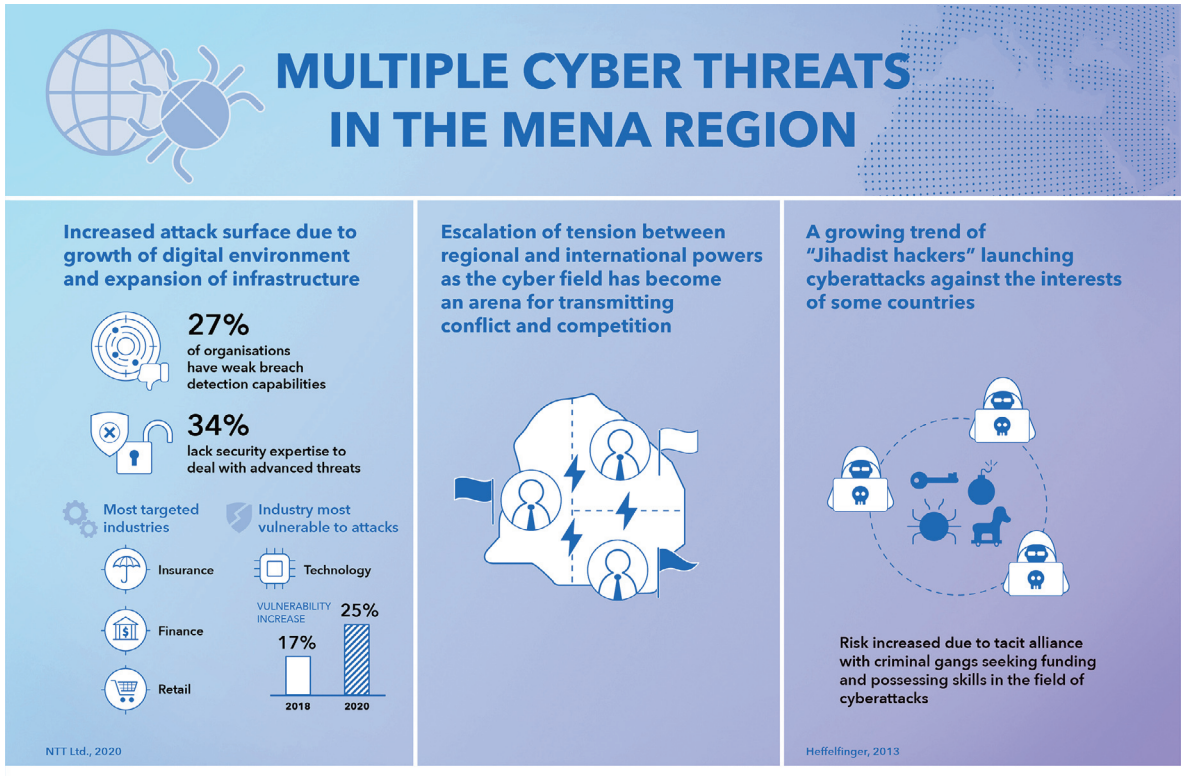
ŠVEDKAUSKAS, Ž. (2019). Three steps in ensuring digital security of Egyptian activists abroad. *EuroMeSCo.* Retrieved from https://www.euromesco.net/publication/three-steps-in-ensuring-digital-security-of-egyptian-activists-abroad/

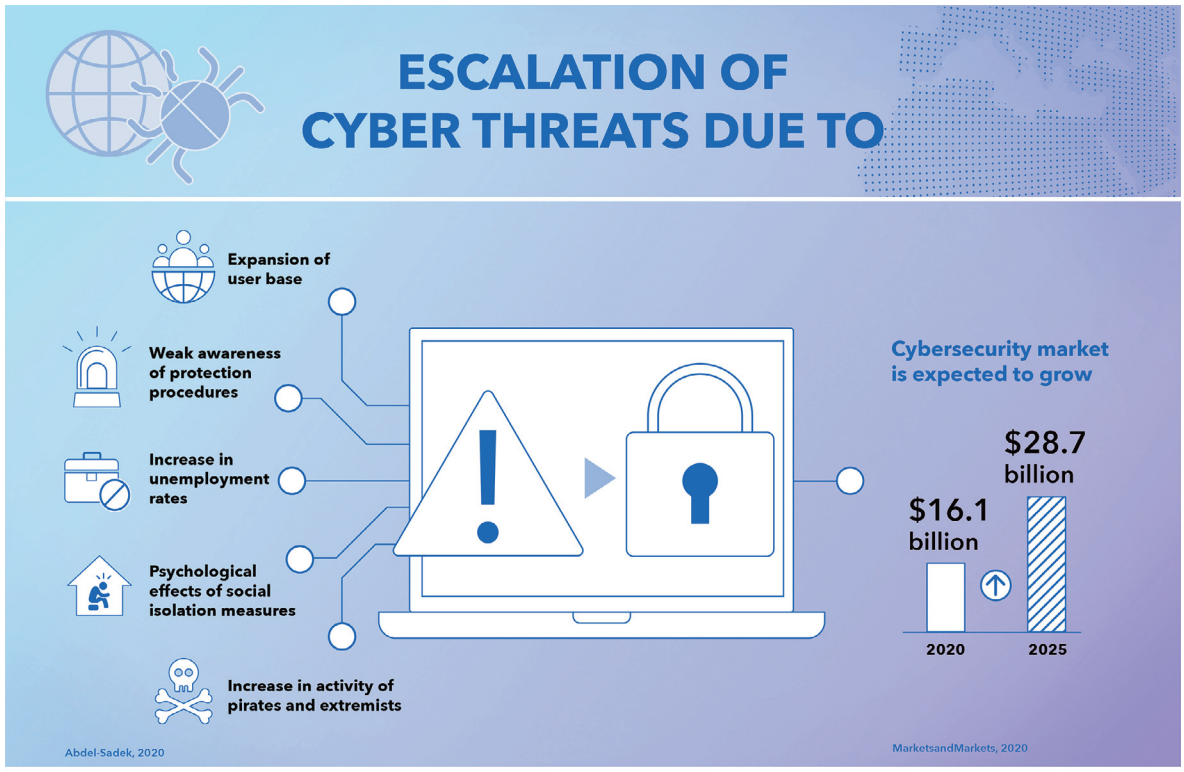
ZETTER, K. (2014, March 11). An unprecedented look at Stuxnet, the world's first digital weapon. *Wired.* Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Annex: Digitalisation and Cyber Resilience

Adel Abdel-Sadek
Expert, Security Studies Unit, Al-Ahram Center for Political and Strategic Studies (ACPSS)


DIGITALISATION GROWTH IN THE MENA REGION
Smartphones will make up
79%
of Internet traffic
1.2
trillion users by 2022
ITP.net, 2019
Telecommunications sector revenues
Growth rate of
2.4%
over 2019
Total spending reached
$160
bilion
in 2020
Compound annual growth rate of
1.7%
2019-2025
Analysys Mason, 2021


MULTIPLE CYBER THREATS IN THE MENA REGION
Increased attack surface due to growth of digital environment and expansion of infrastructure
27%
of organisations have weak breach detection capabilities
34%
lack security expertise to deal with advanced threats
Most targeted industries
Insurance
Finance
Retail
Industry most vulnerable to attacks
Technology
VULNERABILITY INCREASE
17%
25%
2018
2020
NTT Ltd., 2020
Escalation of tension between regional and international powers as the cyber field has become an arena for transmitting conflict and competition
A growing trend of "Jihadist hackers" launching cyberattacks against the interests of some countries
Risk increased due to tacit alliance with criminal gangs seeking funding and possessing skills in the field of cyberattacks
Heffelfinger, 2013



Cyber resilience and sustainable development in the MENA region

"Cyber resilience" means the ability to sense and prepare preventively to face, resist and respond to cyber threats, whether those dangers are anticipated or unexpected, and to enable the ability to quickly recover from their effects in a timely manner. The proactive analysis of weaknesses at all levels of the internal digital environment contributes to reducing the amount of physical and moral damage to institutions in various sectors (WEF, 2020), which include the energy sector, banking services, communications infrastructure, healthcare, security and defence, the stock market, and government services. Applications of "cyber resilience" require that all technical services undergo several procedures such as data backup, disaster recovery, crisis management, business continuity, and institutional resilience. Adopting a cyber resilience strategy requires identification of the assets of critical infrastructure and areas most vulnerable to threats, as well as the actors behind them, whether they are state or non-state, including a comprehensive vision based on sharing data between the government and the private sector, embracing concern for the role of the individual and society, excellence in the proactive dimension, identifying and addressing the causes of disruption and innovation and continuous development to face the acceleration in the level and manner of threats (Carías et al., 2020).

Adopting a cyber resilience strategy requires identification of the assets of critical infrastructure and areas most vulnerable to threats, as well as the actors behind them

There are several reasons why resilience has become an attractive framework for governments to focus their attention

on. **Firstly,** the acceleration of technological change reduces the ability to predict risks and requires more agility. **Secondly,** there is increasing awareness of cybersecurity among decision-makers with the steady increase in threats, on the one hand, and its high cost, on the other. **Thirdly,** the escalation of the role of digitalisation in the functioning and integration of global supply chains and the existence of open-source software or the cross-border nature of technical components or programmes raise problems regarding ownership of systems, legal jurisdiction, and the presence of third parties to provide important functions. **Fourthly,** countries are increasingly dependent on integrated digital services, with the adoption of the Internet of Things (IoT) and applications of artificial intelligence. And, **finally,** the digital economy is becoming more important in achieving the Sustainable Development Goals (SDGs).

According to the National Cyber Security Index 2020 (https://ncsi.ega.ee/ncsi-index/), which measures the preparedness of countries to prevent cyber threats and manage cyber incidents, the situation across the region is very diverse.

The state and reality of cyber resilience in Egypt

Egypt ranked 23rd in the Global Cyber Security Index, 103rd in the ICT Development Index, and 84th out of 134 countries in the Network Readiness Index (NRI) in 2020. Egypt was also among the top 10 Improvers in Digital Inclusion in 2020. It achieved 81st position in the National Cyber Security Index 2020 (NCSI, 2020).

The Egyptian framework of cyber resilience

Firstly, Egypt adopts a strategic vision on becoming cyber resilient through its Constitution, which in article 31 mentions that "the security of cyberspace is an integral part of the economic system and national security. The State shall take the necessary measures to preserve it as regulated by Law" (Egypt Const. art. 31.). The strategic priorities for supporting national capabilities in cyber resilience require effective leadership at national and local levels, which is translated in some of Egypt's strategies and policies for cybersecurity, such as the objectives of the National Cyber Security Strategy 2017-2021, Egypt's Vision 2030, the information and communication technologies (ICT) Strategy 2030, Africa's Agenda 2063, and SDGs. Egypt was investing in developing the infrastructure, not only through the $1.6 billion made in the ICT sector but also in the power and energy sector. Egypt's ICT sector was achieving a growth rate of 15.2% and its contribution to gross domestic product was about 4.4% in 2020 (Daily News Egypt, 2020).

Secondly, Egypt launched a Computer Emergency Readiness Team (EG-CERT) in 2009, and established a Supreme Cyber Security Council in 2014 whose mission is to raise awareness and develop a strategy that counters cyberattacks through response, support, defence and analysis. In 2019, the Egyptian Government formed the National Council for Artificial Intelligence, and the Trend Micro company addressed 12.4 million e-mail cyber threats in Egypt in the first half of 2020 (Alaa El-Din, 2020).

Thirdly, in April 2020 Egypt organised a number of training programmes for government employees nationwide using e-learning applications, and launched many initiatives like Basic Digital Skills Development, Social Media and Internet Safety, Youth Enablement for Freelancing and the Digital Egypt Builders Initiative (DEBI).

Fourthly, Egypt commits to advancing research and innovation and modernising the educational curricula in schools and universities by launching new colleges specialising in artificial intelligence as well as adopting online exams, improving the quality of scientific research within research centres and encouraging creativity and innovation. Egypt launched initiatives for enhancing innovation like the Next Technology Leaders (NTL), InnovEgypt, TIEC Innovation Ambassador, and Entrepreneurship Support Trainings.

Fifthly, Egypt achieved remarkable success in implementing the initiatives for promoting the partnerships with all concerned parties regionally and internationally. It has also facilitated an enabling environment for building cyber resilience capabilities. Egypt organised the training and shared expertise between CERTs in the Arab world and Africa.

Finally, Egypt launched "Digital Egypt", which includes working on developing the infrastructure, promoting digital and financial inclusion, enhancing capacity-building and innovation, fighting corruption, and digitalising government services. Egypt was selected as the Arab digital capital for the year 2021.

The state and reality of cyber resilience in Tunisia

Tunisia ranked 45th in the Global Cyber Security Index, 99th in the ICT Development Index, 91st in the NRI, and 96th in the National Cyber Security Index in 2020 (NCSI, 2020).

The Tunisian framework of cyber resilience

Firstly, in 2019 Tunisia launched its National Cyber Security Strategy, which has the following objectives: (1) leadership and management of the national cyberspace and promoting joint action among all parties; (2) preventing cyber threats by strengthening national capabilities, awareness and protecting infrastructure; (3) supporting digital confidence by developing mechanisms and procedures; (4) achieving leadership in the digital domain; and (5) ensuring the supreme interests of the country (UNIDIR, 2019).

Secondly, Tunisia works to build awareness and trust and protect its citizens and the public and private sector against any cyber threat. The National Agency for Computer Security represented by the Tunisian Computer Emergency Response Team (tunCERT) participated in the first international cybersecurity exercise during the period of 27 October and 5 November 2020. Furthermore, the "Saher" information system was adopted to lure and hunt pirates, and expose penetration attempts that target official websites (https://www.cert.tn/fr).

Thirdly, Tunisia launched the "Tawasol" project to support a community network, which is led by the Institute of Electrical and Electronics Engineers (IEEE) Special Interest Group on Humanitarian Technology (SIGHT) (Project Tawasol, 2020). It aims to connect primary schools across the country to the Internet, and train students to use the Internet through ICT skills workshops conducted by young members of the IEEE.

Fourthly, Tunisia promotes research and innovation and digitalisation in economic and social development by boosting the creation of new innovative small and medium-sized enterprises (SMEs) and the growth of existing SMEs. It also works on the development of the smart electrical grid, renewable energy use, and enhancement of energy efficiency in transportation and the quality of ICT companies and infrastructure, as well as supporting research and learning facilities. The institutions involved in this include the National Engineering School of Tunis, University of Tunis El Manar, University of Manouba, University of Sfax, National Institute of Applied Sciences and Technology, and University of Carthage (IST-Africa, 2017).

Fifthly, Tunisia participated in a Joint Project of the European Union (EU) and the Council of Europe (2017-2020) to strengthen legislation and institutional capacities on cybercrime. In July 2017, the Spain-Tunisia cooperation on cybersecurity was declared and, in April 2015, Tunisia became a member of the Global Forum on Cyber Expertise (UNIDIR,

2020). To support Tunisian authorities with the technical capacities to face cyber threats, the United Nations Office on Drugs and Crime (UNODC) organised four training sessions on specialised digital forensics software, funded by the United States Bureau of International Narcotics and Law Enforcement Affairs (INL) (UNODC, 2020).

Finally, "Digital Tunisia 2020" was launched in 2015, aiming to create 80,000 jobs in 2020 through a combination of offshoring, nearshoring and co-locating public-private partnerships. The government allocated a total budget of around €500 million to support the programme through incentives and funding for local and international companies. In addition, the Tunisian Government is collaborating with a larger pan-African project, the "Smart Africa" start-up investment fund, which was launched in February 2019 (Oxford Business Group, 2020).

The state and reality of cyber resilience in Morocco

Morocco achieved 50th position in the Global Cyber Security Index, 100th in the ICT Development Index, and 93rd in the NRI of 2020, as well as 105th in the National Cyber Security Index (NCSI, 2020).

The Moroccan framework of cyber resilience

Firstly, on 14 July 2020, the Moroccan House of Representatives passed the Law 05-20 on Cyber Security drafted by the Department for National Defence, which aimed to protect and defend the country from cyberattacks by strengthening the foundations of security through awareness raising campaigns, trainings, research and development, promotion and development of national and international cooperation (Amrouche, 2021).

Secondly, Morocco ranked among the top 10 countries for the highest volume of malware attacks in 2020: Kaspersky detected a total of 13.4 million cyberattacks between April and June 2020. Only 8% of people questioned reported that they use any kind of antivirus software. 18% indicated that they do not update their mobile phones, and only 33% of respondents trust their mobile devices to store confidential data. 76% indicated that they are afraid of their personal photos or videos being stolen and 39% of those surveyed are afraid of being spied on through the camera (Dumpis, 2021).

Thirdly, since almost half of the population in Morocco is under 25, reforming higher education in Morocco is one of the main concerns of policy-makers and educators in the country. For this reason, the Ministry of Education started a digitalisation project for 2019-2020 with the public universities of Cadi Ayyad University in Marrakech and Ibn Zohr University in Agadir (Mezgheldi, 2019)

Fourthly, Morocco has adapted research and innovation as a driving force for economic development in a particularly competitive context (Cornell University et al., 2020). Morocco aims to be a technological hub between Europe and Africa and a leader in clean energy technologies and promoting sustainable technology industries.

Fifthly, Morocco also participated in the CyberSouth initiative. On 18 May 2017, during the Morocco-NATO talks, future cooperation prospects in the field of cybersecurity were examined, notably through the exchange of expertise and training (UNIDIR, 2021).

Finally, the "Digital Morocco" project plans to position the country among emerging and dynamic countries (National Cyber Security Strategy of Morocco, 2013).

The key to cyber resilience: more regional and Euro-Mediterranean cooperation

Progress has also been made on bilateral and regional cooperation in the MENA region in the field of capacity-building

Some initiatives have been promoted over the last few years to advance cyber cooperation. On 20 July 2020, the Gulf Cooperation Council announced the launch of the cybersecurity malware analysis platform as a joint Gulf project approved by the Committee of National Centres for CERTs. On 28 January 2021, the Arab parliament called for the need to adopt international rules governing the prevention of cyber warfare and the promotion of digital cooperation. In 2018, the Arab Cybersecurity Convention was discussed, and progress was also made in the field of adopting laws to combat cybercrime, establishing national centres for cybersecurity, and strengthening bilateral and regional cooperation according to global cybersecurity indices.

The North African region is integrated into African efforts in the field of cyber resilience, which consider the 2014 Malabo Agreement an important pillar to support cybersecurity. A strategy for cybersecurity and cybercrime in Africa was approved in 2016 by the African Ministers of Communications. In 2018, the African Union (AU) held an annual conference on cybersecurity in cooperation with the Council of

Europe, considering that cybersecurity is part of Africa's 2063 strategy.

Progress has also been made on bilateral and regional cooperation in the MENA region in the field of capacity-building. The International Telecommunication Union Arab Regional Cyber Security Center (ITU-ARCC) has played a role in this matter, in addition to cooperation initiatives between the region and the EU such as the CyberSouth initiative or the EU Cyber Direct.

Cloud computing, data centres, and smart city applications are also important opportunities to deal with various risks and challenges, such as Egypt's New Administrative Capital project. One of Saudi Arabia's 2030 vision goals is to transform 10 cities all over the Kingdom into smart cities. Furthermore, Saudi Arabia, in cooperation with Bahrain, UAE, Jordan, Kuwait and Pakistan, launched an international organisation for digital cooperation on 24 November 2020 (Digital Cooperation Organization, DCO).

However, more regional cooperation is needed to establish new submarine cable systems and data centres and modernise the infrastructure, as well as to increase the capacity of broadband connections, manage network congestion, ensure continuity of vital public services and enhance digital financial technologies. The COVID-19 crisis has shown that multi-stakeholders at national and global level can only be overcome through joint action, knowledge exchange, resource mobilisation and information exchange, international cooperation and coordination in order to build resilience in the field of cyberspace. The MENA region and the EU should develop a "Pan-Euro-Mediterranean Cybersecurity Strategy (PEMCS)", not only for the public sector and critical infrastructures but also to help economic operators and the private sector facing growing challenges in cyber threats (Lannon, 2019). The EU and MENA region should form a digital economic bloc and establish an association between CERTs in both regions. Finally, through a partnership with the new DCO, the EU could develop the digital economy in the MENA region and achieve the 2030 SDGs.

References

ALAA EL-DIN, M. (2020). 12.4 million cyber-threats addressed in Egypt in H1 2020: trend micro. *Daily News Egypt.* Retrieved from https://dailynewsegypt.com/ 2020/09/30/12-4-million-cyber-threats-addressed-in-egypt-in-h1-2020-trend-micro/

AMROUCHE, A. (2021). *Cybersecurity market in Morocco.* Government of Canada. Retrieved from https://www.tradecommissioner.gc.ca/morocco-maroc/market-reports-etudes-de-marches/0005881.aspx?lang=eng

CARÍAS, J. F., ARRIZABALAGA, S., LABAKA, L., & HERNANTES, J. (2020). Cyber resilience progression model. *Applied Sciences,* 10(21), 7393. Retrieved from https://www.mdpi.com/2076-3417/10/21/7393

CORNELL UNIVERSITY, INSEAD, & WIPO. (2020). *The Global Innovation Index 2020: Who Will Finance Innovation?* Retrieved from https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020/ma.pdf

DAILY NEWS EGYPT. (2020). Egypt's ICT sector demonstrates resilient performance despite COVID-19. Retrieved from https://dailynewsegypt.com/2020/12/03/egypts-ict-sector-demonstrates-resilient-performance-despite-covid-19/

DUMPIS, T. (2021). *Kaspersky: Moroccans not concerned about cybersecurity.* Morocco World News. Retrieved from https://www.moroccoworldnews.com/2021/02/333890/kaspersky-moroccans-not-concerned-about-cybersecurity/

IST-AFRICA. (2017). *National ICT research capacity and priorities for cooperation – Tunisia.* Retrieved from http://www.ist-africa.org/home/default.asp? page=doc-by-id&docid=7004

KINGDOM OF MOROCCO MINISTRY OF INDUSTRY, TRADE AND NEW TECHNOLOGIES. (2013). *Digital Morocco 2013: the national strategy for information society and digital economy.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Morocco_2013_Maroc_CyberSecurity_2013_ENG.pdf

LANNON, E. (2019). EU cybersecurity capacity building in the Mediterranean and the Middle East. Strategic sectors security & politics. *IEMed Mediterranean Yearbook 2019.* Retrieved from https://www.iemed.org/publication/eu-cybersecurity-capacity-building-in-the-mediterranean-and-the-middle-east/?lang=fr

MEZGHELDI, S. (2019). *Morocco is looking for international partners in vocational training and higher education.* Team Finland. Retrieved from https://www.marketopportunities.fi/home/2019/morocco-is-looking-for-international-partners-in-vocational-training-and-higher-education?type=business-opportunity&industry=education-and-learning

OXFORD BUSINESS GROUP. (2020). *The report: Tunisia 2019.* Retrieved from https://oxfordbusinessgroup.com/analysis/successful-start-government-working-develop-local-start-ecosystem-through-new-policies-and

PROJECT TAWASOL. (2020). *Connecting primary schools to create an internet empowered next generation in Tunisia.* 1 World Connected. Retrieved from https://1worldconnected.org/project/africa_digitalskills_youth_projectawasoltunisia/

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDR). (2020). *Cyber security portal – Tunisia.* Retrieved from file:///C:/Users/pract_doc/Downloads/Tunisia%20(3).pdf

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). (2020). *Tunisia: mobile digital forensics as a key method to prevent cybercrime.* Retrieved from https://www.unodc.org/middleeastandnorthafrica/en/web-stories/tunisia_-mobile-digital-forensics-as-a-key-method-to-prevent-cybercrime.html

WORLD ECONOMIC FORUM (WEF). (2020). *Rebounding from COVID-19: MENA perspectives on resilience in manufacturing and supply systems.* Retrieved from https://www.weforum.org/reports/rebounding-from-covid-19-mena-perspectives-on-resilience-in-manufacturing-and-supply-systems

List of acronyms and abbreviations

AFRIPOL	African Police Cooperation Organisation
CBDR	common but differentiated responsibilities
CBM	Confidence-building measure
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CI	critical infrastructure
CoE	Council of Europe
CSO	Civil Society Organization
ENP	European Neighbourhood Policy
EU	European Union
GLACY	Global Action on Cybercrime
ICT	information and communication technologies
ISP	Internet service provider
LEA	Law Enforcement Agency
MENA	Middle East and North Africa
NAM	Non-Aligned Movement
SN	Southern Neighbourhood
T-CY	Cybercrime Convention Committee
UAE	United Arab Emirates
UfM	Union for the Mediterranean
UN	United Nations
UN GGE	UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security
UN OEWG	UN Open-Ended Working Group on Developments in the Field of ICT in the Context of International Security
USA	United States of America

euromesco

Policy Study

IEMed.

European Institute of the Mediterranean