Digital Cooperation in the Mediterranean: Opportunities, Challenges and the Future

Dr. Adel Abdel-Sadek
Director
Arab Center for Cyberspace Research – ACCR

Cyberspace has had different impacts on states' national sovereignty as well as in forming new concepts of security, power, conflict and hegemony, bringing about changes in geostrategic thinking in the 21st century through the interaction between the strategic and geographic dimensions. These concepts have also had an impact on states' foreign policy, on the one hand, and on international politics, on the other.
The Mediterranean region has therefore been driven to finding new ways to provide flexibility and resilience in light of a turbulent regional and international environment. This can be done through building national capabilities or regional and international cooperation, thereby confronting the new geostrategic challenges of the cyber field, especially in light of the ever-increasing role of generative artificial intelligence, and enhancing the role of the digital economy in the region to provide innovative solutions towards achieving the United Nations 2030 Sustainable Development Goals.
This raises questions about the impact of cyberspace on the geostrategic dimension of the Mediterranean region, the opportunities and challenges it is facing, the future role of cyberspace in enhancing regional security, the prospects for cooperation in the field of sustainable digital development and the future impact on global digital cooperation.

Trends in the Escalating Role of the Cyber Domain in Geostrategic Threats

In the Mediterranean region there is an increasing prevalence of telecommunications and internet services, with penetration rates reaching 90.2% in southern Europe and 70% in North Africa. Moreover, it has has a huge population of 500 million people spread across 24 countries. The region represents a strategic link between three continents: Europe, Africa and Asia in the areas of trade and cultural exchange and international navigation, and plays host to a number of strategic waterways, namely the Suez Canal, the Bosphorus Strait and the Strait of Gibraltar. The Mediterranean region performs the role of a data superhighway via submarine cables, which accounts for 95% of the communications traffic globally and makes it a key player in the global digital economy.
During 2024, the Mediterranean region has witnessed increasing trends in the role of cyberspace in geostrategic threats, the most important of which are outlined below.
First: The southern Mediterranean is witnessing mounting pressure on infrastructure, with increased proliferation and use on the one hand, and the absence of the cultural and social dimension of the transformation process on the other. Therefore, there has been a proliferation of digital services that exceeds the ability to absorb the associated risks and the flexibility required to confront them. This has increased exposure to cyber threats, especially in the countries of the southern and eastern Mediterranean, and caused their influence to spread to the northern Mediterranean.
Second: There is a trend towards employing the digital economy to advance digital development and digital transformation efforts to increase productivity and income levels, integrate marginalized people, employ big data in development, search for solutions to confront economic inflation, high rates of unemployment and poverty, especially among young people, and try to raise capabilities in the field of cybersecurity. And this is accompanied by an escalation of cyberattacks and increased economic losses.

Third: We have to confront the impact of the geopolitical crises in the aftermath of the Covid-19 crisis, the Ukraine war and the Gaza war, which requires securing supply chains of food and technology products. There is also the impact of the escalating tensions between China and Russia on the one hand, and the United States and its allies on the other hand, on the patterns of conflict over cybersecurity, markets, wealth and influence in emerging markets, and the rising attempts to penetrate European electoral systems, whether by falsifying the will of the voter or by undermining the democratic system and misleading public opinion, thus further destabilizing confidence between society, the State and the political process.
Fourth: The role of active cyber diplomacy has increased within the European Union in cooperation with the southern Mediterranean to confront the escalation of cyber threats and build regional capabilities. This takes into consideration how cyber threats intertwine with other issues, such as illegal immigration, organized crime and human trafficking, which all benefit from cyber communication in mobilizing, organizing, planning and financing their activities.
Fifth: There is an increased risk of the rise in the activities of terrorist and extremist movements, which attract young people through digital platforms who suffer from poverty, unemployment and lack of education and skills, making them prey to recruitment in the southern Mediterranean. There is also an escalation of the risks of non-state actors employing cryptocurrencies to evade sanctions and financing their activities or using drones in conflicts, whether through support from external countries, through developing their own capabilities or through obtaining these on the black market.
Sixth: The role of digital platforms and major technology companies in the conflict has escalated and started shaping local, regional and global public opinion, thereby giving increased importance to the process of data governance, confronting misleading rumours and deep fakes, and limiting the use of algorithms by technology companies to create bias and violate freedom of opinion and expression.
Seventh: There has been a worrying increase in the activities of non-state actors, or those supported by states, in the field of selling, disseminating, and using advanced comprehensive spyware on millions of users, representing an escalating threat to digital rights, state sovereignty and law enforcement. The "Israeli" Pegasus programme is an example of this.
Eighth: The escalation of military and security tensions negatively affects the Mediterranean region, with less security in digital transactions and an increased risk of internet cables being cut or their maintenance being poorly secured, especially in the Red Sea region, thereby affecting the security of global data traffic.

There has been a proliferation of digital services that exceeds the ability to absorb the associated risks and the flexibility required to confront them

Ninth: The effects of social networks on young people are on the rise in the countries of the South, encouraging them to immigrate to the North illegally, in addition to their role in securing migration routes, coordination, camouflage, transferring money and hunting down new victims, especially from within Africa.
Tenth: Generative artificial intelligence is increasingly at risk of violating human rights. The protection of personal data and privacy by major technology companies is an increasing trend and AI poses a threat to jobs, which entails potential social unrest, especially in the southern Mediterranean, where there is high unemployment among young people and a widening gap between the labour market and the required skills. Finally, there are risks of a widening of the generation gap and the difference in visions and positions between Generation Z, youth and teenagers on the one hand and the older generations on the other. This puts pressure on security, political and legal institutions within the Mediterranean region, especially given the disparity between these groups in terms of digital skills.

Promising Opportunities for Digital Cooperation in the Mediterranean to Confront Cyber Challenges

There are multiple initiatives for regional cooperation, whether within the Mediterranean region or within a broader framework with the European Union, the most important of which are the Barcelona

Process, the Union for the Mediterranean, cyber diplomacy programmes aimed at the southern Mediterranean, and the European "Global Gateway" project, which was launched in 2021, with the aim of raising $600 billion. The Digital Silk Road project, an offshoot of the Chinese Belt and Road Initiative, has the goal of increasing investments in global infrastructure and promoting democratic values, governance, transparency, green transformation and clean energy through international cooperation by 2027. The year 2024 has so far witnessed European diplomatic activity with several countries, including the Egyptian-European summit on 17 March 2024.

The Mediterranean region is witnessing strategic competition between China and the United States, both trying to seize the revenues of the digital economy and digital markets and exploiting the region's weakness in the field of digital services. The situation favours cross-border technological companies, which are most often American and Chinese.

The region, especially Europe, is exposed to strategic pressures to limit openness to China or partnership with the Digital Silk Road in exchange for the American development corridor. In addition to American pressure not to export semiconductors to China, thereby limiting its progress in artificial intelligence, there are new dimensions to the importance of correcting the strategic imbalance in supply chains, including reducing dependence on Taiwan, which dominates the digital chip industry. Cooperation within the Mediterranean region and Europe aims to advance this industry to ensure excellence in the field of artificial intelligence, fifth generation networks, batteries and electric cars, especially since the reality of the situation indicates the dominance of the big countries or big technology companies that specialize in artificial intelligence.

In general, Europe is fortunate to have made progress in the digital legislative system, in line with the nature of the challenges and opportunities offered by the digital field. Opportunities are provided for cooperation with the southern Mediterranean to address its cyber-legislation gap. This includes the improved digital governance of emerging technologies, such as artificial intelligence and digital assets, and the adoption of the General Data Protection Regulation, as well as personal data and privacy protection and advance international efforts to impose digital taxes and regulate digital services and digital markets.

These European policies, in harmony with the goals of the Mediterranean region, aim to regulate the work of major technology companies, protect freedom of competition, prevent monopoly and govern content on digital platforms. They are also looking to correct the imbalance in the structure of the digital market, providing a fair environment for the emergence of new companies, whether at the national or regional level. This is especially important given the Mediterranean region's lack of digital platforms or social networks.

Highlighting the importance of adopting digital currencies to confront the risks of relying on foreign payment applications, which are either American or Chinese, contributes to supporting cyber resilience in the Mediterranean region. Applications for cyber sovereignty need to be developed, benefiting from the European experience.

Advantage should also be taken of the low cost of labour in the southern Mediterranean and the fact that it is a gateway to the African market for implementing joint development projects that localize technology industries at the software or hardware level. Capabilities in the field of satellites can thereby be developed to monitor illegal immigration routes and establish early warning centres. The role of satellite internet services can also be expanded to mitigate pressure on internet cables and provide flexibility in the face of cyber crises.

Digital cooperation in the Mediterranean region contributes to providing new job opportunities and building capabilities among young people in the field of digital skills

Cooperation in the field of digital transformation contributes to improved government, financial, health and education services, in addition to boosting industry and agriculture. In farming, this cooperation contributes to optimizing the use of limited resources such as water, soil and food, confronting climate change and supporting agricultural exports to Europe.

Cooperation in the Mediterranean region is needed to address cyber threats through the exchange of ex-

periences and information between national cybersecurity centres. This will enhance confidence in the digital environment and e-commerce and consolidate the responsible behaviour of states in cyberspace at the regional and international levels.

Digital cooperation in the Mediterranean region contributes to providing new job opportunities and building capabilities among young people in the field of digital skills, especially artificial intelligence skills, in the southern and eastern Mediterranean, particularly given the demographic challenge in the northern Mediterranean. It can help strengthen programmes to combat poverty, unemployment, illegal immigration, violence, extremism and crime, and confront the dangers posed by exporting extremism into Europe or the growing power of the extreme right. This requires launching programmes to support emerging projects and platforms for dialogue and cyber peace among Mediterranean youth.

This is all linked to the development of the education system, enhancing the culture of creativity and innovation and supporting the role of civil society in developing human capital. We need to encourage the private sector and attract foreign investments to the economies of the southern and eastern Mediterranean countries, especially given the strategic location of countries like Egypt, for example, through which 90% of submarine cables pass. Last February, for example, saw the inauguration of the first submarine cable linking Egypt to Albania and from there to the Balkans and eastern and central Europe, and the European Bank for Reconstruction and Development in Africa is making valuable contributions to the technical support and digital transformation programme for the Suez Canal Economic Zone.

Towards a Sustainable Future for Digital Cooperation in the Mediterranean Region

The integration of the cyber domain into the other four international domains – land, sea, air and outer space – prompted the emergence of the concept of comprehensive state power, at the level of hard power or soft power. The applications of generative artificial intelligence brought with them new opportunities and challenges. Many countries have come to realize that whoever maintains control over these technologies will enjoy victory, wealth and domination in the future. It has emerged that the development approach is the way to sustainably confront security threats, whether physical, cyber or both. As a result, trends for digital cooperation have arisen in the Mediterranean region, especially in terms of the progress made by the countries of the South in the field of digital transformation. Sustainable digital cooperation within the Mediterranean region requires work in the areas of digital development, building the digital economy, digital skills, protecting human rights and cyber legislation, achieving social justice and integrating marginalized groups and reducing the digital gap, whether between the northern and southern Mediterranean or between major cities, towns and villages within the country. It also requires reducing the gender gap and bridging the gap in digital skills among Mediterranean youth, confronting the challenges of information infrastructure such as submarine cables, raising awareness of cyber threats, attracting investments to support the digital economy in the southern Mediterranean, reducing the cost of data consumption or connecting to the Internet and the growth of technology industries.

This is all in addition to enhancing confidence, security and stability in the cyber field, since this is the cornerstone of regional security and securing global supply chains. These regional efforts come within the framework of a global trend towards digital cooperation led by the United Nations and potentially strengthened if a global digital agreement is reached during the Future Summit in New York in September 2024.

And none of this can be separated from the importance of establishing peace; whether between Russia and Ukraine, through the implementation of the two-state solution in the Middle East, by supporting democratic transformation and building state institutions and economies in the Mediterranean region, supporting regional efforts to govern artificial intelligence and making it available for populations to benefit from or reaching a binding international agreement on autonomous weapons. One way or another, the global governance system has to be reformed to keep pace with the changes that are posing new threats in the digital age, and the same applies for the systems of international institutions tasked with maintaining international peace and security.