LUISS

**Corso di laurea in International Relations**

Cattedra di Geopolitics, Geoeconomics and Digital Transformation

# The Digital Wider Mediterranean

## *Cyber and digital challenges affecting the Italian geostrategic region*


Prof. Alfonso Giordano

RELATORE

Prof. Giuseppe Scognamiglio

CORRELATORE

Giacomo Leccese (644552)

CANDIDATO


Anno Accademico 2021/2022

# Indice

# Introduction

Adapting to new technologies is primarily an economic and commercial issue, but it is increasingly also about foreign and security policy.[1] Thanks to the advent of "Revolution 4.0", digital technologies have reached a level of influence and pervasiveness never seen before in history and they alter even the balance of power between countries.[2] There is a new map of power in the modern world that is no longer defined by geography, by control of territory or oceans but rather by control over flows of people, goods, money and data and by exploiting the connections technology creates. In this context, "*technological progress generates new conditions in which states exercise their sovereign rights and pursue their interests, both in domestic and foreign policy*".[3]

While the relationship between digital transformation and the Italian domestic context has been mostly analyzed following the establishment in June 2021 of the National Cybersecurity Agency (ACN), the transposition of the European NIS directive in 2018 and the EU Recovery Plan, less attention has been given to the relationship between digital transformation and Italian foreign policy. This analysis is instead particularly timely considering that, in the light of the increasing multipolar international system and the highly insecure geopolitical context shaken by the Russian invasion of Ukraine, "*Italy is now more than ever forced to face its foreign policy in a more systematic way, reviewing the traditional parameters of action in which it has moved in the past*".[4]

The following thesis therefore aims to analyze the relationship between digital transformation[5] and Italian foreign projection. In doing so, it will specifically examine the Italian foreign policy in the region of the Wider Mediterranean, considered the area of priority national strategic interest for Italy. Indeed, in addition to the historic geopolitical importance for Rome, the region has recently acquired an increasing centrality following the war in Ukraine. The breakdown of relations with Russia means that the only geopolitical border for a projection of Europe is towards the south – towards the

[1] Burrows M. et al. (2022), *Unpacking The Geopolitics Of Technology: How Second- and Third-Order Implications of Emerging Tech are Changing the World*, Atlantic Council, Geotech Centre, p. 5
[2] Benigni D. & Ercolani A. (2017), *Digital Transformation: Nuovi Confini, Crescita e Sicurezza del Paese*, The European House – Ambrosetti, p. 12
[3] Szkarłat M. & Katarzyna M. (2016), *New Technologies as a Factor of International Relations*, Cambridge Scholars Publishing, p. 13
[4] Martini L. et al. (2022), *Crises in the Mediterranean. The Italian pivot: a new strategy for European and US engagement in the MENA region*, European Council on Foreign Relations, p. 1
[5] This paper will consider a general definition of digital transformation, such as the one provided by the Council of Europe: "*Digital transformation refers to the use of digital technologies, tools and applications of any kind: from digitisation of processes to blockchain and artificial intelligence*." https://rm.coe.int/study-on-the-impact-of-digital-transformation-on-democracy-and-good-go/1680a3b9f9

Mediterranean – and, furthermore, many European countries, among which Italy, are trying to reduce their energy dependence on Russia securing gas imports from the region, especially from North Africa and the Gulf.[6]

The first chapter introduces the Italian geostrategic concept of the Wider Mediterranean, analyzing how it has evolved over the last forty years according to Rome's national interests and how it has increasingly become the focus of Italian foreign policy. The section also deals with the strategic reorientation of foreign policy instruments towards the region, specifically taking into consideration the military, diplomatic and economic aspects. This part then outlines the growing digital transformation that has invested and is investing the region, explaining what consequences it entails from a social, economic and political point of view.

The second chapter examines the strategies with which Italy's main competitors relate to the geostrategic region, paying particular attention in this sense to the use of new digital technologies. Since the years of the second Obama administration, the US disengagement has led to a greater Russian and Chinese presence and to the growth of their influence at political, economic, and military levels.[7] In parallel with these global powers, regional powers are emerging with increasingly aggressive and destabilizing agendas. This is the case of Turkey, which is trying to expand its influence more and more towards Africa, and of Iran, which with its asymmetrical threats undermines the stability of the Middle East. This context evokes new challenges even in the traditional framework of Italian alliances. Indeed, as underlined by US Defense Secretary Lloyd Austin, in order for the United States to carry out a real pivot-to-Asia to begin the containment of China, the NATO allies must show readiness to take over the reins in other areas of the world from which Washington intends to disengage. This is particularly true for the Wider Mediterranean, where the space left by the US must be filled by European allies to curb the rise of global competitors and regional powers.[8] The section analyses if and how the strategies of these new emerging players, China, Russia, Turkey and Iran, take into account and are adapted to the new digital context that characterizes the macro-region.

Finally, the third chapter shifts the focus to Italian foreign policy. In particular, this analyses the relationship between digital transformation and Italian national interests in the Wider Mediterranean. To do this, with the help of the main programmatic document of Italian foreign policy, five aspects of particular Italian interest in the macroregion were identified: the protection of critical submarine

[6] Martini L. et al. (2022), *Crises in the Mediterranean. The Italian pivot: a new strategy for European and US engagement in the MENA region*, European Council on Foreign Relations, p. 1
[7] *Ivi*
[8] Rossi E. (2021), "Indo-Pacifico? L'Europa si concentri sul Mediterraneo Allargato. Il monito di Lloyd Austin", *Formiche.net*, https://formiche.net/2021/07/indo-pacifico-lloyd-austin/

infrastructures, the security of maritime trade, the fight against illegal immigration, counterterrorism and strategic autonomy in the procurement of raw materials.

# Chapter 1: Definition, evolution and digitalization of the concept of Wider Mediterranean

## 1.1 The "third and half circle" of the Italian foreign policy

The Mediterranean region has always represented an area of particular strategic interest for Italy since the time of the Unification. In addition to more strictly internal needs, such as that of securing a role in international relations and in the "concert of the great powers" for the new state, the reasons for this interest in the area were mainly linked to geopolitical aspects and strategic security. Firstly, the Mediterranean constitutes a privileged area of trade and traffic, not only with the states bordering it but also with those located on the main communication routes; secondly, for a country overlooking the sea as Italy, a lack of presence in the area would have represented an element of weakness and an incentive for the expansionist desires of other states.[9] These aspects have remained a priority throughout Italian history so much so that in the metaphor of the three concentric circles, to which academic literature has often referred to outline the main pillars of Italian foreign policy, Mediterraneanism has always been considered the "third circle" alongside Atlanticism and Europeanism.[10]

The theory of the three circles is also useful for figuratively understanding how the strategic concept of the Mediterranean has progressively evolved over time for Italy. As underlined by Dario Cristiani, indeed, "*the delimitation of these circles has never been too rigid and over the years they have adapted to the evolution of the international system and to the changes that have occurred and that have affected Italy, both on a more immediate scale and on a more global*".[11] Italian national interests in the region over the years have not remained limited to the Mediterranean basin and, for this reason, the Mediterranean circle gradually expanded to include territories and waters that progressively became strategic for Rome. Now it is possible to speak of a "third and a half circle"[12] and the strategic concept that has allowed this expansion is the "Wider Mediterranean". This is founded on the perception according to which, "*although geographically closed, the Mediterranean is strategically open along its two natural extensions: to the east, towards the Red Sea, the Western Indian Ocean*

[9] Perfetti F. (2011), "Mediterraneo e Medio Oriente nella politica estera italiana*", La Comunità internazionale*, fasc.2, pp. 185-202.
[10] Coralluzzo V. (2011), "Italy's Mediterranean Policy from a Transatlantic Perspective" in Aliboni R. et al., *Southern Europe and The Mediterranean: National Approaches and Transatlantic Perspectives*, German Marshall Fund of the United States, Mediterranean Paper Series 2011
[11] Cristiani D. (2021), "Tra Ue e Nato, così l'Italia è protagonista in Africa. L'analisi di Cristiani (Iai/Gmf)", *Formiche.net*, https://formiche.net/2021/04/italia-protagonista-in-africa-cristiani/
[12] *Ibidem*

*and the Persian Gulf; and to the west, towards the central Atlantic Ocean and the Gulf of Guinea"*. To this maritime arc is also added a terrestrial one that concerns inland areas such as the Sahel and the Balkans.[13]

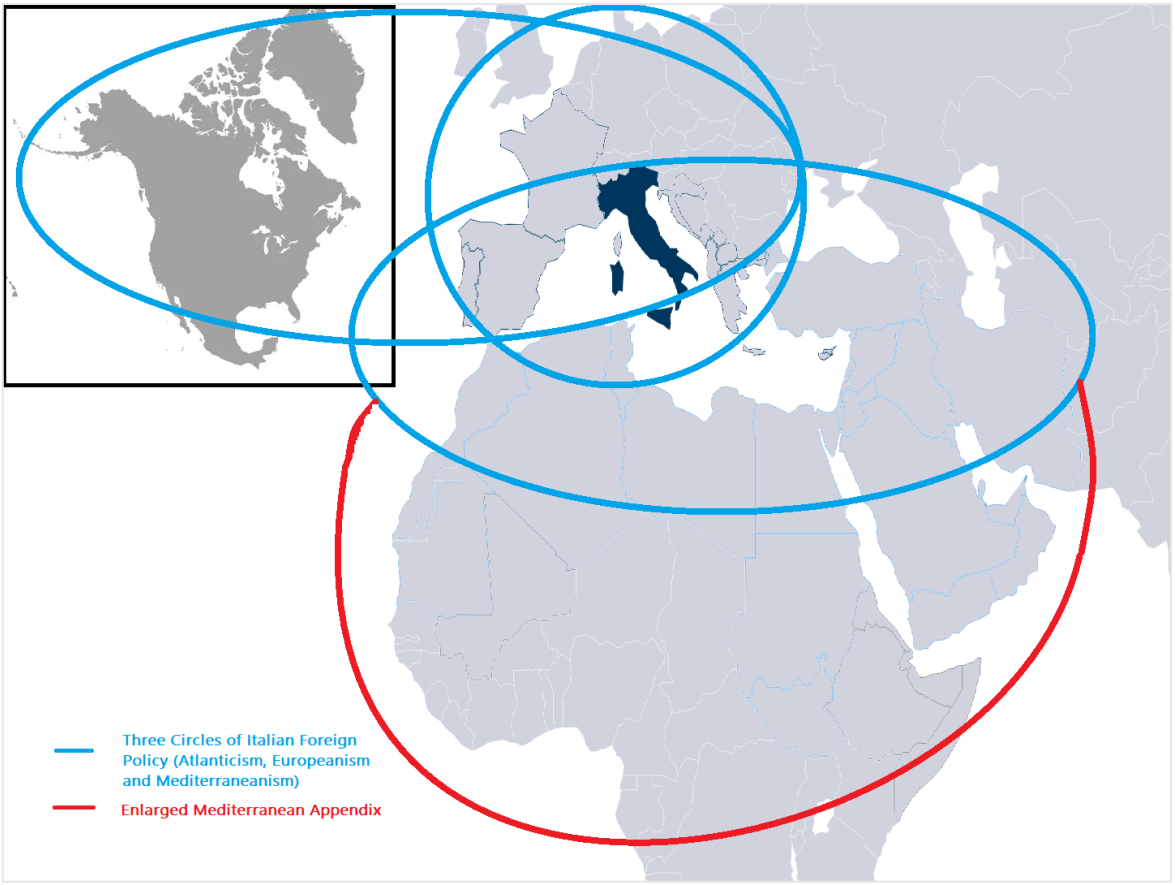


*Figure 1: the Three Circles and an half of the Italian foreign policy. Source: author's elaboration*

## 1.2 The evolution of the geostrategic concept over the years

### *The "first enlargement" towards the Middle East*

The Wider Mediterranean, however, is not a new concept and has not always been characterized by the borders just described, because the *mare nostrum* has "strategically" expanded over the years in relation to the evolution of Italian economic, political and military interests. The first attempt in this direction dates back to the end of the 1980s, by the War Institute of the Italian Navy, when the need to expand the focus even beyond the usual borders of the Mediterranean basin emerged in particular

[13] Franchetti Pardo L. (2020), *Sicurezza e gestione delle crisi. La dimensione marittima*, Circolo Studi Diplomatici, Dialoghi Diplomatici n. 250

towards the Middle East.[14] This necessity adapted and reflected the evolution in the approach of the Italian foreign policy towards the region, occurred at the beginning of the decade under the presidency of Spadolini. The leader of the Republican Party "*sought to adopt a more assertive role, proposing Italy as a mediator in a number of complicated situations that had developed in the Middle East"*.[15] This line of action was implemented both through the use of the Italian armed forces in peacekeeping operations, as the MFO (Multinational Force & Observers) in the Sinai and the two missions in Lebanon, but also through a great diplomatic commitment in contexts like the Israeli-Palestinian impasse and Lebanese civilian war itself.[16]

The 1985 Defense White Paper, published under the Spadolini Ministry of Defense, underlined for the first time the convergence between the concept of national security and the safeguarding of political and economic interests abroad, considering local conflicts as one of the main threats in this sense.[17] In this perspective, the conflict between Iraq and Iran and the various episodes of international terrorism, such as that of October 1985 with the kidnapping of the *Achille Lauro* steamboat by a Palestinian group, made the Middle East even more relevant for Italian foreign policy. This, also given the importance of the hydrocarbons import from the Persian Gulf and the call by the US to other countries for a more substantial presence in the area, highlighted the need to ensure an adequate Italian presence in the region[18] and was at the basis of the "first enlargement" of the Mediterranean.

The focus on the Middle East was further strengthened when the region became crucial for the fight against international jihadism following the terrorist attacks of 11 September 2001. In those years terrorism emerged as the main risk of international insecurity and instability, replacing the East/West opposition of the Cold War ended in 1989. In this context the protection of national security assumed a Wider meaning including, in addition to the defense of national sovereignty, the contribution to international stability and security, the legitimate safeguarding and protection of national interests, the prevention of old and new risks as well as the contrast to violations of law and peace.[19] This

[14] Di Cecco V. (2004), "Un "grande Medio Oriente" o un "Mediterraneo allargato"", *Panorama Internazionale: Informazioni della difesa*, n. 2

[15] Riccardi L. (2020), "Italy's foreign policy and the Palestinian question", in Monzali L. & Soave P. (eds.), *Italy and the Middle East*, Bloomsbury Publishing

[16] *Ibidem*

[17] Battisti G. (2017), "Le caratteristiche del "modello italiano" nelle operazioni di peacekeeping", in Caracciolo I. & Montuoro U., *L'evoluzione del peacekeeping. Il ruolo dell'Italia*, Centro Alti Studi per la Difesa, Giappichelli Editore, Turin, p. 310

[18] N.A., "Dal Libro Bianco 1985 al Golfo Persico", Marina Militare, Ministero della Difesa, https://www.marina.difesa.it/noi-siamo-la-marina/storia/la-nostrastoria/storianavale/Pagine/librobiancoMarina.aspx

[19] Italian Ministry of Defense (2002), *Libro Bianco 2002*

perspective was at the basis of the new Italian activism in the Middle East and the decision to follow the US in military interventions in Afghanistan and Iraq in the so-called "war on terror".

### *The renewed interest in Africa*

Parallel to the growing interest in the Middle East, Italian foreign policy has gradually concentrated also towards Africa after years of "minimalist approach" on the continent. Indeed, despite the strategic geographical position of Italy at the centre of the Mediterranean Sea, which could make the country the main point for convergence between Europe and the African continent, "*this geographical advantage has had no real bearing on Rome's relations with Africa, and its relations have instead been limited"*.[20] The first signs of a slow increase in the Italian interest in sub-Saharan Africa came in the 1990s but economic constraints, the "clean hands" scandal and the typical short duration of governments limited any successful attempts made by Rome in this sense. The efforts to increase its role in Africa, indeed, were not particularly effective, as demonstrated by the partial failure of the Italian military missions in Somalia (1992-1994) and by the mediations in regional crises (as the Ethiopian-Eritrean dispute), where Italy has never managed to establish itself as a relevant mediator. The most significant reapproach to the continent occurred only in 2013, under the government guided by Enrico Letta and, especially, under the executive guided by Matteo Renzi (2014-2016). The continent began to be increasingly defined as a "priority" in Italian foreign policy and the first Italy-Africa conference was organized in 2016. In those years the Prime Minister and the President of the Republic made visits to Sub-Saharan countries for the first time.[21] This renewed interest in the continent was due to two main reasons: on the one hand, the need to put the country's economy back on its feet after the 2008 economic crisis required focusing on emerging or frontier markets towards which to promote the internationalization of Italian businesses (the so-called "growth diplomacy"); on the other hand, the migratory crisis of 2014-2016 emphasized the need to manage and control migratory flows from Africa.[22] In particular, this second aspect was probably indicative in understanding that the traditional Mediterranean region, historically strategic for Italian foreign policy, can no longer be separated from the African context, which is often the place of origin of phenomena and factors of instability in the Mediterranean and constitutes a scenario in which

[20] Venturi, B. (2018), "Africa and Italy's Relations After the Cold War", In: Nagar, D., Mutasa, C. (eds) *Africa and the World*. Palgrave Macmillan
[21] *Ibidem*
[22] Carbone G. (2021), "Tra alti e bassi: l'Italia torna a guardare all'Africa", *ISPI*, https://www.ispionline.it/it/pubblicazione/tra-alti-e-bassi-litalia-torna-guardare-allafrica-29226

numerous Italian national interests intersect. An indication in this sense came from the 2015 Defense White Paper, which expresses a much Wider concept of Mediterranean:

*"The Euro-Mediterranean region does not represent a closed system or one not influenced by the dynamics that occur in other areas, in particular in those directly adjacent to it. Indeed, it is not possible to deal with certain crisis situations that develop in the areas of most direct interest without a broad understanding of the complex dynamics that generated them and an involvement in initiatives aimed at their resolution. For the protection of national interests and for the consolidation of the security and defense framework, therefore, the areas of the Mashreq, the Sahel, the Horn of Africa and the Persian Gulf countries are of particular interest*."[23]

This "enlargement" towards Africa clearly underlined for the first time the strategic importance of the Sahel and the Horn of Africa in addition to the traditional areas of interest such as the Mashreq and the Persian Gulf.

According to the document, in the Sahel the lack of state structures capable of adequately protecting the internal security conditions of the countries created the risk to project factors of instability towards the Mediterranean area.[24] In the last decade, indeed, the region has become particularly crucial for the security dynamics of Africa, but even of Europe. Since 2015, the border region between Mali, Niger and Burkina Faso - the "Liptako-Gourma" area - has been the stage for the "recomposition of the jihadist galaxy", with the establishment of the Islamic State in the Greater Sahara (ISGS), a local IS franchise, and the creation of the Group of Support for Islam and Muslims (Jama'a Nusrat al-Islam wa al-Muslimin, JNIM), a network composed by the main qaidists groups. These jihadist formations, leveraging on inter-ethnic tensions in rural areas, are gradually replacing state governance, presenting themselves to local communities as a preferable alternative to the central state.[25] To this context of instability are added the numerous illegal trafficking of which the region is a crossroads: from human beings, to drugs, weapons and natural resources.[26]

Even the "*significant, although indirect, importance"* of the political and social stability in the Horn of Africa was equally stressed.[27] The Horn, located between the Red Sea and the Gulf of Aden, close to the Bab al-Mandeb Strait, is strategic especially for its geographical position, representing a key artery of international trade between Europe and Asia. Guaranteeing the safety of the waters of the region, therefore, has become crucial around the 2010s, following the increase in cases of piracy and

[23] Italian Ministry of Defense (2015), *Libro Bianco 2015*
[24] *Ibidem*
[25] ISPI (2021), *Dal Sahel al Mozambico: Insorgenze Jihadiste in Africa Subsahariana*, Osservatorio di Politica Internazionale, Senato della Repubblica, n. 175
[26] UNODC (2012), *The United Nations Office on Drugs and Crime (UNODC) Contribution to the United Nations Integrated Regional Strategy for the Sahel*
[27] Italian Ministry of Defense (2015), *Libro Bianco 2015*

the economic impact they caused.[28] The region has also assumed particular relevance for the control of migratory flows, being the origin of many migrants who reach the European coasts, and for the containment of many outbreaks of instability for the African continent, such as the relations between Ethiopia and Eritrea, the Ethiopian-Egyptian dispute regarding the exploitation of the Nile waters and the presence of the jihadist group al-Shabaab in Somalia.

Over the last decade, a third has been gradually added to these two regions: the Gulf of Guinea, in which "*Italy has shown an active and growing commitment to stabilization*".[29] From 2019 onwards, all defense planning documents have begun to include the Gulf of Guinea in the definition of the Wider Mediterranean and to define it as "*one of the most important contexts for the country*"[30]. Indeed, the region has recently become particularly important for Italian national interests in particular in the energetic and commercial sectors. In 2020 Rome imported 18% of oil from African countries, almost half of which from those of the Gulf of Guinea, with Eni and Saipem having important infrastructures in the Niger Delta region.[31] From the commercial side, almost all of the goods exchanged with the African continent travel by sea passing through the Gulf and, for this reason, it is crucial for Italy to contribute to the safety of those waters, which over the last 15 years have become the world's hotspot for maritime piracy (in 2020, out of the 135 maritime kidnappings worldwide, 130 took place in the Gulf of Guinea[32]).

## 1.3 The recent shift towards the macro-region in the traditional Italian foreign policy instruments

Today, according to the Italian Parliament, the concept of the Wider Mediterranean, after the long process of evolution just described, "*sees the Mare nostrum basin as its pivot and extends from the Gulf of Guinea to the Indian Ocean, considering the entire African belt of the Maghreb and the Sahel, the Horn of Africa, the Middle East, the Black Sea and the Caspian Sea*". This wide area has

[28] Middleton R. & Quartapelle L. (2010), *Le conseguenze della pirateria nel Corno d'Africa*, Osservatorio di Politica Internazionale, Senato della Repubblica, n.11
[29] Crippa P. & Di Liddo M. (2021), *Sviluppo, Insicurezza E Volatilità Politica nel Golfo di Guinea*, Osservatorio di Politica Internazionale, Senato della Repubblica, p.35 https://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/affariinternazionali/osservatorio/approfondimenti/PI0165.pdf
[30] Italian Ministry of Defense (2020), *Documento Programmatico Pluriennale della Difesa per Il Triennio 2020-2022*, p. 17 https://www.difesa.it/Content/Documents/DPP/DPP%202020-2022.pdf
[31] Crippa P. & Di Liddo M. (2021), *Sviluppo, Insicurezza E Volatilità Politica nel Golfo di Guinea*, Osservatorio di Politica Internazionale, Senato della Repubblica, p.32
[32] IMB annual piracy report 2020

increasingly become the center of Italian foreign policy and "*one of the areas crucial for national security*." As a result, in recent years all the traditional instruments of Italian foreign policy have undergone a strategic reorientation towards the region: from the military and diplomatic presence to economic aid and development cooperation.[33]

### *Strategic reorientation of the Italian missions abroad*

The aspect where this reorganization has been most evident is perhaps the military one, where the 2015 Defense White Paper introduced the idea that "*maintaining stability in the areas incident on the Mediterranean Sea*" represents - after the defense of the state and the safeguarding of institutions - the main mission of the Italian armed forces. Since that moment, indeed, the Italian defense policy has undergone a progressive transformation which has seen the relocation of the troops engaged abroad towards the Wider Mediterranean area.[34] Today almost all Italian international missions focus

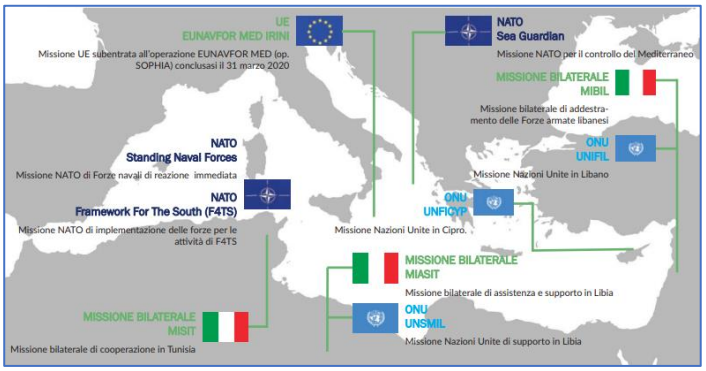


*Figure 2: Italian military presence in the Mediterranean basin*

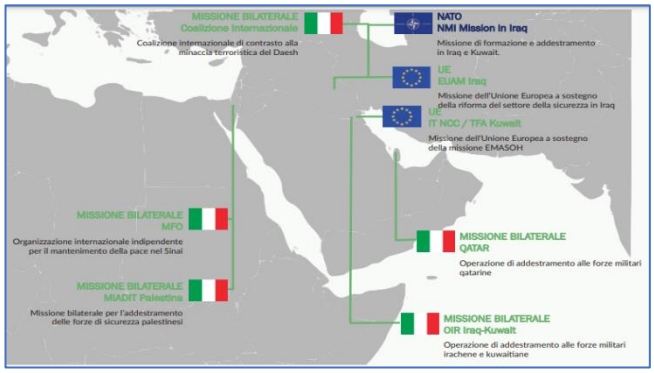


*Figure 3: Italian military presence in the Gulf*

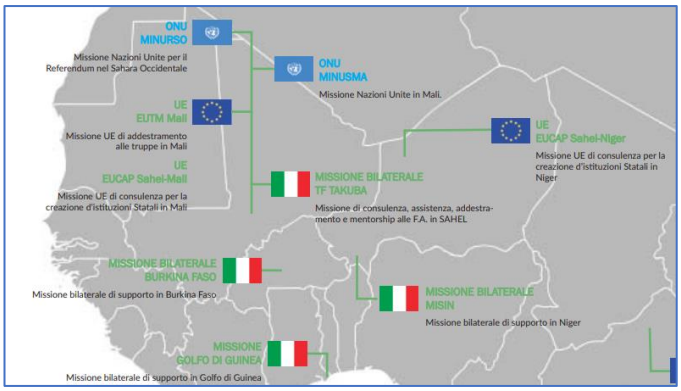


*Figure 4: Italian military presence in the Sahel and in the Gulf of Guinea*

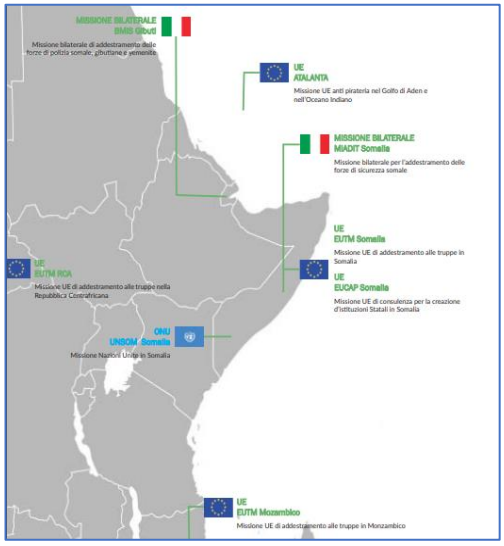


*Figure 5: Italian military presence in the Horn of Africa*

[33] Italian Parliament (2022), Relazione Annuale COPASIR 2021-2022
[34] Coticchia F. (2021), "Un centro di gravità permanente? La difesa italiana e il Mediterraneo allargato", *Formiche*, https://formiche.net/2021/04/mediterraneo-allargato-coticchia-unige/

on this theatre, with a military commitment which has progressively followed the emergence of new strategic regions for Rome. In addition to the traditional presence in the Mediterranean basin, functional to strengthening the ability to prevent "*strategic surprises*" and to support political-diplomatic activities aimed at protecting national interests in the region[35], the Italian armed forces have also been progressively sent to the rest of the Wider Mediterranean. This is particularly visible in Africa, where this relocation has been more pronounced in the last years. In the Sahel, Italy is engaged in the area that includes Mali, Niger and Burkina Faso integrating multilateral, coalition and bilateral activities, including the recent participation in the French-led Takuba Task Force. This effort aims to develop "*an ideal bond between North Africa and the Sahelian belt*"[36] in order to maximize the effectiveness of the contribution to the fight against terrorism and to the stabilization of the region. In the Horn of Africa and in the Gulf of Guinea, instead, Rome is engaged in various missions for maritime safety and the protection of maritime commercial traffic, as shown by the creation of an Italian aeronaval device on the coasts of the Gulf of Guinea in 2020. The Italian military presence in the entire Wider Mediterranean is also guaranteed in the Middle East, where, in addition to participating in multilateral missions for the fight against terrorism, it is also involved in training and supporting the local armed forces (the latest example is the new bilateral mission to support the Armed Forces of Qatar on the occasion of the 2022 World Cup).[37]

### *Diplomatic, cultural and economic focus*

Alongside the reorganization of military missions abroad, Italy has adapted its foreign policy to the new centrality of the Wider Mediterranean in other ways as well. First of all, this adaptation is visible in the expansion of the diplomatic network. In recent years, Italy has greatly increased its diplomatic representation in the region, as evidenced by the reopening of the Italian embassy in Mogadishu and by the new embassies in Niger, Burkina Faso, Guinea and Mali, plus the future one in Chad. Italy is even the first European country to have opened a Permanent Representation to the African Union. In parallel, Rome is also trying to increase its soft power in the area, as evidenced by the opening of the Italian Cultural Institute in Dakar and by the high number of scholarships granted by the Italian government to students belonging to the macro-region (Iran, Ethiopia and Tunisia are among the main beneficiaries of the scholarships funded by Rome for foreign students). Both diplomatic and cultural commitment in the area is also reflected in the annual organization of the "Mediterranean Dialogues",

[35] Italian Ministry of Defense (2022), *Defense Policy Document 2022-2024*
[36] *Ibidem*
[37] Italian Parliament (2022), *Autorizzazione e proroga missioni internazionali nell'anno 2022*

an annual conference launched in 2015 which has quickly become the global hub for high-level dialogues on the Wider Mediterranean, engaging prominent leaders of Mediterranean governments, business, civil society, media and academia.

Even from an economic point of view, the Italian line is consistent with this strategic reorientation. Indeed, Italian economic diplomacy has confirmed its willingness to adapt to the new centrality of the Wider Mediterranean and promote Italian commercial penetration in the region by opening two new ICE offices in Dakar and Nairobi and a SACE office in Accra which will act as commercial hub towards West Africa and, therefore, towards the Gulf of Guinea.[38] The Italian strategy is based not only on the trade of high quality products, but also on long-term investments and structured cooperation, through industrial partnerships in strategic sectors and transfers of technologies and know-how (not just the promotion of "Made in Italy", but also “Made with Italy”).[39] In this context, indeed, the Italian geopolitical position in the center of the Mediterranean, in the face of increasingly complex global phenomena, emphasized the need for a coherent foreign policy action in the region that is also based on development cooperation and sustainable economic development.[40] Among the countries identified as priorities by the AICS (Agenzia Italiana Cooperazione allo Sviluppo), the clear prevalence falls within the boundaries of the Wider Mediterranean (figure 6) and, among the main destinations of Italian economic aid, in addition to the more purely Mediterranean countries (Tunisia, Lebanon, Libya and Morocco), there are the Sahel (Mali and Niger), the Gulf of Guinea (Senegal) and the Horn of Africa (Ethiopia, Sudan and Somalia).

[38] Agenzia Nova (2022), *Diplomazia Economica Italiana: la cabina di regia per l’Internazionalizzazione*, MAECI, https://www.esteri.it/wp-content/uploads/2022/01/20220119-Newsletter-DEI-01_2022.pdf
[39] ISPI (2017), *La strategia italiana nel Mediterraneo*, MAECI, https://www.ispionline.it/sites/default/files/media/img/rapporto_med_maeci_2017_internet_1.pdf
[40] AICS (2021), *Documento Triennale Di Programmazione e di Indirizzo 2021 – 2023*, https://www.esteri.it/wp-content/uploads/2021/11/Schema-di-Documento-triennale-2021-2023.pdf

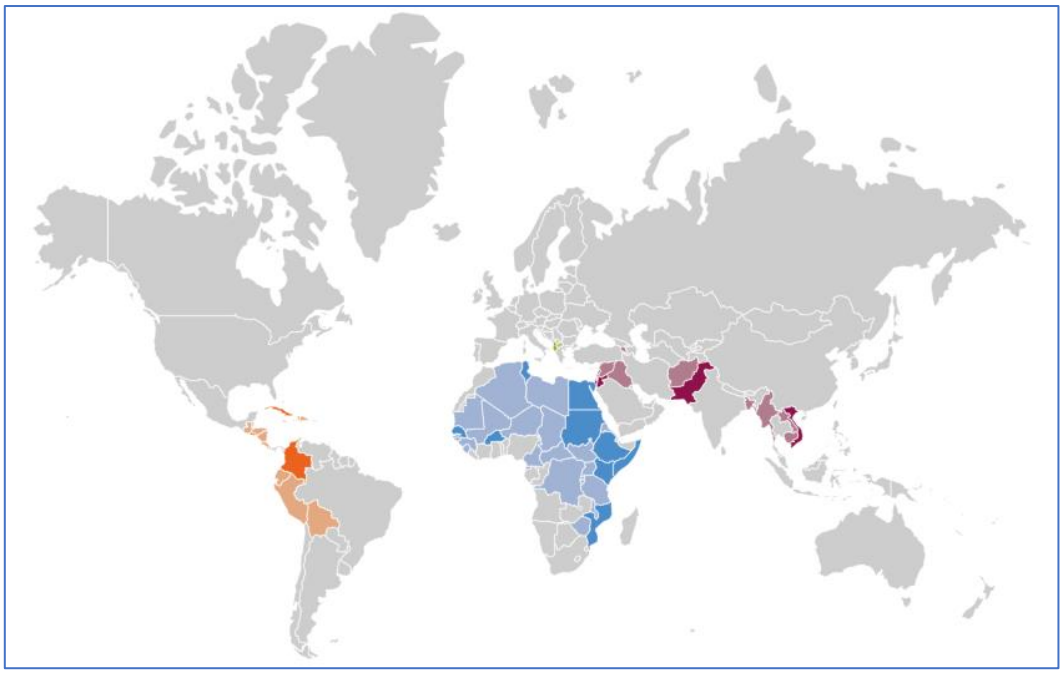

*Figure 6: Countries identified as priorities by the AICS (Agenzia Italiana Cooperazione allo Sviluppo). African countries in blue, Asian ones in violet and Americans in orange. Source: AICS*

## 1.4 The digitalization of the region and its consequences

### *The digital transformation of the macro-region*

Alongside these military, diplomatic and economic domains, in the global scenario and specifically in the Wider Mediterranean, another dimension has recently emerged, the digital one, which, rather than constituting a domain on its own, intersects and completes the others. The geostrategic region is grappling with a strong digital transformation, which is now a crucial factor to take in consideration to deal with this area. Indeed, according to the forecast from International Data Corporation (IDC), digital transformation investments in the Middle East and Africa are set to double across the 2020-25 period and the spending in this field in the region will accelerate at a compound annual growth rate (CAGR) of 16.6% over the five-year period, accounting for 40% of all ICT investments.[41] Despite the level of digitalization of the Wider Mediterranean varies between the MENA area and the countries of sub-Saharan Africa, in the whole macro-region the digital transformation, and in particular Information and Communication Technology, will play a crucial role in defining social, political and economic factors.

[41] Data by International Data Corporation (IDC), https://www.idc.com/getdoc.jsp?containerId=prMETA48468821

Over the last years, the Middle East and North Africa have witnessed one of the fastest-growing internet penetration rates in the world: from 30% in 2014 to more than double (67%) in only five years. The current trends will likely increase over the next years, as the region has a very young population (60% is under 30), who is particularly technological savvy and there is still a large portion of the population to connect, especially in North Africa (figure 7)

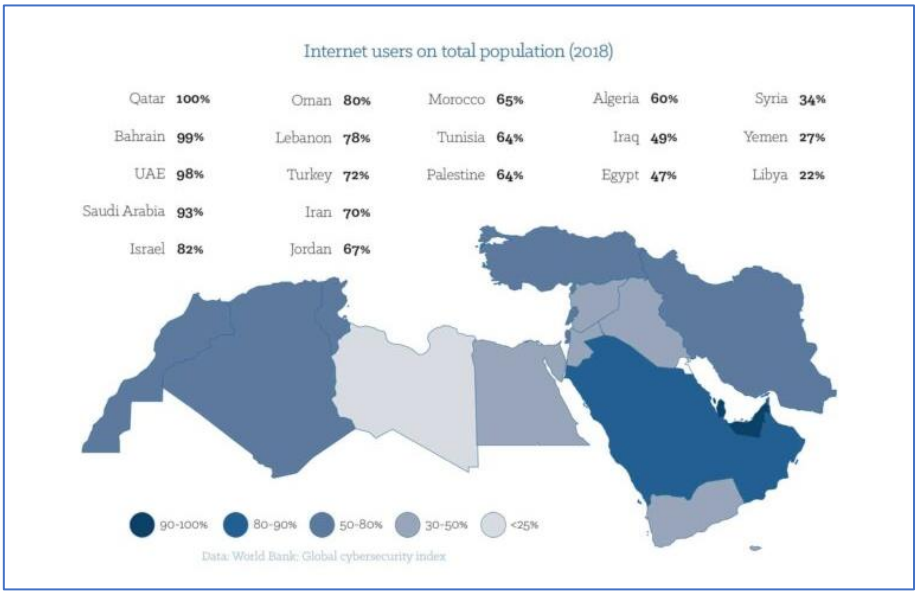


*Figure 7: Internet Penetration in the MENA. Source: ISPI*

The percentage of Internet users in the region according to July 2022 data was 79.7% (compared to a worldwide percentage of 69%)[42] and there are increasingly investments in information and communication technologies (ICTs). Especially in the Gulf, social infrastructure, the financial sector, government services, schools, and hospitals are irreversibly dependent on interconnectivity and Internet[43], in particular after the Covid-19 pandemic which emphasized the need to digitize many services. Governments are even implementing a series of measures to accelerate this process: for example the re-structuring of key public sector authorities to account for digital focus and ensure the prioritization of government digital transformation efforts, as in the case of Saudi Arabia which established a Digital Government Authority (DGA) in March 2021, following the launch of the Kingdom's national digital strategy, aiming to increase the prevalence, efficiency, and integration of digital services.

As regards the sub-Saharan appendages of the Wider Mediterranean, the trend is linked to the more general one of the entire continent. Africa is far behind in connectivity levels with the respect of the

[42] Data by Internet World Stats, https://www.internetworldstats.com/stats5.htm
[43] Aboul-Enein S. (2017), *Cybersecurity Challenges in the Middle East*, The Geneva Centre for Security Policy, Research Series n. 22/17

rest of the world but has the fastest-growing telephone and Internet networks, with a youthful population and rapid urbanization which are both strong drivers of demand for digitalization. The continent has more than 500 million Internet users, but this volume of users relative to population equates only to about 38%, which implies the number is expected to grow in the coming years with an additional 300 million Africans online by 2025.[44] The AU's Digital Transformation Strategy for Africa 2020-2030, in this sense, aims for a Digital Single Market and the full connectivity of the African population by 2030. Therefore, African countries are moving forward to incorporate digital infrastructure into the foundations of their society, including government, banking, business and critical infrastructure, with a strong growth in investment in mobile network, fibre-optic cables and data center localizations.[45] Focusing specifically on the regions of greatest Italian interest, it is possible to note how digital transformation will represents a crucial dynamic in the next few years. The Sahel is one of the regions in the world with the fastest growth rate in connectivity and Mali, Niger, and Burkina Faso are three of the fastest growing internet user bases in the world, even if the absolute numbers remain low: in just one year - from 2020 to 2021 - internet users increased by 18.5% in Mali, 18.9% in Burkina Faso, and 20.9% in Niger.[46] In the Horn of Africa, Kenya is considered the main technological hub of the entire continent, the so-called African Silicon Valley, and Ethiopia, despite the low percentages regarding access to information and communication technologies, "*has developed some of the most ambitious projects in Africa employing ICTs to support development*" and can count on huge foreign investments, mainly Chinese.[47] Finally, the Gulf of Guinea will benefit from the construction of two new cable systems, developed respectively by Google and Meta, Equiano and 2Africa , which will increase the connectivity of the region, improving the quality of the connection and lowering the prices of Internet.[48]

### *The consequences of the expansion of cyberspace*

This digitalization and expansion of cyberspace, however, bring different challenges and risks to face in the whole geostrategic region, which obviously differ according to the level of internet penetration and advancements in digital technology.

---

[44] INTERPOL (2022), African Cyberthreat Assessment Report
[45] *Ivi*
[46] Bako H., et al. (2022), *Conflict and Online Space in the Sahel: Challenges and Recommendations*, Search for Common Ground, Issue Brief
[47] Gagliardone I. (2016), *The Politics of Technology in Africa. Communication, Development, and Nation-Building in Ethiopia*, Cambridge University Press, p. 1
[48] Atkinson M. & Oshadami O. (2022), "Closing the Digital Divide in Africa", *Equinix*, https://blog.equinix.com/blog/2022/11/02/closing-the-digital-divide-in-africa/

In the Middle East, in its potential to be used overtly or covertly, cyberspace "*affords flexibility to states in the region, non-state actors, and state actors beyond the MENA region to pursue their geopolitical, ideological, and financial agendas"*.[49] One of the most analyzed dimensions regarding the effects of new technologies in the region concerns the relationship between society and the state. Indeed, wider access to the Internet is undermining censorship in a region that has traditionally been averse to the free flow of information. For instance, the proliferation of youth-generated media, especially YouTube and Twitter, gives access to content that would generally not be accessible due to government control of local media and also plays a key role in overcoming some gender barriers or traditionalist norms, providing citizens with the opportunity to come into contact with different cultures and interact with each other in the virtual world in a way that would not be possible in the real one. A huge amount of literature focuses in particular on the role of social media in the Arab Springs of 2011 in extend activism, facilitate collective action and mobilize social networks, with many which have seen precisely in their spread the determining factor of revolutions. The advent of new information and communication technologies, however, has not only influenced civil society, but also the strategies of the states of the region, which have shown a great ability to adapt to the changes brought by new technologies. A first example is the tendence by many politicians to adopt social media as a tool to engage citizens on public matters, but the most indicative one is related to the ability of governments to be able to extend their control and their repression of dissent even in virtual space.[50] In many cases, indeed, new technologies have allowed the authoritarian states of the region to intensify these measures as in the case of Egypt, first with Mubarak and then even more clearly and systematically with Al-Sisi.[51] Alongside this dimension, in the MENA region in the last two decades the cyberspace has been also "*a domain in and through which power is projected*".[52] The Middle East is the region in which the first act of cyber war, commonly referred to as Stuxnet, took place in 2010 when a malware, probably of Israeli and US planning, affected the turbines of the Natanz nuclear enrichment facility in Iran. Since then, cyber warfare has assumed an ever greater centrality in the strategies of the actors of the region, in particular of Iran and Israel, which have built

[49] Ach A. & Kurtz P. (2021), Conduct of Code: A Historical Overview of Cyberspace in MENA, in Campbell E. & Sexton M., (Eds.), *Cyber War & Cyber Peace In The Middle East: Digital Conflict In the Cradle of Civilization*, Middle East Institute

[50] Zayani M. (2018), Mapping the Digital Middle East: Trends and Disjunctions. In Zayani M. (ed.) *Digital Middle East: State and Society in the Information Age*, Oxford University Press

[51] For an insight into the cybersecurity policies of the Egyptian authorities over the last decade: Hassib B. & Shares J. (2021), Manipulating uncertainty: cybersecurity politics in Egypt, in *Journal of Cybersecurity*, Oxford University Press, pp. 1–16

[52] Ach A. & Kurtz P. (2021), Conduct of Code: A Historical Overview of Cyberspace in MENA, in Campbell E. & Sexton M., (Eds.), *Cyber War & Cyber Peace In The Middle East: Digital Conflict In the Cradle of Civilization*, Middle East Institute

and consolidated their gains as full-fledged cyber powers. Alongside the very expensive and difficult operations of penetration and manipulation of physical systems, many MENA states have focused on advancing their agendas in the information sphere, seeking to mobilize both domestic and international support for their policies through influence and information operations ("info-ops"), with a clear example coming from the disinformation effort following the 2017 Gulf crisis, in particular between the UAE and Qatar.[53] The scenario is made even more complicated by the fact that global powers (US, China and Russia) continue to treat MENA cyberspace as a proxy battleground in attempts to strategically shape norms of engagement in the domain and, at the same time, for nonstate actors, native to or operating in the region, cyberspace has become an environment conducive to criminal activity, a digital arms trade, and the propagation of false information and extreme ideologies.[54]

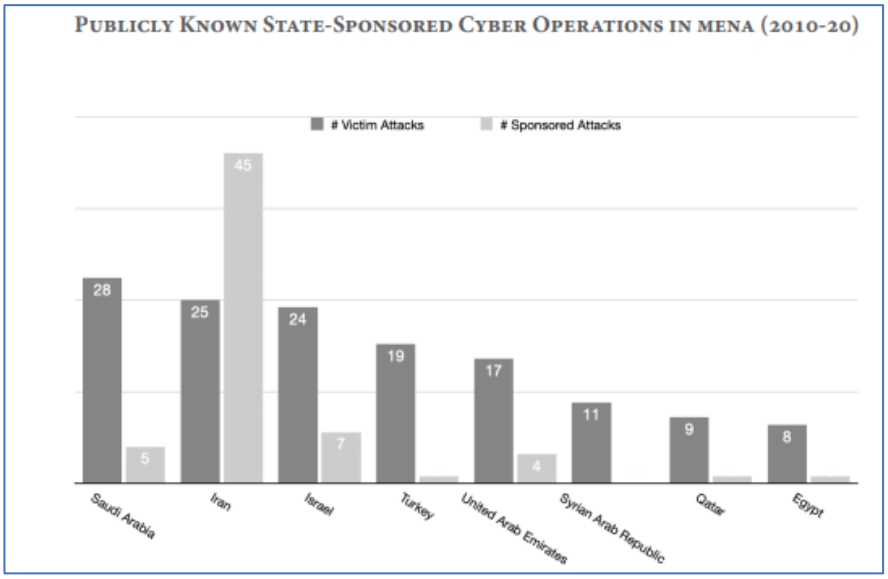


*Figure 8: the eight MENA countries most frequently victimized by cyberattacks (dark gray) and the frequency with which they sponsored attacks against other states (light gray) from 2010-20. Source: MEI*

Even in Sub Saharan Africa the spread of information, communications, and related technologies is amplifying and altering a variety of national security challenges and threats. These threats are exploited by a broad array of actors, who vary significantly in their capabilities and intentions, from nation states to lone wolf hackers and complex cybercriminal enterprises.[55] As in the Middle East, cyberspace is becoming a theatre of action increasingly frequented by state entities. On one hand, it has fundamentally changed the methods and means through which states gather information on one another and their citizens, rapidly diffusing espionage and surveillance capabilities across the continent; but even the use of information operations by states, their proxies and adversaries.[56] This particularly applies to the Sahel, where "*online spaces create a new arena for social challenges like*

[53] *Ach A. & Kurtz P. (2021), Conduct of Code: A Historical Overview of Cyberspace in MENA, in Campbell E. & Sexton M., (Eds.), Cyber War & Cyber Peace In The Middle East: Digital Conflict In the Cradle of Civilization, Middle East Institute*
[54] *Ibidem*
[55] N.A. (2022), "Understanding Africa's Emerging Cyber Threats", *Africa Center for Strategic Studies*, https://africacenter.org/programs/cyber/
[56] *Ibidem*

*disinformation, hostile confrontations, political manipulation, radicalization, and polarization to manifest*".[57] The Russian backed online-campaign targeting Mali, aimed to foment anti-Western sentiment and undermine democratic institutions by creating consensus around the May 2021 coup, is a clear example in this sense, but even other countries, for instance Burkina Faso, "*have found themselves engulfed in a world of deniable hybrid threats as they are swept up in a digital proxy war between East and West*".[58] On the other, cyberspace has transformed non-violent means of covert action and coercive statecraft causing an increasingly use of enhanced surveillance capabilities and emerging technologies, such as drones, on the African battlefield. In addition to the growing use of AI within surveillance systems, which for instance have enabled authorities to track violent, organized criminals with suspected ties to the Islamic State, AI has also been integrated into weapon systems. Relatively low costs, tactical advantages, and the emergence of multiple suppliers have led to a booming market for low-and-mid tier combat drones, particularly Turkey's Bakratyar TB2, which have been acquired and used by well over a dozen African countries.[59] Obviously, however, states have not been the only actors involved in the process of expansion of cyberspace, but more and more private actors have emerged alongside them. This applies in particular to cybercrime, which is rapidly expanding on the continent especially following the digitalization "promoted" by Covid-19. The spread of cyberspace, indeed, is providing tech-savvy groups with novel business opportunities and new means to steal, transfer, or extort resources, leading to new kinds of cyber-dependent criminal activities, such as business email compromise or online scams. This is a particularly worrying issue for the growth prospects of the African continent, considering that a research from a Kenyan IT cybersecurity company highlighted that cybercrime reduced African GDP by more than 10%, at a cost of an estimated 4.12 billion USD in 2021.[60] Among these cybercriminal activities, the attack on critical African infrastructures has recently become more and more popular, above all through the use of ransomware. In this context, Africa's government networks, military systems, banking and telecommunications industries are vulnerable to cyberattacks, coming from both private criminal organizations and nation states, that seek to disable or destroy them.[61] For instance, in May 2022, the Director General of the Ethiopian Information Network Security Agency (INSA) reported that INSA

[57] Bako H., et al. (2022), *Conflict and Online Space in the Sahel: Challenges and Recommendations*, Search for Common Ground, Issue Brief
[58] Allen K. (2022), "Hybrid warfare – Africa beware", *Institute for Security Studies*, https://issafrica.org/iss-today/hybrid-warfare-africa-beware
[59] Allen N. & Opkali M. (2022), "Artificial Intelligence Creeps on to the African Battlefield", Brookings, https://www.brookings.edu/techstream/artificial-intelligence-creeps-on-to-the-african-battlefield/
[60] INTERPOL (2022), African Cyberthreat Assessment Report
[61] N.A. (2022), "Understanding Africa's Emerging Cyber Threats", *Africa Center for Strategic Studies*, https://africacenter.org/programs/cyber/

had intercepted an international cyber-attack attempt on the Grand Ethiopian Renaissance Dam that targeted 37,000 interlinked computers used by financial institutions and the country's major financial institutions.[62]

## 1.5 An evolving social, economic and political context

The chapter analyzed the geostrategic concept of the Wider Mediterranean which, starting from the 1980s, progressively enlarged the strategic borders of the "*Mare Nostrum"*. The first "enlargement" involved the Middle East and the Persian Gulf, which have become particularly crucial areas for energy supplies and for the fight against jihadist terrorism. In the following years the geostrategic region, mainly for security reasons, expanded towards Sub-Saharan Africa, integrating the two natural extensions of the Mediterranean, the Gulf of Guinea and the Red Sea (therefore the Horn of Africa), but also the internal strip that connects them, the Sahel. In addition to the expansion of its borders, the Wider Mediterranean has seen a progressive growth of importance within Italian foreign policy to the point of being identified as an area of main national interest. This centrality has effectively been confirmed by the reorientation of all the main Italian foreign policy instruments towards the region: almost all of the military missions abroad have been concentrated in the Wider Mediterranean; diplomacy has also followed this line with the opening of new embassies in the Sahel; and even the economic dimension has seen a concentration of development cooperation in the macro-region. Alongside these aspects, however, the region imposes the need to take into consideration another domain, the digital one, which inevitably intersects with the previous ones. Indeed, the Wider Mediterranean is experiencing, albeit on different levels given the disparity of digital penetration in the macro-region, a growing digital transformation. The impact of digitalization and the expansion of cyberspace affects all aspects of society: from the economy, to society and politics, but also regional warfare and conflicts. This has changed both the logic with which states carry on their rivalries, for example with the emergence of cyberattacks or the disinformation operations, and the relationship between the state and citizens, affecting the amount of information available for civil society. In particular the phenomenon of cybercrime assumes a crucial relevance, because it severely slows down the growth prospects of the region. Cyberattacks against critical infrastructures are on the rise, particularly in Africa, where cyber resilience is not yet developed enough.

[62] Makory J. et al. (2022), *Combating Cybercrime on Critical Infrastructure in the Region*, ALN Kenya Anjarwalla & Khanna

# Chapter 2: The evolving geopolitical framework and the digital strategies of the new competitors

## 2.1 China and the Digital Silk and Road Initiative

***A new protagonist in the Wider Mediterranean***

The 2022 COPASIR report defines China as "*a strategic adversary*" for Italy and highlights Chinese dynamism in the Wider Mediterranean, which for Beijing *"represents a basin of energy resources, an important market for Chinese goods and an indispensable maritime transit point for the global export*".[63] The macro-region constitutes a strategic junction for the global power ambitions of Xi Jinping's China, as "*whoever controls the Mediterranean has a direct access to the oil resources of the Persian Gulf, the rapidly growing economies of Africa, the military power of NATO, the economic engine of the European Union, and the often unstable regions of the Middle East and sub -Saharan Africa*".[64]

Chinese interest in the macro-region has deep historical roots, with a crucial turning point following Deng's revolutionary economic reform and opening in 1979, when Chinese capital started to be used to set up companies abroad. "*In the four decades that followed, the Mediterranean region shifted from being a distant component of the "intermediate zones" into the most important area, after the Asia Pacific region, for the strategic projection of Chinese interests and influence"*.[65] In particular, Beijing's focus on the Wider Mediterranean, has strengthened over the past decade with the rise to power of Xi Jinping and his willingness to increase China's international weight, making it a global power promoting a new "community of shared destiny". Although Chinese assertiveness remains mainly focused on the economic sphere, Beijing is starting to be an increasingly present player in the area also in other sectors. Not only have diplomatic ties been strengthened, but relations have also increasingly extended into the field of security cooperation, especially in the African appendices of the geostrategic region. In addition to the more than 40,000 Chinese peacekeepers that have served in 24 UN missions since 1989, including peacekeeping operations in South Sudan and Mali, China strongly supports regional peace and security organisations (such as African Union and IGAD), and

[63] Italian Parliament (2022), Relazione Annuale COPASIR 2021-2022

[64] Attanasio Ghezzi C. & Cavalieri R. (2021), "Is the Mediterranean Sea Still the Mare Nostrum? The Belt and Road Initiative and Chinese Investments in the Region" in Corrao F.M. and Redaelli R. (eds.), *States, Actors and Geopolitical Drivers in the Mediterranean*, Palgrave MacMillan

[65] Fardella E. & Ghiselli A. (2019), "Introduction" in Fardella E. & Ghiselli A. (eds.), *China's New Role in the Wider Mediterranean Region*, Torino World Affairs Institute, ChinaMed Report 2019

participates in counter-piracy measures in the Gulf of Aden. Bilaterally, Beijing conducts joint military exercises, sells arms, supported peace mediation in Sudan and South Sudan, and, since 2017, operates a military base in Djibouti.

Despite this, Xi's main tool for achieving this coveted "community of shared destiny" remains the Belt and Road Initiative (BRI), an investment project launched in 2013 with the aim of connecting China with the rest of the world through two primary routes: the land-based 'Silk Road Economic Belt' and ocean going 'Maritime Silk Road'. Under this framework, especially regarding the route by sea, "*the Mediterranean region is becoming a fundamental component of China's anti-hegemonic struggle in the New Era*", because of its recent renewed cruciality in connectivity. Since 2015, the Suez Canal expansion, the emerging naval gigantism, and the acceleration of global alliances made by shipping companies progressively reinforced the competitive advantage of the Europe–Far East route, restoring to the Mediterranean Sea a forgotten 'centrality'. For this reason, China, which aims to become a "*strong maritime country*" and whose trade goes by sea for three-fifths, placed the Wider Mediterranean at the center of the global network of shipping and port assets shaped by the Chinese state-owned companies in recent years.[66] They provide the capital to build or upgrade commercial terminals; then they direct container traffic to those ports through shipping lines that are controlled directly by the port's parent company or indirectly through companies associated with China's strategic port owners. Examples of this strategy are the investments in the Athens' port of Piraeus which, since its acquisition by the Chinese company COSCO in 2016, has experienced a large increase in traffic volumes and 92% higher profits, but even the investments in the North African ports of Port Said in Egypt, Cherchelle in Algeria or Tangier in Morocco.[67] As visible in the figure 9, the Chinese strategy clearly extends even to the rest of the Wider Mediterranean involving the Gulf of Guinea and in particular the Horn of Africa. Here, China is engaged in various projects for the construction and expansion of strategic ports that face the Indian Ocean sea lanes connecting China to Africa, such as Doraleh in Djibouti or Mombasa and Lamu in Kenya. These projects are considered a potential gateway to vast, underserved markets and untapped resources in inland Africa and are linked to the clear Chinese need to reduce transport costs on its huge and growing trade with the continent.[68]

[66] Fardella E. & Ghiselli A. (2019), "Introduction" in Fardella E. & Ghiselli A. (eds.), *China's New Role in the Wider Mediterranean Region*, Torino World Affairs Institute, ChinaMed Report 2019
[67] *Ibidem*
[68] Kardon I. (2022), "China's Ports in Africa", in Rolland N. (eds.), *(In)Roads and Outposts: Critical Infrastructure in China's Africa Strategy*, National Bureau of Asian Research, Special Report no. 98


*Figure 9: PRC Ports Projects in Africa. Source: National Bureau of Asian Research*

This need is even the basis of the Chinese focus on improving connectivity by land, especially by rail. In particular in Africa railways carry a strong political salience in China's infrastructure investment and have become one of the largest sectors of financing and construction on the continent. This has included several massive national infrastructure investments, utilizing Chinese standard-gauge railway (SGR) technology and construction contractors.[69] Also in this case it can be seen how Chinese investments are once again favouring the regions that are part of the Wider Mediterranean. The three largest national SGRs in Africa in terms of value are located in Ethiopia, Nigeria and Kenya and involve Chinese financing, Chinese construction, and eventual Chinese management over their entire life cycles. These railways have become symbols of African modernization for political leaders as well as flagship projects in BRI.[70] On one hand, they respond to Chinese commercial needs to lower transport costs for its exports and reach African growing markets more easily, on the other, they offer opportunities in terms of political and economic influence on the continent. In the last two decades, indeed, China has become the largest bilateral lender on the continent and African governments are increasingly indebted to China for funding these large infrastructure projects, so much so that many analysts have denounced the predatory nature of the investment agreements and

[69] Chen Y. (2022), "African Railway Ambitions Meet China's Belt and Road", in Rolland N. (eds.), *(In)Roads and Outposts: Critical Infrastructure in China's Africa Strategy*, National Bureau of Asian Research, Special Report no. 98
[70] *Ibidem*

have spoken of a "debt trap" orchestrated by Beijing. Among a sample of 100 Chinese government loans to developing countries, researchers last year found that all loans since 2014 included confidentiality clauses. These clauses not only hide loan conditions from citizens and civil society but also prevent other lenders from accurately assessing the borrower country's debt profile. *The costly drawbacks of Beijing's loan conditions are a prime example of what scholars call China's "sharp power." Unlike military hard power or cultural soft power, China's sharp power represents the manipulative erosion of good governance to advance Beijing's position within the global order*.[71]

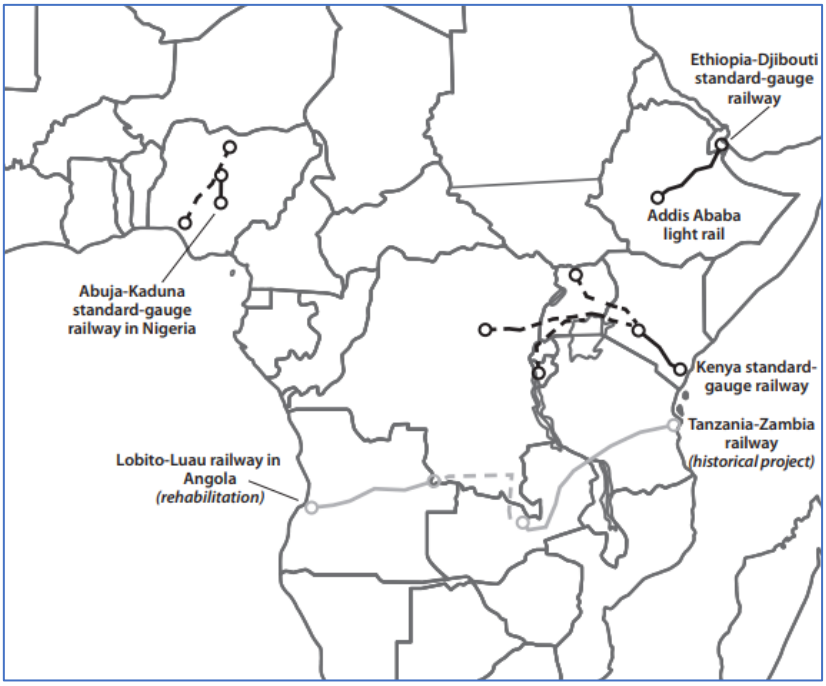


*Figure 10: Chinese-built railways. Source: National Bureau of Asian Research*

### *The Digital Silk Road*

Beijing's strategy, however, is not limited only to increasing maritime and terrestrial connectivity but also take in strong consideration the digital sphere. At the World Internet Conference in 2015, Xi declared that "*China will vigorously implement a strategy to make China a cyber great power*" including through construction of a "*community of common destiny in cyberspace*".[72] According to the China's 2015 National Development and Reform Commission White Paper, indeed, regional integration has three types of connectivity: transport infrastructure, energy infrastructure, and ICT infrastructure, conventionally referred to as the "Information Silk Road". In this sense, in 2017, at the

[71] McPherson-Smith O. (2022), "Transparency is derailing China's debt trap diplomacy", *The Hill*, https://thehill.com/opinion/international/3738211-transparency-is-derailing-chinas-debt-trap-diplomacy/
[72] De La Bruyere E. et al. (2021), *China As A "Cyber Great Power" Beijing's Two Voices In Telecommunications*, Brookings, Foreign Policy Report, p. 5

first Belt and Road Forum, Xi outlined the critical role of digital technologies to the overall BRI and called for the construction of a 21st-century Digital Silk Road. As stated by the Chinese Politburo member Wang Huning, the aim of the DRS is to create a: *"…mutually beneficial, win-win direction of development; to deepen Internet and information technology, build a cyber superpower, and advance society through a digital China*".[73] At the time of its first formulation, one of the essential components of the DSR was the construction of physical infrastructure – such as cross-border optical cable network – which, being able to be positioned for example alongside the railways, could benefit from the transportation infrastructure that China planned via the BRI. In the following years, however, the Chinese government has greatly expanded the ambition and scope of the Digital Silk Road , and nowadays, according to the MERICS BRI Tracker database, Beijing's updated policy goals also include data and research centres, smart city projects, and large e-commerce and mobile payment deals.[74]

To achieve these objectives a pivotal role is played by domestic companies, which "*are sought out by policymakers to assist China in becoming a cyber superpower […] and are tasked with becoming drivers to elevate digital value creation and standard-setting, with the ultimate goal of promoting Chinese state-defined interests*".[75] The DSR strategy is thus accompanied by a series of domestic initiatives which are intended to elevate the role of technology and the internet in China's national security agenda. The "MIC 2025", "China Standards 2035", "Internet+", the "MCF" and the so-called "Going-Out Strategy" are some examples in this sense and involve commercial IT promotion and encouraging state (financial) support. For their part, Chinese companies have shown enthusiastic support for the DSR, given that Chinese telecommunications infrastructure and cable industries face domestic overcapacity and the DSR gives them an opportunity to have new markets abroad.[76]

Obviously the DSR presents a series of opportunities even for the government. First of all, the increased overall competitiveness and involvement in the construction of IT infrastructures around the world by Chinese firms is functional to the boost of the Chinese economy and China's global influence, in particular within the global telecommunications industry. Indeed, Chinese internally directed discourse suggests competitive ambitions to set international technical standards for the sake of increasing global power, because, as underlined by Xi Jinping, "*at present, the cybersecurity game*

[73] Chan K. & Hungerland N. (2021), *Assessing China's Digital Silk Road: Huawei's engagement in Nigeria*, LSE Ideas, Digital IR Working Paper, n. 11, pp. 3-4
[74] Arcesati R., Eder T.S., Mardell J. (2021), "Networking the "Belt and Road" - The future is digital", *Mercator Institute for China Studies*, https://merics.org/en/tracker/networking-belt-and-road-future-digital
[75] Chan K. & Hungerland N. (2021), *Assessing China's Digital Silk Road: Huawei's engagement in Nigeria*, LSE Ideas, Digital IR Working Paper, n. 11, p. 4
[76] *Ivi*, pp. 4-5

*of the great powers is not only a game of technology, but also a game of ideas and discourse power*".[77] In particular, 5G and information technology more broadly play a central role in China's standard-setting agenda, as "*setting those standards offers the chance to write the rules of the future world and, in doing so, to leapfrog, or supplant, the Western order*."[78] This perspective is clearly explained by the words of Yang Zhen, former-chairman of the Council of Jiangsu Institute of Communications, according to which "*if the key technologies and main standards of the Internet of Things are in the hands of Western developed countries, and [China] has no independent intellectual property rights, then China will have no chance of achieving its peaceful rise and national rejuvenation*".[79] In this project of reform of the global internet governance system, Digital Silk Road is one the principal mechanisms and constitutes an important mean to reach consensus on Chinese proposals.

Another advantage of the DSR for the government concerns the data acquisition, which is considered by Beijing as a critical commodity and source of power. Since the publication of the Action Plan to Promote the Development of Big Data (2015) and the 13th Five-Year-Plan (2016), which designate data as "a foundational strategic resource", China has created legal frameworks for companies to provide data to the central government on national security grounds. This is particularly significant considering that much of the infrastructure along the Digital Silk Road is data-driven, as the undersea cables, which transmit more than 95 percent of global internet traffic. [80] Information power is even strictly linked with military power, as underlined by Zheng Anqi of the China Academy of Information and Communications Technology, and, therefore, information capabilities lie at the heart of China's military modernization program.[81] In particular the generation and utilization of geospatial data is considered crucial by Chinese military experts, especially after the 1996 Taiwan strait missile crisis, when the PLA lost track of two missiles it fired into the East China Sea and attributed the failure to a disruption in the U.S.-controlled Global Positioning Satellite (GPS) technology.[82] In this sense, the implementation of a myriad of Chinese-owned or Chinese-linked satellites permits inter-satellite linking ("ISL"), allowing the different satellites to connect and communicate with each other

[77] De La Bruyere E. et al. (2021), *China As A "Cyber Great Power" Beijing's Two Voices In Telecommunications*, Brookings, Foreign Policy Report, p. 15
[78] *Ivi*, p. 18
[79] *Ivi*, p. 19
[80] Aluf D. (2022), "China's Tech Outreach in the Middle East and North Africa", *The Diplomat*, https://thediplomat.com/2022/11/chinas-tech-outreach-in-the-middle-east-and-north-africa/
[81] De La Bruyere E. et al. (2021), *China As A "Cyber Great Power" Beijing's Two Voices In Telecommunications*, Brookings, Foreign Policy Report, p. 12
[82] Aluf D. (2022), "China's Tech Outreach in the Middle East and North Africa", *The Diplomat*, https://thediplomat.com/2022/11/chinas-tech-outreach-in-the-middle-east-and-north-africa/

and providing a boost to the military capabilities of the People's Liberation Army, such as in the areas of missile guidance and military forces tracking.[83]

***DSR in the Wider Mediterranean***

Even in the case of the Digital Silk Road, the Wider Mediterranean is a crucial region due to its strategic position in terms of connectivity between China and the West. The Digital Silk Road has become a substantial part of Chinese engagement in the Mediterranean basin for a series of reasons. First of all, in absence of internet connection, software, and cybersecurity, much of the infrastructure built within the framework of the BRI, as ports or railways, would not be able to operate effectively. Therefore, infrastructure like the Chinese PEACE undersea cable ensures that port operators enjoy the high-speed, low-latency connectivity critical for maintaining the integrity of supply chains and other activities that promote China's economic stability. Secondly, the region represents an attractive market for Chinese tech firms to expand their presence abroad, given the various projects of economic diversification of the MENA countries such as Smart Dubai 2012 or Saudi Arabia's Vision 2030, but even a strategic hub to acquire digital innovations and know-how, as in the case of Israeli vibrant innovation ecosystem which has become a Chinese prime target. Digital involvement in the region is also strategic for China from the side of information and data acquisition, with the 2017 launch of the China-Arab States BeiDou Cooperation Forum, which gives Beijing the opportunity to use data gathered from these satellites in the military domain and in other fields as environmental monitoring, smart agriculture, disaster relief, and transportation.[84] Finally, the Digital Silk Road in the MENA region also has important strategic implications for China in terms of competition with the US. Indeed, *Beijing has come to view its technology cooperation with MENA as increasingly important in countering U.S. efforts to contain China's rising power and influence*. The region is the only one in which Chinese investment has not fallen since 2018, following US measures to discourage allies from cooperating with Beijing. The MENA countries, in fact, due to the decline in energy exports to Washington, have a particular need of the Chinese market and are therefore more inclined to accept Chinese technological investments and cooperation in their countries, even due to the apolitical and neutral approach of China, which avoid to take parts in the various Middle Eastern conflicts such as the Israeli-Palestinian question or the rivalry between Saudi Arabia and Iran. This allows China to

[83] Chan K. & Hungerland N. (2021), *Assessing China's Digital Silk Road: Huawei's engagement in Nigeria*, LSE Ideas, Digital IR Working Paper, n. 11, p. 5

[84] Aluf D. (2022), "China's Tech Outreach in the Middle East and North Africa", *The Diplomat*, https://thediplomat.com/2022/11/chinas-tech-outreach-in-the-middle-east-and-north-africa/

insert itself and gain influence in a region traditionally recognized as US dominance, without even having to adopt an assertive posture like the Russian one.[85]

If DSR represented a crucial factor of acceleration for Chinese digital investment in the MENA region, in the Sub Saharan appendages of the Wider Mediterranean this initiative was only a rebranding of the previous and pre-existing Chinese investments in telecommunications.[86] Indeed, the Chinese influx into African telecoms sector started with the continent's telecommunications revolution in the 1990s, when many African countries liberalized their telecommunications sectors and upgraded their infrastructure. In this context, Chinese telecoms companies—through competitive pricing, low production costs, cost-effective equipment and solutions, and access to Chinese state-subsidized funding and support—have penetrated and dominated Africa's telecoms sector, wresting market share from major non-Chinese firms, such as Ericsson, Alcatel, Nokia, and Siemens.[87] This penetration took place especially in areas of Italian national interest as China's strategic priorities clearly focused on the Horn of Africa and the Gulf of Guinea. In the period between 2000 and 2014, the African country that received the most Chinese funding for telecommunications was by far Ethiopia, with over 3.5 billion $, followed by Nigeria and Angola.[88]

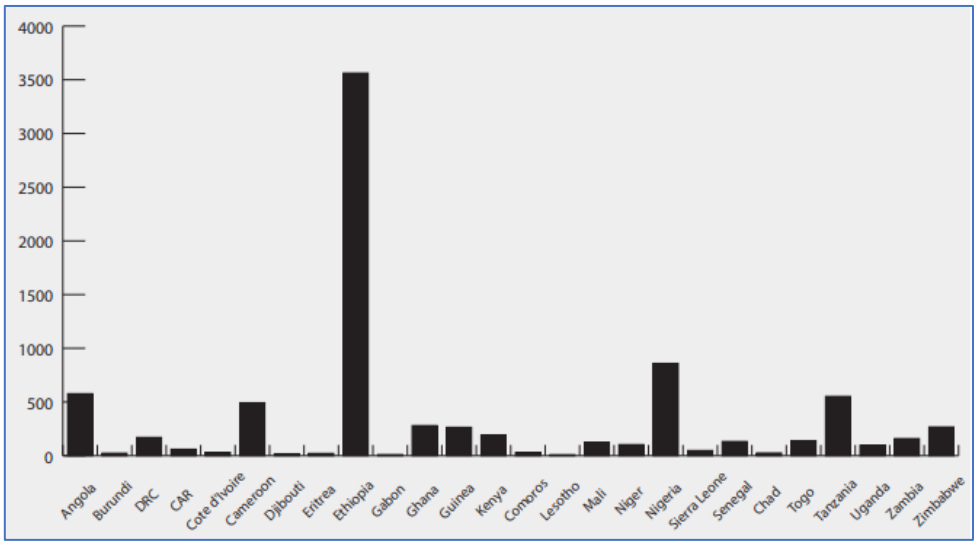


*Figure 11: Chinese Technology Infrastructure Loans by Country in US$ Millions (2000-2014). Source: Johns Hopkins University*

[85] Afterman G. (2021), *China's Evolving Approach to the Middle East: A Decade of Change*, Institute for National Security Studies, Strategic Assessment, Vol. 24, n. 1
[86] Tugendhat H. & Voo J. (2021), *China's Digital Silk Road in Africa and the Future of Internet Governance*, School of Advanced International Studies, Johns Hopkins University, China Africa Research Initiative, Working Paper n. 50, p. 18
[87] Agbebi M. (2021), *China's Digital Silk Road and Africa's Technological Future*, Council on Foreign Relations, p. 2
[88] Tugendhat H. & Voo J. (2021), *China's Digital Silk Road in Africa and the Future of Internet Governance*, School of Advanced International Studies, Johns Hopkins University, China Africa Research Initiative, Working Paper n. 50, p. 16

China's digital footprint started with the "infrastructure layer" – the fiber optic cables and mobile broadband systems that provide the Internet to the population – (70 percent of the continent's 4G networks were built by Huawei)[89] and over time has extended to the entire digital ecosystem of the continent. Indeed, by building core telecoms network infrastructure in these countries, companies such as Huawei and ZTE have positioned themselves to win subsequent network upgrade contracts and provide complementary services in the contracting countries, as in Tanzania, where China International Telecommunication Construction Corporation (CITCC) constructed the national ICT broadband backbone to be compatible only with Huawei routers.[90] In the following years, the launch of the DSR helped even more these companies to expand their presence on the continent thanks to the incentives and funding they can count on from the Chinese government. So much so that, in 2015 and 2017, Chinese ICT infrastructure financing (not limited to development assistance) surpassed the combined funds from multilateral agencies, G7 nations, and African governments.[91] Now "*Chinese technology companies permeate almost all layers of Africa's telecommunications technologies, from undersea cables, satellites, and backbone infrastructure to applications and platforms for individual consumers"* (Figure 13) and *"this dominance draws African countries further into China's technological sphere of influence"*.[92] One factor that helped the

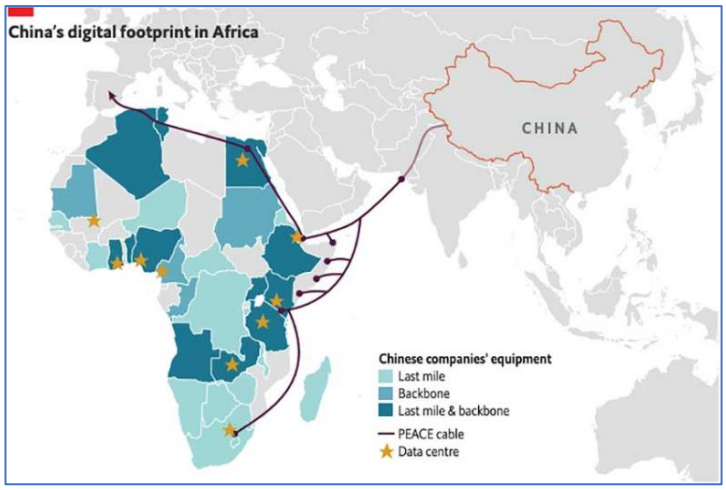


*Figure 12: China's digital footprint in Africa. Source: The Economist Intelligence Unit*

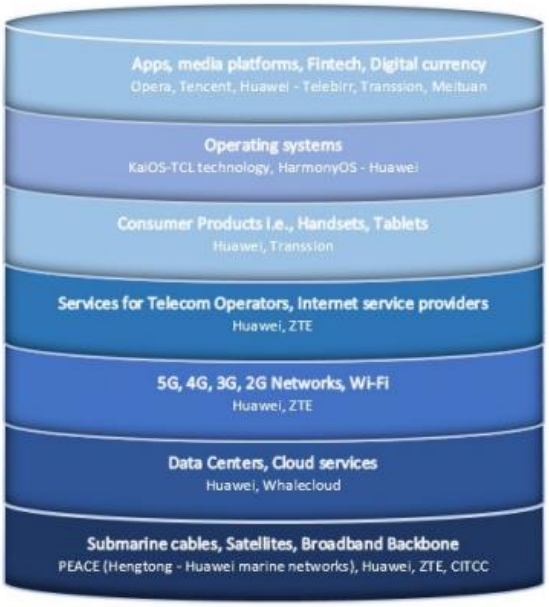


*Figure 13: China's in Africa telecom technology stack*

[89] Arcesati R. (2021), "China's Evolving Role in Africa's Digitalisation: From Building Infrastructure to Shaping Ecosystems", *ISPI*, https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247

[90] Agbebi M. (2021), *China's Digital Silk Road and Africa's Technological Future*, Council on Foreign Relations, p. 4

[91] Arcesati R. (2021), "China's Evolving Role in Africa's Digitalisation: From Building Infrastructure to Shaping Ecosystems", *ISPI*, https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247

[92] Agbebi M. (2021), *China's Digital Silk Road and Africa's Technological Future*, Council on Foreign Relations, p. 3

imposition of this dominance was the Covid-19 pandemic, which gave Chinese companies the opportunity to enter even more clearly in sectors such as e-health and more generally in the digitalization of public services. According to data compiled by the Center for Strategic and International Studies, Huawei alone already has 23 deals for e-government and cloud services in Africa. Even Senegal has recently decided to migrate its government data to a national data center which will be built by Huawei with a Chinese government loan. The pandemic even boosted cross-border e-commerce and, also in this case, Chinese companies, backed by Chinese government, took the opportunity to improve its digital footprint on the continent. An example is the Alibaba's electronic World Trade Platform (eWTP), with regional hub in Ethiopia, which is a useful asset in promoting Africa's exports to China. Finally, Beijing has acquired a leading role in mediating both African online communications (with the social media app "Vskit" from the joint venture between Chinese companies which counts over 10 million users in Africa), and transactions, a sector in which Chinese companies are increasingly present through local partnerships that allow them to bring their digital payment services.[93] This dominance in the African digital ecosystem poses two important strategic risks for the West. On one hand, China's dominant involvement in Africa's telecommunications landscape has raised concerns that the importation of its technology into the continent could lead to African countries' adopting Chinese internet and technology governance norms, on the other, this dominance has also important information security implications. The clear ties of many Chinese companies to the Chinese government have been a source of concern, especially in the US, where the government has repeatedly claimed that Huawei is an extension of the Chinese Communist Party and can use its equipment to collect intelligence, steal intellectual property, and monitor critics on behalf of the Chinese government. African countries, however, are not particularly concerned of these risks because of their pragmatic approach, placing access to infrastructure above security risks. They continue to partner with Chinese firms such as Huawei on ICT development projects as demonstrated by the deal between the Ivorian government and Huawei for the design of the Ivorian national digital economy strategy.[94]

[93] Arcesati R. (2021), "China's Evolving Role in Africa's Digitalisation: From Building Infrastructure to Shaping Ecosystems", *ISPI*, https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247

[94] Agbebi M. (2021), *China's Digital Silk Road and Africa's Technological Future*, Council on Foreign Relations, pp. 7-10

## 2.2 Russia and the Information warfare

***Moscow's renewed assertiveness in the region***

The other global player that has increased its footprint in the Wider Mediterranean in the last decade is Russia, which, compared to Beijing, shows a more assertive posture as evidenced by the presence with naval forces in the Mediterranean and by the interventions in Syria, Libya, Central African Republic, and Mali by its own military forces or connected to them, such as the Wagner company. This activism is the "*product of enduring national security requirements, threat perceptions, and economic interests*"[95] shaped by geography and historical legacy. Indeed, Russia's presence in the region after 2014 shows a great deal of continuity with Soviet and pre-Soviet times and is linked to the age-old Russian need to ensure a presence and an outlet on the warm seas of the Black Sea and the Mediterranean. Furthermore, especially considering the fear of an expansion of the Atlantic Alliance demonstrated in the decision to invade Ukraine in February 2022, it is probable that "*the principal rationale for Russia's return to the region has been the prospect of a military confrontation in the European theatre and concerns about the vulnerability of its southern flank in a conflict with NATO*".[96] This was also the rationale behind the Russian intervention in Syria in support of the Assad regime in 2015. Indeed, the defense of its only remaining ally in the Mediterranean has allowed Moscow to re-establish a significant military presence in this region with the Tartus naval facility and Hmeimim air base, both of which are undergoing major expansion in order to accommodate a greater naval and air presence. The support for Haftar and his LNA in the Libyan civil war also fits into this logic, providing the possibility of guaranteeing a privileged relationship at low costs with a country strategically situated in the middle of the Mediterranean's southern coastline, right on the southern borders of NATO. It is possible to consider in this perspective even the interventions in the Sahel aiming to counteract the operations of Western countries in a very delicate area, considered the southern border of Europe from which some major threats originate, such as jihadist terrorism and illegal migration, and so a possible strategic leverage against European rivals.[97]

This more strictly geostrategic vision can be integrated with another narrative often used to explain the renewed Russian interest in the region: the aspirations of global power and the consequent competition with the US and more generally with the West. According to this logic, "*Russia's great-power strategy in the Middle East and elsewhere is still influenced by the Soviet way of thinking,*

[95] Rumer E. & Sokolsky R. (2021), *Russia in the Mediterranean: Here to Stay*, Carnegie Endowment for International Peace, p. 3
[96] *Ivi*, p. 8
[97] Italian Parliament (2022), Relazione Annuale COPASIR 2021-2022

*which portrays the world in a simplistic yet detrimental dichotomy of Russia versus "the West".*"[98] Especially since the international isolation initiated by the 2014 annexation of Crimea, the increased Russian presence in the Middle East and in some parts of Africa can be seen as a way to balance Western influence, extend the geostrategic playing field and advance Putin's vision of a post-liberal international world order. Given a long history of colonization and multiple recent political mistakes by the U.S., the region provides a fertile ground for Russia to promote its dominant foreign policy narrative that demonizes the West. Rather than offering an alternative model, as does Chinese authoritarianism, the Russian strategy appears to be aimed at smearing the perception that democracy offers a more effective, equitable, transparent, or inclusive form of governance. In this, undermining of legitimate governments, fomenting social polarization, and propping up unconstitutional claims are all functional tools for Moscow's strategy. In this framework, Russia has increasingly resorted to the use of mercenaries, in order to reduce political costs and not imply a direct Russian involvement. Mercenaries from the Wagner Group (closely tied to Russia's military intelligence agency, GRU) have been deployed in Libya, CAR, Sudan, and Mozambique and "*in each case, following the Syrian model, the Russians supported a beleaguered leader facing a security challenge in a geographically strategic country with mineral or hydrocarbon assets*".[99] Russia has officially denied a role or even the presence of Russian mercenaries in these contexts, but, this remains a useful strategy for Moscow to gain greater influence in a region where it had little previous presence.

***Russian Information warfare***

Alongside the use of proxies, the other tool on which Moscow bases its hybrid war strategy towards the region are disinformation campaigns within the information warfare framework. On one hand, information warfare reflects enduring principles of the Russian approach to competition between states, on the other, it is an evolution of Russian strategy as part of Moscow's recent preparations for conflict in conditions of overall conventional inferiority. As described by President Vladimir Putin, "*We must take into account the plans and directions of development of the armed forces of other countries… Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive*." [100] The peculiarity of the Russian approach lies in the concept of information warfare itself. As stated in a glossary of key information security terms produced by the Military Academy of

[98] Janadze E. (2021), "Russia and the digital Middle East: An old game made new?", *Middle East Institute*, https://www.mei.edu/publications/russia-and-digital-middle-east-old-game-made-new

[99] Siegle J. (2021), "Russia and Africa: Expanding Influence and Instability", in Graeme P. Herd, ed., *Russia's Global Reach: a Security and Statecraft Assessment*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies

[100] Giles K. (2016), *Handbook of Russian Information Warfare*, NATO Defense College, Rome, p. 3

the General Staff, the Russian concept for "Information war" (*informatsionnaya voyna*), being all-encompassing and not limited to wartime, differs from the Western one, which, on the contrary, refers to limited, tactical information operations carried out during hostilities. The Russian channels and methods cover a "*broad range, including computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops by concerned citizens, YouTube videos, or direct approaches to individual human targets*".[101] The same variety also extends to the targets Moscow seeks through information warfare, all of which originate from previously tried and tested Soviet tactics: creating a "permissive environment" that allows Moscow to disseminate its message; obtaining a "reflexive control" where the enemy is driven to make favourable decisions to Moscow; pushing towards subversion and destabilisation, which weaken both governments and military authorities and benefit Moscow in accordance with its zero sum game rationale.[102]

The digital dimension fits perfectly to this Russian approach in the relationship between information warfare and the traditional state of war, because it allows the erosion of the distinction between war and peace and the emergence of a grey zone, as noted in the presentation by Chief of General Staff Valeriy Gerasimov widely referred to in the West as the "Gerasimov doctrine". In synthesis, as underlined by Antonovich, "*dividing lines between war and peace can be eroded conveniently in cyberspace. Damage (whatever its nature) can actually be done to an adversary without overstepping formally the line between war and peace*."[103] Therefore, the digital dimension clearly forms a substantial part of the new Moscow's approach, even if it does not constitute an element on its own but is always placed side by side with the other tools that are part of the information strategy. The current approach is indeed the culmination of an evolutionary process, seeking to revive well-established Soviet techniques of subversion and destabilisation and update them for the internet age.[104] Since the 1990s, Russian military realized that "*one can penetrate a state's information networks in the simplest way through Internet channels in addition to the traditional channels of radio, television and the mass media*" and this implied that mass audiences could be reached with much greater impact, and much less expense and effort, than previous techniques of planting and disseminating disinformation.[105] Nowadays, much of the Russian information warfare is applied by relying on a combination of traditional and social media. In this framework, information campaigns

[101] Giles K. (2016), *Handbook of Russian Information Warfare*, NATO Defense College, Rome, p. 4
[102] *Ivi*, pp. 16-30
[103] Antonovich P. (2011), "Cyberwarfare: Nature and Content", in *Military Thought*, No. 3, Vol. 20, pp. 35-43.
[104] Giles K. (2016), *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, p. 4
[105] Giles K. (2016), *Handbook of Russian Information Warfare*, NATO Defense College, Rome, p. 34

via the mass media, usually developed through RT (formerly Russia Today) and Sputnik, "*are only part of a broad multilingual front, including not only state-backed media and trolling, but also fake media – sock puppet websites set up to resemble genuine news outlets, but seeding their news feeds with false or contentious reporting that ties in with Russian narratives*."

***From Syria to Ukraine war: Russian disinformation in the Middle East***

A strategy of this kind has been used in the Middle East since the Russian intervention in Syria in 2015. In this sense, the examples of the TV channels Rossiya 24 and, more importantly, Russia Today (via its Arabic version Rusia Al-Yaum) in suggesting an "alternative" vision to the Syrian conflict, are clear example of the strategy to shape a Russian perspective on international politics and countering the dominant narratives of Western media in the region. Russia pushed the idea that in Syria the only two options were Bashar al-Assad or the Jihadists, without any other possible alternative emanating from civil society. This narrative, endlessly hammered through RT and social media, has had major local consequences, since it effectively discredited the Syrian opposition, as well as reducing the complexities of the Syrian conflict to a binary choice between the Assad regime and a takeover by Salafist Jihadists. These information campaigns resulted in fading Western public support for Assad's departure at a time when refugees were fleeing massively to Europe.[106]

In addition to the specific Syrian context, the Russian disinformation has also achieved important results on the perception of Moscow in the Middle East. Arab perceptions of Russia's regional role have improved, as shown by the 2022 Arab Youth Survey, which demonstrates how young Arabs consider Moscow a better ally than US and the rest of the West. The perception of the population has not changed even following the Russian invasion of Ukraine but, rather, nearly a third of young Arabs believe the US and its NATO allies are more responsible for the war in Ukraine than Russia. This is mostly due to the new momentum of Moscow's disinformation campaign, which takes full advantage of the overreliance on social media platforms for news in MENA. Indeed, locals in countries with

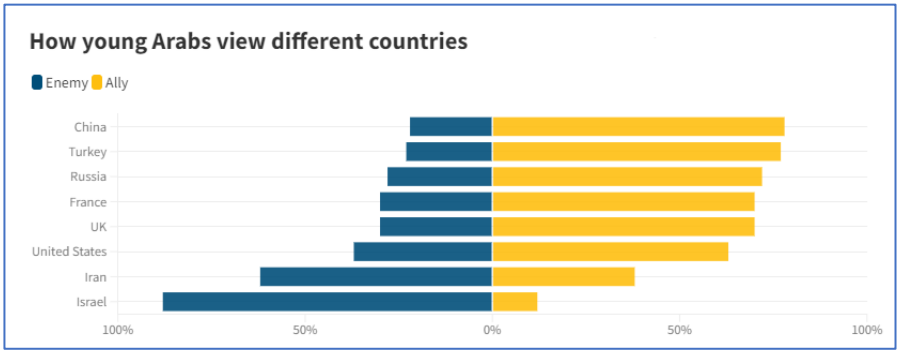


*Figure 14: Perception of different countries among Arab youth. Source: Arab Youth Source*

[106] Nocetti J. (2019), *Dazed And Confused: Russian "Information Warfare" And The Middle East – The Syria Lessons*, EuroMesc Policy Brief, n. 93

authoritarian governments do not often trust their own state-sponsored media and rely more on news reports shared via social media. In this context, the Middle Eastern cyberspace beckons the Kremlin to expand its informational outreach.[107] RT is now one of the five most popular broadcasters in the region, with 85 million of users, of which about ten earned since the start of the offensive in Ukraine.[108] The Russian-backed broadcast regularly performs better on social media than Arabic offerings from Western media outlets, as it posted twice or three times as much as Al Jazeera or the BBC. The daily post frequency of the RT Arabic and Sputnik Arabic has increased significantly on Twitter (by 35% and 80% respectively) since the start of the invasion.[109] As underlined by Ayad, in addition to these state-affiliated agencies is important to consider "*the impact of Facebook-only media outlets which are sharing, repurposing and rebranding RT and Sputnik content. These are entities that exist solely on social media platforms, are typically not accredited news agencies, but play a role in spreading pro-Kremlin content*." These sorts of supposedly non-affiliated users and outlets, stretching across all social media platforms, get twice as much attention as any official media.[110] An example are the numerous social media accounts with hundreds of thousands of followers that are run by the so-called "attractive Kremlinistas," Russian women who post pro-Russian stories in Arabic and spread pro-Moscow disinformation among male audiences across the region.[111]

### *Prigozhin's disinformation strategy in Africa*

The use of social media as a disinformation tool obviously also extends to the African continent, specifically in Libya, the Sahel and the Gulf of Guinea. Even in this case, one of the first strategy involves the use of online news websites, such as Sputnik and RT in several languages. These Kremlin-sponsored media are rising in popularity across the African continent, as evidenced by a significant increase in subscribers to the RT France Facebook page (from 50,000 to 850,000), the vast majority of which were from countries of the Maghreb and Sub-Saharan Africa. Both channels "*have succeeded in their aim to obtain the 'normalisation' and institutionalisation of their position as part of the media landscape of French-speaking Africa*" and African online news websites are relaying

[107] Janadze E. (2021), "Russia and the digital Middle East: An old game made new?", *Middle East Institute*, https://www.mei.edu/publications/russia-and-digital-middle-east-old-game-made-new
[108] Data from Institute for Strategic Dialogue (2022)
[109] Janadze E. (2021), "Russia and the digital Middle East: An old game made new?", *Middle East Institute*, https://www.mei.edu/publications/russia-and-digital-middle-east-old-game-made-new
[110] Hassan E. & Schaer C. (2022), "How Russia is winning the Mideast information war", *Deutsche Welle*, https://www.dw.com/en/russia-is-winning-the-information-war-in-the-middle-east/a-62900269
[111] Ayad M. (2022), "Propaganda Primping: The 'Kremlinistas' of Twitter", *Institute for Strategic Dialogue*, https://www.isdglobal.org/digital_dispatches/propaganda-primping-the-kremlinistas-of-twitter/

content from these media on a large scale.[112] A study by the NATO Strategic Communications Centre of Excellence analyzed 561 articles by RT France and Sputnik France about seven Western military missions in Mali (MINUSCA, EUTM RCA; MINUSMA, Barkhane, EUTM) over the five-year period 2015-2020. It identified some recurring narratives that aim to propose these missions as ineffective and to present negatively Western countries who participate. This is a continuation of mass communication narratives utilised in the Soviet era, which are considered to resonate with local populations due to the fact that Russia, unlike many Western nations, was never a colonial power in Africa. In particular, articles in the context of Barkhane often served as a platform for conspiracy theories and criticism against France[113] and this explains the celebrations with Russian flags among supporters of the August 2020 coup in Mali. Social media sites blamed the former colonial power, France, for Mali's militant Islamist insurgency in the north and called for France to pull out the 5,000 troops it had deployed to help combat the jihadists. These themes were subsequently picked up in protests organized by opposition groups in the months leading to the coup.[114]

The disinformation carried out by the official pro-Russia media is complemented by a network of social media pages and accounts. In 2019 the Stanford Internet Observatory identified a large network of Facebook Pages that were engaged in a broad, long-term influence operation targeting six countries: Libya, Sudan, the Central African Republic, Madagascar, Mozambique, and the Democratic Republic of the Congo. In total these 73 Pages posted more than 48,800 times, received more than 9.7 million interactions on these posts, and were liked by over 1.7 million accounts. Despite the fact that these pages were presented as authentic domestic voices, they were actually based outside of Africa and have been attributed by Facebook to Yevgeny Prigozhin, the Russian oligarch who funded the Internet Research Agency and is the Chief of the Wagner Group. These pages produced almost universally positive coverage of Russia's activities in these countries, disparaged Moscow's rivalries such as US, the EU but even Turkey and Qatar, and supported national actors linked to Russia, such as Khalifa Haftar's LNA in Libya or the Transitional Military Council protagonist of the 2019 coup in Sudan. [115]

[112] Limonier, K. (2019). *The Dissemination of Russian-Sourced News in Africa*, Institut de Recherche Stratégique de l'École Militaire, Research Paper No. 66, p. 19

[113] Hanley M., VanSant K., Pildegovičs T. (2021), *Russia's Activities In Africa's Information Environment Case Studies: Mali and Central African Republic*, NATO Strategic Communications Centre of Excellence

[114] Siegle J. (2021), "Russia and Africa: Expanding Influence and Instability", in Graeme P. Herd, ed., *Russia's Global Reach: a Security and Statecraft Assessment*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies

[115] Bush D., DiResta R., Grossman S. (2019), *Evidence of Russia-Linked Influence Operations in Africa*, Stanford Internet Observatory

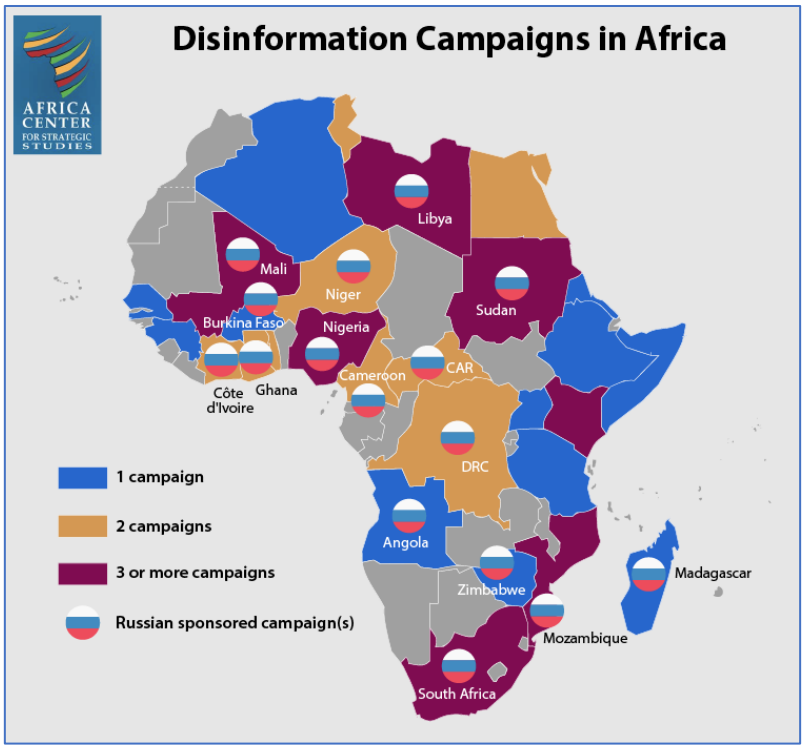


*Figure 15: Disinformation campaigns detected and publicly documented in Africa. Source: Africa Center for Strategic Studies*

Another recent strategy developed by Prigozhin in the African context is the "franchising" of the disinformation efforts by creating or sponsoring African hosts for the pro-Russian and anti-West messaging. With so many African journalists relying on small paid jobs, this approach is likely a highly effective recruitment method even because it creates more locally authentic content that resonates with users and makes it so much harder to detect these disinformation campaigns.[116] Furthermore, as underlined by Giles, "*once the disinformation placed there has been fed into the mainstream news flow at one or more points, and is picked up and reported by reputable traditional media whose editors and reporters are not aware that it is spurious, others will follow: even in the new climate of awareness, major news media do not wish to be left behind on a story which has made it to the news agenda.*"[117]

[116] Siegle J. (2021), "Russia and Africa: Expanding Influence and Instability", in Graeme P. Herd, ed., *Russia's Global Reach: a Security and Statecraft Assessment*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies

[117] Giles K. (2016), *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, p. 8

### *A future development: interference on internet undersea cables*

Many analysts then underlined the probability of an evolution of Russian information warfare techniques and one of the most probable developments seems related to the sabotage and acquisition of information from Internet infrastructures, in particular from submarine cables. In the last decade there have been several sightings of Russian investigation of subsea communications cables, for example in American waters and in the Baltic Sea.[118] NATO officials spoke openly of a sustained pattern of Russian submarines and vessels "aggressively operating" near cables, highlighting that the vital lines of communication are vulnerable to attack by Russian naval forces.[119] The technologies for accessing data from subsea cables are well established[120] and, according to former SACEUR Jim Stavridis, targeting them would meet a wide range of Russian objectives as "*a rich trove of intelligence, a potential major disruption to an enemy's economy and a symbolic chest thump for the Russian Navy*."[121] Russia has both experience and an interest in using this type of tactics, such as disrupting communications networks, as demonstrated during the Crimea annexation when Moscow severed the main terrestrial cable connection to the outside world to gain control of the peninsula's internet infrastructure and hence the flow of information. This enabled the Kremlin to spread disinformation and promote its actions as legitimate.[122] Another indicative factor is the large investments in submarines within the modernization of the Russian Navy. Russia's auxiliary submarines, often referred to as deep sea underwater stations, are considered a particular threat as equipped to be able to manipulate objects on the seafloor and may also carry sensitive communications intercept equipment in order to tap into undersea cables or otherwise destroy or exploit sea floor infrastructure. Even a class of Russian surface vessel, the Yantar-class intelligence ship, is notable for its capability to interfere with cables through the deployment of submersible craft.[123] All these indicators suggest possible Russian interference on the submarine cables of the Wider Mediterranean, crucial for the connection of the regional countries but also for Europe. For instance, since 2015 the Kremlin's 'Yantar' spy ship was tracked loitering near undersea cables off the coasts of Cyprus, Israel, Syria and Iran and the ship's activities have, in some cases, coincided

[118] Giles K. (2016), *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, p. 11
[119] Sunak R. (2017), *Undersea Cables: Indispensable, insecure*, Policy Exchange, Westminster, London
[120] Khazan O. (2013), "The Creepy, Long-Standing Practice of Undersea Cable Tapping", *The Atlantic*, https://www.theatlantic.com/international/archive/20
[121] Stavridis J. (2015), "A New Cold War Deep Under the Sea?", *Huffington Post*, https://www.huffpost.com/entry/new-cold-war-under-the-sea_b_8402020
[122] Bueger C., Liebetrau T., Franken J. (2022), *Security threats to undersea communications cables and infrastructure – consequences for the EU*, Directorate General for External Policies of the Union, Policy Department for External Relations, p. 32
[123] Sunak R. (2017), *Undersea Cables: Indispensable, insecure*, Policy Exchange, Westminster, London

with temporary connectivity disruptions in the neighbouring countries, causing concern in security and defence policymakers.[124]

## 2.3 Turkey and the "Drone diplomacy"

***A regional power with the same theatre of strategic interest as Italy***

Turkey is another one of the main players in the geopolitical dynamics of the Wider Mediterranean, especially considering that the Turkish theatre of priority interest often coincides with the Italian one.[125] Since the rise to power of Erdogan's Justice and Development Party (AKP) in 2002 Ankara has developed an aggressive foreign policy in the macro-region, which draws its theoretical inspiration from the essay "Strategic Depth", written by Ahmet Davutoglu in 2001. This doctrine proposed a dynamic reinterpretation of Turkish geopolitics so as to increase the country's global influence especially on the former Ottoman territories (Neo-Ottomanism), by exploiting the country's geostrategic position and its role as a model for the democratization of Muslim majority societies.

The Mediterranean is one of the areas in which this policy is implemented and there have been various aggressive initiatives that have resulted in diplomatic controversies or international clashes. After an initial phase where these power aspirations were pursued above all with the use of soft power, since 2015 Turkey adopted a more hard power-based approach which led to military interventions in various contexts, such as the "Operation Peace Spring" in Syria and "Peace Storm" in Libya. This assertiveness, justified with humanitarian aims, has been accompanied by a very aggressive posture also in the waters of the eastern Mediterranean, where Turkey is trying not to be isolated in the management of gas resources discovered in the area and, therefore, questions the international maritime borders with Greece and Cyprus.[126] Turkish assertiveness in the Mediterranean has allowed Ankara to bring under control the main migration routes - from Libyan to Balkan ones - as well as the main energy routes that supply Italy and Europe from the south, with particular reference to the TAP gas pipeline passing through Turkish territory.[127]

Turkish ambitions are not limited to the Mediterranean basin but also concern Africa, where in recent years there has been a geographical enlargement of Turkey's areas of strategic interest. In 2005, the

[124] Koka A. (2022), "The Gulf Submarine Network amid Sabotage and Mine Warfare Threats", *The Euro-Gulf Information Centre*, https://www.egic.info/gulf-submarine-network-amid-sabotage-mine-warfare
[125] Italian Parliament (2022), Relazione Annuale COPASIR 2021-2022
[126] Nocera L. (2021), "Perspectives on the New Centrality of the Mediterranean States: The Role of Turkey in a Changing Region" in F. M. Corrao and R. Redaelli (eds.), *States, Actors and Geopolitical Drivers in the Mediterranean*, Palgrave MacMillan
[127] Italian Parliament (2022), Relazione Annuale COPASIR 2021-2022

Turkish government proclaimed the Year of Africa and, since then, Turkey has employed various tools to consolidate diplomatic and economic relations with African countries. Until 2019, the Turkish focus within the continent was on the Horn of Africa, where Turkey was competing with Middle Eastern powers. In particular, the relationship with Somalia is very close, given that for years Turkey has launched various humanitarian initiatives in the country and it trains about a third of the troops of the Somali National Army (SNA). A relationship that is testified even by the Turkish military base in the port of Mogadishu, on the Red Sea. In recent years, however, external factors, such as the retrenchment of France's military commitment in Mali, have opened a window of opportunity westward and Ankara aims to strengthen its presence even in the Sahel and the Gulf of Guinea, creating a "Turkish Arc" of influence over sub-Saharan Africa, which practically coincides with the areas of Italian national interest.[128]

***Drones as a powerful foreign policy asset***

The sector that has most contributed to the expansion of Turkish influence in the Wider Mediterranean is the defense and security one, especially from 2020 onwards. This is due to both opportunity and political factors: on one hand, there is the growing demand and diversification of the African arms market, which have created opportunities for Turkey and other emerging producers; on the other, Turkey intends to capitalize on investments made over the last fifteen years in the defence industry. In particular, drones have given Turkey's defence sector a definitive boost by opening up the global market to Turkish products. Indeed, most of the recent interest shown by African states in Turkish defence industry items is geared toward Turkish-made UAVs.[129] Turkish drones are cheap as well as effective. A Bayraktar TB2 drone costs roughly $5m – compared to $20m for an American-built MQ-9 Reaper and $28m for a more advanced US-made Protector RG Mk 1. However, unlike other low-cost models, such as China's Wing Loong, Turkey's drones provide most of the capabilities of Western ones at a fraction of the price. As TB2 proved game-changing in the conflicts in Libya and Nagorno-Karabakh and have shown combat efficiency in Syria, Ankara has gained a prominent role in a sector previously dominated by the United States, Israel, and China.[130] Via unmanned aerial-combat systems transactions, the Turkish administration have built strategic bonds with other countries, pursuing an effective "drone diplomacy". Indeed, often the export does not only concern the sale of the drone itself, but leads to lucrative, long-term partnerships built on the provision of spare parts, munitions, training, and other technical assistance, as in the case of the burgeoning

[128] Donelli F. (2022), *UAVs and beyond: Security and defence sector at the core of Turkey's strategy in Africa*, Megatrends Afrika, Policy Brief, n. 2, p. 6
[129] *Ivi*, p. 4
[130] Borsari F. (2022), *Turkey's drone diplomacy: Lessons for Europe*, European Council on Foreign Relations, p. 2

military partnership between Turkey and Ukraine, in which Turkey buys Ukrainian engines and the two states closely cooperate on research and development.[131] Geopolitically, Turkey has demonstrated how these drones can be a powerful foreign policy asset. This technology has helped the country to coerce its geopolitical rivals, conducting military operations where it once may have been too costly and dangerous to do so, but even to escape years of regional isolation, strengthening its existing partnerships and creating new ones.[132]

### *"Drone Diplomacy" in Africa*

Drones have become a precious bargaining chip in economic and political negotiations with African counterparts. The first and most exemplary case was in Libya, where, in April 2020, forces loyal to the Government of National Accord used Turkish-made Bayraktar TB2 drones to halt Field Marshal Khalifa Haftar's assault on Tripoli. In the following years, the export of drones has been a constant help in establishing privileged relationships with the countries of the Wider Mediterranean. In the Maghreb for example, in addition to Libya, even Morocco and Tunisia have bought Turkish UAVs and Algeria seems to want to follow suit. In the Horn of Africa TB2s were sold to Ethiopia, where they were used by the federal government of Addis Ababa in the conflict with the federal state authorities of Tigray. In exchange, and in addition to the economic gain from the sale, Turkey obtained the closure of ten schools affiliated with the U.S.-based Muslim cleric Fetullah Gülen, who is accused of orchestrating the 2016 coup against Erdogan. The sale of UAVs was certainly an incentive also for the strengthening of relations with Niger, considered as the gateway to expanding Turkish influence on the Sahel region, where Ankara plans to get a military outpost and increase its role as special forces training in counterterrorism and counterinsurgency. After a few years of stalemate, Turkey is likely to ask Niger to use the former French military base Madama, near the Libyan border, in order to establish a training camp on the model of Camp TURKSOM in Somalia. As demonstrated by the exports in Nigeria and Angola, drones have also increased Turkey's bargaining power in the Gulf of Guinea, which is an area particularly strategic for its import of hydrocarbons.[133]

[131] Kasapoglu C. (2022), *Techno-Geopolitics and the Turkish Way of Drone Warfare*, Atlantic Council, Issue Brief, p. 6
[132] Borsari F. (2022), *Turkey's drone diplomacy: Lessons for Europe*, European Council on Foreign Relations, p. 4
[133] Donelli F. (2022), *UAVs and beyond: Security and defence sector at the core of Turkey's strategy in Africa*, Megatrends Afrika, Policy Brief, n. 2, p. 6

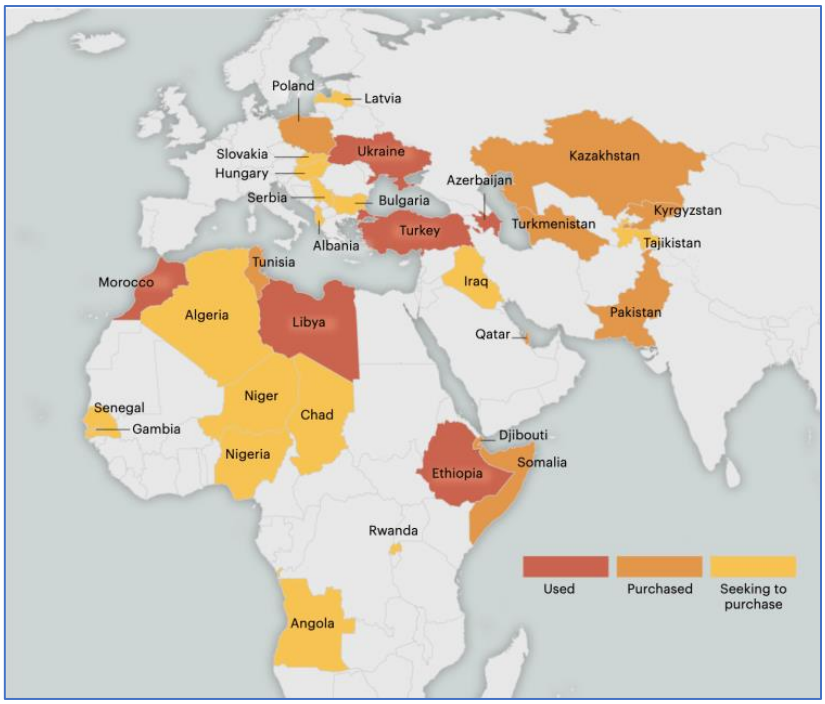


*Figure 16: countries which have bought or are interested in buying Turkish drones. Source: AsiaTimes*

***The invisible power behind drones success: KORAL as another foreign policy asset?***

In the Turkish unconventional drone doctrine, that prescribes the use of drones as an air force in a conventional battle, Ankara incorporated even the use of an Electronic Warfare System (EWS) against communication and radar systems. Turkey, indeed, has understood the increasing dependence in modern warfare on radars, radio signals and satellites to command, control and coordinate the movement of or communicate with military assets. Turkish investments in the electronic warfare sector, which began in the 70s, led to the production of various systems and platforms, among which the KORAL occupies a unique position and has played a critical role in Ankara's recent involvements in several regional theatres. The KORAL is a land-based transportable EWS, with an effective range of 150–200 km, which offers advanced options and supports Suppression of Enemy Air Defences (SEAD) operations. It consists of two subsystems: the first provides electronic support operations for conducting ISR (Intelligence, Surveillance and Reconnaissance), while the other is dedicated to attack operations to degrade, neutralise or destroy enemy combat capabilities. This system has enabled Turkey's strategic and military planners to boost the efficiency and lethality of its UACVs and is considered "*the invisible power behind their success*", as demonstrated in Syria, Libya and Azerbaijan.[134] The efficiency of the KORAL has highlighted the need to invest in the electronic

[134] Bakir A. (2021), "Turkey's Electronic Warfare Capabilities: The Invisible Power Behind its UACVs", *RUSI*, Turkey's Electronic Warfare Capabilities: The Invisible Power Behind its UACVs | Royal United Services Institute (rusi.org)

warfare sector within many national armies. This has also turned into a growing demand for the purchase of KORAL, especially in the Wider Mediterranean area. Ankara has already signed an agreement for the export of the system to Morocco, while Oman and Iraq have expressed interest in purchasing. Therefore, electronic warfare systems could constitute another instrument of influence in the region in the future, related and complementary to Turkish drone diplomacy.

## 2.4 Iran as a regional cyber power

***Iranian expansionism as a factor of instability***

Finally, another key player for the dynamics of stability in the Wider Mediterranean, even if more focused on the Levant, is Iran. Concern for Iranian foreign policy is not limited to its nuclear ambitions and the future of the JCPOA, but even to its proxy forces and alliances with violent groups across the Middle East. Since the Iranian revolution of 1979, when the Shah was overthrown and Ayatollah Khomeini returned to the country, the Iranian regime has sought to embed its influence across the region. Regional instability and weak states have allowed Iran to develop alliances with Hezbollah in Lebanon, militia groups in Iraq and the Houthi group in Yemen. Teheran has also supported President Assad in Syria, with the two countries being long-standing allies.[135] These policies are particularly destabilizing for the region, even considering the tensions with the two historical rivals of Saudi Arabia and Israel and the strengthening of the axis with Moscow and Beijing, as evidenced by the joint naval actions in the Indian Ocean.[136]

Furthermore, the new Raisi presidency and the current increasingly multipolar international system could lead to an expansion of the Iranian foreign policy theatre towards the other regions of the Wider Mediterranean, in particular North Africa. Indeed, while Iran has long been a major Middle Eastern power, under the Islamic Republic it has more recently been known as part of the so-called "axis of resistance" as a counterbalancing strategy against the structure of international relations, which Teheran consider as built and imposed by the US. For this reason, Iran's foreign policy orientation provides a focus on "Third Worldism", aimed at expanding Iran's influence in the "Global South" and boosting Iranian overall deterrence capability against the "threat of regime change" posed by the West. In this context, the Raisi presidency will intensify efforts to pivot to non-Western countries and, as demonstrated by recent diplomatic and economic initiatives, Africa is likely to be an

[135] Loft P. (2022), *Iran's influence in the Middle East*, House of Commons Library, Research Briefing
[136] Italian Parliament (2022), Relazione Annuale COPASIR 2021-2022

increasingly important part of this effort. Iranian officials believe Africa is an opportunity for Tehran to reject the dominant world order, which the Islamic Republic recognizes as a threat to its identity and discourse.[137]

### *Iranian offensive cyber operations*

Many of the Iranian actions causing instability in the Middle East are related to the cyber domain. Teheran has shown remarkable progress on the issues of cybersecurity and operational cyber capabilities, after strengthening its national cyberinfrastructure following the 2010 Stuxnet attack, which targeted Iran's uranium enrichment centrifuges in Natanz nuclear facilities. Since then, Tehran has constantly developed defensive, but above all offensive, cyber capabilities.[138] Indeed, cyber warfare is seen as a tool that could help the country to fill the gap with the superior conventional military capabilities of its rival countries (U.S., Israel, Saudi Arabia), along with other classical asymmetrical strategy such as terrorism and guerrilla warfare. Iran, especially the Iranian Revolutionary Guards Corps (IRGC), believes that enhancing its cyberwarfare capabilities could have, at least partial deterrence against its enemies. For this reason, Iran recur to all its cyberwarfare capabilities against enemy countries in cases of serious diplomatic or military escalation, with the hope do deter its enemy from further attacks.[139] For this reason, as underlined by Cohen, "*Iranian offensive cyber activity is intricately linked and constantly adapting to the country's geopolitical interests at any given time*".[140] A link clearly shown in the attack and espionage operations against Israel, sometimes in cooperation with regional geopolitical allies Hamas and Hezbollah hacking groups. These campaigns tend to occur during periods of security activity in the region, such as Israeli incursions into Gaza or Lebanon. Another example is related to the JCPOA agreements, with the number of cyberattacks to regional and western rivals clearly linked to the progress of the negotiations.[141] Even the 2012 Shamoon attack on Saudi Aramco is connected with specific economic motivations that might push Iran to target the Saudi energy industry. The attack occurred at a time when strong sanctions against Iran were causing great damage to the country's oil industry, and Saudi Arabia was acquiring many shares of the oil market previously belonging to Iran.[142] Iranian cyber

[137] Naeni A. (2021), "Iran and Africa: Why Tehran will boost its ties with the continent under the Raisi administration", *Middle East Institute*, https://www.mei.edu/publications/iran-and-africa-why-tehran-will-boost-its-ties-continent-under-raisi-administration

[138] Çahmutoğlu E. (2021), *Iran's Cyber Power*, Center for Iranian Studies in Ankara (İRAM)

[139] Spadoni G. (2019), IRGC Cyber-Warfare Capabilities, *International Institute for Counterterrorism,* p. 5

[140] Cohen S. (2019), "*Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests*", Cyber, Intelligence, and Security, Vol. 3, No. 1

[141] *Ibidem*

[142] Bronk C. & Tikk-Ringas E. (2013), "The Cyber Attack on Saudi Aramco", *Survival: Global Politics and Strategy*, Vol. 55, no. 2, p.89

operations have recently shifted even more westward, as evidenced by the attack on Albania in September 2022, following the relocation in the Balkan country of the exiled Iranian opposition group MEK.[143]

Iran's cyber threat also extends to the maritime sphere, as evidenced by a series of alleged Iranian cyber-attacks to shipping vessels. In January 2016, researchers attributed GPS spoofing, an attack that attempts to manipulate a GPS receiver by broadcasting counterfeit signals, to the Iranian capture of two United States riverine patrol boats which unknowingly sailed into Iranian waters and were accused of violating Iran's territorial integrity. That case showed as cyber-attacks on shipping could be a way for Iran to exercise power and control over the Strait of Hormuz, a chokepoint of economic importance for global oil markets and the West, while also showing resistance to Western-imposed sanctions.[144] In 2021, indeed, classified documents, allegedly from an offensive cyber unit called Shahid Kaveh, part of Iran's elite Islamic Revolutionary Guard Corps' (IRGC) cyber command, reveal secret research into how a cyber-attack could be used to sink a cargo ship or blow up a fuel pump at a petrol station. The papers appear to reveal a particular interest in researching companies and activities in western countries, including the UK, France and the United States.[145] This Iranian maritime cyber threat could become particularly salient in the dynamics of the Wider Mediterranean especially considering the recent Iranian military maritime activity in the Red Sea, which, according to the former Israeli Minister of Defence Benny Gantz, is the "most significant" in a decade and "*also a direct threat to peace and stability in the maritime arena, which may affect the Mediterranean and beyond*."[146]

**Iranian Digital Influence Efforts: propaganda operations in the cyberspace**

However, offensive cyber operations are not the only way Iran has adapted its foreign policy to digital transformation, but they are complemented by a strong attention on the informational side of social media. Information dominance represents a central focus of both foreign and domestic policy as Iran sees itself as engaged in a perennial information war: against Sunni Arab powers, against the forces of perceived Western neo-colonialism, and particularly against the United States. Should the

[143] Zaimi G. (2022), "Iran's Balkan front: The roots and consequences of Iranian cyberattacks against Albania", *Middle East Institute*, https://www.mei.edu/publications/irans-balkan-front-roots-and-consequences-iranian-cyberattacks-against-albania

[144] Gray I.W. (2016), "Cyber Threats to Navy and Merchant Shipping in the Persian Gulf", *The Diplomat*, https://thediplomat.com/2016/05/cyber-threats-to-navy-and-merchant-shipping-in-the-persian-gulf/

[145] Haynes D. (2021), "Iran's Secret Cyber Files", *Sky News*, https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871

[146] Fabian E. (2022), Gantz: Iran's maritime activity in Red Sea is 'most significant' in a decade, Times of Israel, https://www.timesofisrael.com/gantz-irans-maritime-activity-in-red-sea-is-most-significant-in-a-decade/

information conflict be lost, many Iranian officials believe the collapse of the state will soon follow.[147] Having well understood the information potential of the new digital platforms, Iran on the one hand has curtailed Internet freedom for its own citizens, fearing the foreign "soft war" aimed at creating elements of subversion and discord among the public opinion, on the other, has greatly expanded its use of social media platforms for diplomacy and propaganda abroad.[148]

Iran has built a prolific online influence apparatus but its approach differs from the disinformation campaigns of Russia. Whereas Moscow's ongoing disinformation campaigns are intended to obfuscate truth and discredit Western institutions, Iran's efforts exemplify the art of indirect "Persian persuasion" and deflection, seeking to elevate itself as an alternate leader of the Muslim world and as a bulwark against the perceived forces of neo-colonialism and US interventionism. While Russia uses fake news, Tehran spreads a distorted and partial truth functional to proposing a positive image of the country. In this sense, Iran's digital influence operations represent a continuation of public diplomacy, albeit conducted through misleading websites and social media sockpuppets. Teheran invests significant energy injecting pro-Iranian content into the information environments of countries that offer little direct strategic utility. An example is the proliferation of various pro-Iranian Facebook pages in Nigeria, which has the largest Muslim population in Africa and which includes a restive Shia minority, but the main focus is obviously the Iranian regional context, the MENA.[149] Arabic was the most used language in the Iranian information operations, followed by English and Persian. The propaganda tactics to influence MENA users are various and range from directing Arab users to Pro-Iran third-party websites and social media pages to imitate website names, as in the case of the famous Egyptian TV channel Nile TV.[150]

In addition to propaganda and the dissemination of pro-Iranian content, Teheran turns this apparatus against the United States and its allies to achieve definable foreign policy objectives. In 2014, for example, Iran helped amplify a Lebanese conspiracy theory that the United States had created the self-declared Islamic State of Iraq and al-Sham (ISIS). The clear objective was to blunt US soft-power efforts in Lebanon and to strengthen the relative position of the Iranian-backed Hezbollah, which was engaged in its own propaganda battle. Iran exhibits similar behaviour in its routine amplification of Palestinian civilian deaths at the hands of the Israeli Defense Forces, the killing of Yemeni civilians by the Saudi-led coalition, or its focus on the toll of US air strikes in Iraq and Syria. Each is intended

[147] Brooking E. T. & Kianpour S. (2020), *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, Atlantic Council, p. 8
[148] *Ivi*, p. 10
[149] *Ivi*, p. 19
[150] Elswah M. & Alimardani M. (2021), "Propaganda Chimera: Unpacking the Iranian Perception Information Operations in the Arab World", *Open Information Science*, vol. 5, p. 167

to diminish the image of US-aligned powers, while masking Iran's role in these and other proxy conflicts. More broadly, it is no coincidence that Iranian-attributed Twitter activity saw its most significant spikes in mid-2015 and mid2018. The first spike aligned with the contentious US domestic debate regarding adoption of the JCPOA, which set limits on Iranian nuclear development; the second aligned with the unilateral US withdrawal from that same agreement. For Iran, this digital influence apparatus represents a natural and potent tool to achieve its geopolitical ends.[151]

## 2.5 Digital technologies in the competitors' strategies

This chapter has analyzed the policies of the four major Italian competitors in the Wider Mediterranean, starting from the traditional foreign policy tools and seeing if and how these relate to the digital environment. The analysis showed that all four cases taken into consideration (China, Russia, Turkey and Iran), albeit in very different ways and with very different means, particularly consider the digital tool as a useful foreign policy asset in dealing with the macro-region.

For China, the Wider Mediterranean region is highly strategic in geographical terms as it is a crucial passage to connect China to Europe. The strategic importance of the area is demonstrated by the great focus dedicated to it within the BRI global investment project, in particular as regards investments in transport such as ports or railways. However, these investments are closely linked to the digital environment, which, in fact, constitutes one of the three main drivers of the Belt and Road Initiative. The Digital Silk Road aims to digitally connect China to the rest of the world and to make China a leader in the sector. Beijing has therefore heavily invested in the digital ecosystem of the Wider Mediterranean, both in the MENA region and in the sub-Saharan appendages. In particular, the African digital ecosystem is almost totally dependent on China, which has been investing in the sector since long before the DSR. These digital investments in the macro-region allow Beijing to achieve important strategic advantages. First, they allow China to acquire global power and international weight in the context of competition with the US. The digital dependence of the countries of the region on China could in fact be a leverage to be used to acquire consensus on Chinese policies and objectives in the international arena, in particular in deciding the international technical standards for new technologies. Second, the huge Chinese presence in the area's digital ecosystem gives China a great informational advantage, giving it access to a large variety of data. Information superiority is considered by Chinese leaders to be a crucial objective for the nation and this is also closely linked to Chinese military modernization.

[151] Brooking E. T. & Kianpour S. (2020), *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, Atlantic Council

Since 2015, Russia has shown a renewed interest in the region, which has distant historical and geographical origins. For centuries, due to geostrategic reasons, Russia has had the need to obtain an outlet towards the warm seas of the Black Sea and the Mediterranean. The military intervention in Syria and the support for General Haftar in Libya go in this direction. In addition to the more strictly geopolitical reasons, there is also a rationale linked to global competition with the West, as for Moscow it is crucial to expand its international alliances to promote an alternative global order. To increase its influence in the Wider Mediterranean, Moscow mainly resorts to asymmetric tactics, such as the use of proxy troops as the Wagner group or information warfare. Within this framework, the digital environment provides an important opportunity especially considering the concept of Russian information warfare, which is not limited only to times of war. Cyberspace, indeed, allows the erosion of the distinction between war and peace and the emergence of a grey zone. Russian disinformation, therefore, resorts to a mix of traditional and new media to carry forward a pro-Moscow and anti-Western narrative. Generally, the disinformation campaigns launched by the major Russian mass media RT and Sputnik are amplified and integrated by a network of social pages and profiles. This is a pattern seen in the Middle East but especially in Africa, where a vast network of disinformation social pages linked to Russian oligarch Yevgeny Prigozhin has emerged over the years. These disinformation campaigns have had positive effects on Russia's image in the region, but have also helped Moscow achieve foreign policy goals, such as increasing support for Assad in the Middle East or growing anti-French sentiment in the Sahel, which then translated into the withdrawal of French troops from Mali. In addition to online disinformation campaigns, Russian information warfare in the future could probably expand to another field, which is the exploitation of internet infrastructures such as submarine cables, from which Moscow could obtain sensitive data and information.

In the last twenty years Turkey has had a renewal of its foreign policy, which began with the rise to power of Erdogan's AKP party and is in line with Davutoglu's "Strategic Depth" doctrine. In its policies of Neo Ottomanism, Ankara has identified the Wider Mediterranean as an area of strategic interest, inevitably positioning itself as one of Italy’s main competitors. In particular, Turkish expansionism has turned towards Africa by exploiting the attractiveness of its defense and security sector. In this area, Ankara has managed, through the export of its means of automated warfare, to build increasingly solid partnerships on the continent. In particular, two products of the Turkish defense industry have proved to be particularly useful: the Bayraktar TB2 drone, increasingly requested due to its limited cost compared to its efficiency, and the KORAL electronic warfare system, which increases the performance of these drones. Both of these products have proved particularly effective in recent conflicts, such as in Syria, Libya and Nagorno Karabakh. Through

these exports Ankara is carrying out a real "drone diplomacy" which has allowed it to increase its influence in North Africa, in the Sahel, in the Horn of Africa and in the Gulf of Guinea.

Iran is a potential destabilizing actor in the macro-region, not only for its nuclear program but also for the asymmetrical threats it carries out, many of which take place in cyberspace. Indeed, since the 2010 Stuxnet cyber-attack, which targeted Iran's uranium enrichment centrifuges in Natanz nuclear facilities, Tehran has constantly developed defensive, but above all offensive, cyber capabilities. Iran has often used these cyber offensive capabilities as a means of deterrence and as a foreign policy tool. On several occasions, Tehran's cyber-attacks have coincided with geopolitically relevant events for the country, such as the Israeli incursions into the Gaza Strip or the negotiations for the JCPOA. These threats are now even more dangerous for Western countries, considering the latest attack on Albania and the growing trend of maritime cyberattacks in the Strait of Hormuz against Western ships. Finally, Iran also uses cyberspace for online propaganda. Tehran, on the one hand, restricts access to online information on the domestic front, on the other, carries out propaganda campaigns abroad. The aim is to promote a positive image for Iran, especially in the Islamic world, as evidenced by information operations in the MENA region. Also in this case, the online propaganda operations are closely linked to the relevant geopolitical events for the country, given the concomitance with the most important political implications in Lebanon, Yemen, Syria and Palestine.

Considering the results of this brief analysis, it becomes clear how the digital technology has become an important and essential foreign policy asset in the Wider Mediterranean and how this has already been understood by the main competitors in the region. In this context, it is essential for Italy to consider new foreign policy tools that adapt to the new digital reality of the macro-region and allow to effectively counter the moves of global and regional competitors.

# Chapter 3: The interconnection between Italian national interests in the region and digital transformation

## 3.1 Protection of critical undersea infrastructures

***Recent trends in the protection of critical infrastructures***

Critical Infrastructures are defined as "*any system which is essential for providing vital economic and social functions: health, food, security, transport, energy, information systems, financial services*".[152] The operational environment in which these critical entities operate has changed significantly in recent years. Firstly, the risk landscape is more complex, involving today natural hazards (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents). Secondly, operators are confronted with challenges in integrating new technologies such as 5G and unmanned vehicles into their operations, while at the same time addressing the vulnerabilities that such technologies could potentially create. Thirdly, these technologies and other trends make operators increasingly reliant on one another.[153] This complexity has made it necessary to adapt the protection measures, which, at the EU level, were integrated and adapted with the introduction of the CER directive in December 2022. It ensures a broader and more inclusive approach to critical infrastructure protection, which would allow Member States to equip themselves with more and more effective tools to address cross-border interdependencies and the potential effects of threats and incidents. In this sense, it provides the adoption of an effective national strategy and the determination of one or more competent authorities, requiring improved risk prevention and response capabilities.

The most urgent risk seems related to the cyber domain. Threats in the cybersphere are changing, gradually shifting from criminal actions mainly conducted by 'recreational' hackers or actors moved by financial motives, towards intelligence and destructive activities suspected of being conducted by state entities or criminal organisations. Moreover, advances on the Internet of Things (IoT) have increased the risk of information security incidents implying severe consequences over critical infrastructures. In the near future, it is likely not only that they will experience an increase in cyber

[152] Muti K. & Tessari P. (2021), *Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations*, European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union, p. 1

[153] European Commission (2020), *Proposal for a Directive of The European Parliament and of the Council on the resilience of critical entities*

threats, but that attempts of this kind will also have a higher degree of success.[154] For this reason, the EU has integrated the CER with the Network and Information Security (NIS) Directive, which laid the necessary foundations for regulating the essential aspects of information security within the companies operating in fundamental services and infrastructures, and the NIS-2, which extends the sectors, critical entities and essential services falling within the scope of the previous law. In Italy, NIS directive was transposed at national level by the D. L. 65/2018. This rule was then joined by the D. L. 82/2021, which accredited the National Cybersecurity Agency as "NIS competent authority", and by the D.L. 109/2019, which established methods and procedures for the establishment of the National Cybersecurity Perimeter, aimed at ensuring the security of networks, information systems and information services necessary for the performance of functions or the provision of services from whose discontinuity could derive a prejudice to national security.

***The cyber threat to energy infrastructures***

Much of the critical infrastructures for Italy in the Wider Mediterranean is linked to energy supply. The geographical position of the peninsula places it at the center of a complex network of submarine gas pipelines which are essential for Italian and European energy diversification, especially to decrease dependence on Russian export. Italy receives on its coasts the Transmed and the Green Stream from North Africa and the Trans-Adriatic Pipeline (TAP) which carries Azeri gas passing through Turkey. Added to these is the Eastmed project, which will connect Italy with the gas fields discovered by ENI in the Eastern Mediterranean (Zhor and Nour in Egypt, Leviathan in Israel and Calypso in Cyprus).


*Figure 17: Gas pipelines in the Mediterranean: Source: Il Messaggero*

[154] Muti K. & Tessari P. (2021), *Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations*, European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union, p. 12

The protection of these energy infrastructures is defined as a national strategic interest in the Italian 2022 National Security and Defense Strategy for the Mediterranean and assumes particular relevance considering the latest international trends. In September 2022, the damage to the Nord Stream gas pipeline, which connect Russia to Europe under the waters of the Baltic Sea, has raised a global alarm about the vulnerability of underwater energy networks. In Russian strategic thought, indeed, the attack on critical non-military infrastructure is widely considered a viable option, both in the initial stages of an open conflict and as an "asymmetric response" to enemy actions. Inflicting damage to economically important infrastructure is seen as a decisive step in eroding the adversary's willingness to engage in open or protracted conflict with the Russian Federation.[155] These concerns add to a trend that has seen the Mediterranean's energy infrastructure increasingly targeted by terrorist organizations and non-state actors since the 2011 Arab Spring. Energy assets are symbolic, strategically important and comprised of distributed infrastructures, many in remote locations that make them difficult to protect and thus attractive targets.[156] In Libya, since the start of the civil war oil and gas sector has been continuously disrupted by the actions of violent groups – such as those affiliated with the Islamic State of Iraq and the Levant (ISIL) as well as ethnic minorities like Berbers and Toubous – which have carried out a number of attacks on energy facilities, including Ras Lanuf, Es Sider, and Zuetina (oil and gas terminals). Syria and Egypt are two other important cases in relation to the impact of conflicts and terrorism on energy security. In Egypt, the Sinai Peninsula has been home to a number of attacks targeting its energy infrastructure (for instance, the gas pipeline connecting Egypt to Israel and Jordan was attacked at least once a month from mid-2011 to July 2012), in Syria the IS has repeatedly bombed electrical and natural gas infrastructure to deny resources to the government and weaken its position.[157] In light of this trend, the Italian navy has strengthened its commitment to protect critical submarine energy infrastructures. In 2021 it entered into an agreement with ENI to guarantee the physical protection of energy infrastructures also outside the Italian territorial sea and, after the sabotage of the Nord Stream, launched a mission to protect submarine energy assets consisting of two surface ships, equipped with submarines and auxiliary underwater drones, and a

[155] Freyrie M. & Leoni R. (2022), "Come la Russia minaccia i gasdotti nel Mediterraneo", *Affari Internazionali*, https://www.affarinternazionali.it/come-la-russia-minaccia-i-gasdotti-nel-mediterraneo/

[156] Giroux J. (2015), *Energy Infrastructure Targeting in the Mediterranean: a Shifting Threat*, IEMed Mediterranean Yearbook 2015

[157] Caşın M.H. (2016), "Critical Infrastructures: Security and Energy Politics in the Eastern Mediterranean Region and the Role of the OSCE" in Colombo S. & Sartori N. ed., *The OSCE's Contribution to Energy Governance in the Mediterranean Region*, New-Med Research Network, IAI, Rome

core of divers. This team accompanies the "Safe Mediterranean" operation, deployed to guard the maritime lines of communication and to identify any threats.[158]

While physical attacks on pipelines have been more common, cyberattacks on pipeline systems are becoming more frequent as systems are computerized. Already in June 1982, a major explosion occurred on the Trans-Siberian gas pipeline as the pipeline's control software unknowingly contained a malicious code that massively increased the pipeline pressure, leading to the explosion. In the Mediterranean basin, in 2008 the Baku-Tbilisi-Ceyhan (BTC) pipeline exploded due to a sophisticated cyberattack carried out through the pipeline's surveillance camera system.[159] In May 2021, the Colonial Pipeline, one of America's largest gas pipelines, was sabotaged through a ransomware attack, rendering an 8,850 km network of pipelines unusable and paralyzing supplies of 2.5 million barrels per day. This, which is the largest cyber-attack on infrastructure in US history, prompted the authorities to declare a state of emergency in seventeen US states along the east coast and in Washington. By early February 2022, a slew of subsequent cyber-attacks had struck oil and gas facilities across Europe, disrupting the operations of multiple oil transport and storage companies in Germany, Belgium, and the Netherlands, and threatening production and distribution in the sector.

Such attacks are possible due to some unique vulnerabilities of the global energy ecosystem. Firstly, it relies on inherently complex infrastructure. Utility companies are exposed to relatively high risks because their networks of both physical infrastructure and cyber-infrastructure – including distributors, suppliers, storage facilities, and other assets – often overlap and are spread across many countries. Secondly, the digital infrastructure that supports the global energy sector operates around the clock, with virtually no downtime.[160] Therefore, given the interconnection and interdependence of these infrastructures, as well as their transnationality, it is not enough to guarantee their cybersecurity at a domestic and European level, but becomes necessary to develop a cooperation framework at the regional level also with the countries of transit and origin of these pipelines. A common crisis prevention system must be developed, for example by identifying the operators of essential services and analyzing the cyber resilience of the individual infrastructure components, but even an effective cyber response framework and coordination should be defined and implemented.[161]

---

[158] Freyrie M. & Leoni R. (2022), "Come la Russia minaccia i gasdotti nel Mediterraneo", *Affari Internazionali*, https://www.affarinternazionali.it/come-la-russia-minaccia-i-gasdotti-nel-mediterraneo/

[159] Dancy J.R. & Dancy V.A. (2017), "Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks", *Oil & Gas, Nat. Resources & Energy Journal*, vol. 2, n. 6

[160] Nelson J. & Romero A. (2022), *Why Europe's energy industry is vulnerable to cyberattack*, European Council on Foreign Relations

[161] Picard R. (2022) , "Cybersecurity in Energy Markets: Challenges and Opportunities", in MEDREG Consumer Working Group, *The Digitalization of Energy Markets And The New Role Of Consumers*, Association of Mediterranean Energy Regulators

In this sense, as underlined by the Italian Ambassador Pasquale Ferrara, there is the need to further explore existing dialogues with the Mediterranean partners and the private sector regarding the energy field, the shared critical infrastructure and the emerging technologies.[162]

### *The physical backbone of the internet: submarine cables as new targets of geopolitical competition*

In addition to the pipelines, the Wider Mediterranean hosts another type of critical infrastructure for Italy and for Europe, the submarine internet cables. The global subsea data cable network is a vital critical infrastructure as much as 99% of the world's digital communications transit through the network, and the global economy and digital services are fully dependent on it. In particular, the most vital bottleneck concerns the passage between the Indian Ocean and the Mediterranean via the Red Sea because the core connectivity to Asia runs via this route.[163] A crucial case which underline the cruciality of the undersea internet cables in the region is provided by an incident that occurred in December of 2008, when three of the world's largest undersea cables, connecting Italy with Egypt, were unwittingly severed by shipping traffic in the Mediterranean. In a matter of hours, disruptions to regional connectivity had knocked out 80% of the connectivity between Europe and the Middle East.[164]

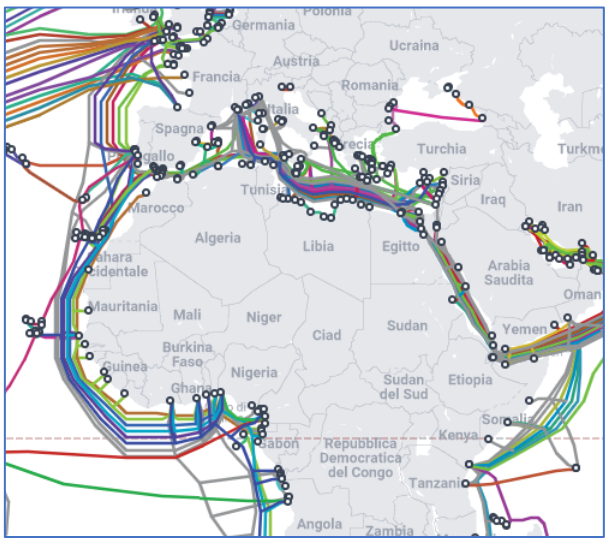


*Figure 18: Undersea cables in the Wider Mediterranean. Source: Telegeography*

[162] Ferrara P. (2021), "As Cyber Threats Target the Wider Mediterranean Region, Countries Must Act Together", *ISPI*, https://www.ispionline.it/en/pubblicazione/cyber-threats-target-wider-mediterranean-region-countries-must-act-together-35345

[163] Bueger C., Liebetrau T., Franken J. (2022), *Security threats to undersea communications cables and infrastructure – consequences for the EU*, Directorate General for External Policies of the Union, Policy Department for External Relations

[164] Sunak R. (2017), *Undersea Cables: Indispensable, insecure*, Policy Exchange, Westminster, London

As underlined by Sherman, "*Western governments often conceptualize the internet as an abstract thing — "cloud," "cyberspace" — while forgetting it depends on physical infrastructure to run. Since cables lay out at sea, across national borders and are often hidden underground, they have frequently been forgotten and received limited attention from policymakers. The same cannot be said for every other government*".[165] Indeed, submarine cables have become a new terrain of geopolitical competition in the Wider Mediterranean, especially considering the interest that China and Russia have placed on them.

As seen in the previous chapter, digital connectivity, and therefore submarine internet cables, constitute the core of the Chinese Digital Silk Road. Chinese entities including the Hengtong Group and its subsidiaries, Huawei Marine and Hengtong Marine, are currently leading the construction of the PEACE cable, a Digital Silk Road project that starts in Gwadar and Karachi in Pakistan and is planned to land in Marseille in France. This creates concerns that relate to the wider problem of the region's digital dependence on China and the consequent opportunity for Beijing to get its hands on data and informations in the area. Indeed, thanks to a constellation of consortia, Hengtong Group is both the owner and the operator of the PEACE and this setup raises concerns because the consortium could potentially manage and redirect the data flow travelling through the cable. Chinese investments in submarine cables of the region are still growing as evidenced by the agreement between Hengtong's international business unit and Telecom Egypt to open a landing point or by the one between the Libyan International Telecom Company and Huawei Marine to construct the Silphium cable system, which connects Derna in Libya with Chania in Greece.[166]

The Chinese strategy highlights the need for an integrated approach among the European partners to counter Beijing's economic expansionism. Three European companies are particularly active in the internet infrastructure sector in the Wider Mediterranean region: Telecom Italia Sparkle, Orange, and Telxius, based respectively in Italy, France and Spain. Competition between them remains the dominant framework as member states' strong diplomatic relations with countries in the region often helps these firms secure contracts. For example, the positive relationships between France and countries in the Sahel have helped Orange secure licences in that region or Italian diplomatic efforts to maintain positive ties with Libya and Israel helped Sparkle launch infrastructure projects in those countries. One of the main ways to reduce Chinese influence would be to increase cooperation

[165] Sherman J. (2022), "Internet Security Under the Ocean: EU-US Must Cooperate on Submarine Cable Security", *ISPI*, https://www.ispionline.it/en/pubblicazione/internet-security-under-ocean-eu-us-must-cooperate-submarine-cable-security-35471

[166] Colombo M., Solfrini F., Varvelli A. (2021), *Network Effects: Europe's Digital Sovereignty In The Mediterranean*, European Council on Foreign Relations

between these three companies and create consortia among them for the construction of cables in the region. The EU could help in this sense by financing projects directly – as in the case of BELLA consortium, where the European Commission financed an undersea cable connecting Portugal to Brazil through EllaLink – but also by working with states in its neighbourhood to set similar legislative standards on privacy and ownership. "*In doing so, it has the potential – still largely untapped – to facilitate European companies' investments in the region and curtail the efforts of hostile powers"*.[167]

In addition to China, another threat to the submarine cables of the Wider Mediterranean could come from Russia. As previously underlined, indeed, analysts foresee interference towards submarine cables as one of the future evolutions of Russian information warfare, also considering that the modernization of the Russian Navy has led to the emergence of highly specialized naval assets in this sense and that Moscow has shown on several occasions that it considers the attack on critical infrastructures as a viable option. The Russian threat, therefore, requires measures to physically protect submarine cables and the main European navies have already acted in this sense. French 2023 budget includes an "ocean floor" item for the "protection of natural resources and submarine cables" and Paris has invested in the purchase of two remotely piloted underwater vehicles. The UK has planned to add two Multi-Role Oceanographic Survey (MROS) vessels to their naval fleet in 2023. The Italian Navy has also intervened in this area, stipulating an agreement with Sparkle for the surveillance of the submarine cables produced by the company.[168] NATO has also stated that an attack by a foreign power on strategic infrastructure of member states could be considered as an attack on members of the Alliance. Therefore, if Russia were to strike a strategic infrastructure in the territorial waters of a member state, this would most likely trigger the activation of collective defense pursuant to Article 5 of the NATO Treaty.[169]

All these initiatives indicate a growing attention to the physical protection of submarine cables but this should be further integrated. Italy, working with international partners, should seek to encourage the establishment of Australian-style Cable Protection Zones (CPZs) in the Mediterranean and Suez, in order to safeguard connectivity in strategically important theaters. Furthermore, it should press at the NATO level to promote the undertaking of naval exercises and war games to hone potential responses to an attack on undersea cable infrastructure. These exercises would work with the

[167] *Colombo M., Solfrini F., Varvelli A. (2021), Network Effects: Europe's Digital Sovereignty In The Mediterranean, European Council on Foreign Relations*
[168] Turato M. (2022), "La difesa europea delle infrastrutture sottomarine", *Formiche*, https://formiche.net/2022/10/difesa-europea-sottomarina/
[169] Gili A. (2022), "Cavi: interessi di Stato in gioco", *ISPI*, https://www.ispionline.it/it/pubblicazione/cavi-interessi-di-stato-gioco-36487

submarine cable industry to test protocols and defense strategies in an international setting.[170] Finally, it would be strategic to guarantee the security of submarine cables also outside the Italian national borders, in particular in North Africa and in the Sahel, where there is an exceptionally high risk that non-state armed groups will target this infrastructure and disrupt countries' internet connections. For instance, in 2013 the Egyptian navy arrested three scuba divers in the waters off the coast of Alexandria under charges of having attempted to cut the SeaMeWe-4 internet cable. Cooperation with the countries of the region in this sense could involve the military ships that are deployed to the Red Sea, the Mediterranean, and the west coast of Africa to protect international trade.[171]

In addition to physical threats, these critical infrastructures are particularly vulnerable to cyber-attacks. Indeed, there are numerous ways in which cyber offensive operations can be carried out against them. One of the most significant is linked to the reliance on remote network management systems. Hacking into network management systems can provide attackers control of multiple cable management systems, visibility of networks and data flows, knowledge of physical cable vulnerabilities, and the ability to monitor, disrupt, and divert traffic. In addition, Network Operation Centres, remote access portals, and other systems needed for the functioning of the cable network – such as electrical power, routers, heating, ventilation and air-conditioning – are also potential cyber-attack vectors.[172] One of the first cases of an undersea cable cyberattack occurred in April 2022 in Hawaii, when US authorities interrupted a cyberattack on a telecommunications company's servers, associated with an undersea cable responsible for internet, cable services and cellular connections in the Pacific region.[173] Also in this case, therefore, as with energy infrastructures, it is necessary to establish cooperation frameworks with the countries of origin and transit of the cables, but even with the private companies that built them, to ensure adequate cybersecurity of the infrastructure.

[170] Similar recommendations have been made for the UK: Sunak R. (2017), *Undersea Cables: Indispensable, insecure*, Policy Exchange, Westminster, London
[171] Colombo M., Solfrini F., Varvelli A. (2021), *Network Effects: Europe's Digital Sovereignty In The Mediterranean*, European Council on Foreign Relations
[172] Bueger C., Liebetrau T., Franken J. (2022), *Security threats to undersea communications cables and infrastructure – consequences for the EU*, Directorate General for External Policies of the Union, Policy Department for External Relations
[173] Tarabay J. (2022), "An Underwater Hack and the Digital Ripple Effects", *Bloomberg*, https://www.bloomberg.com/news/newsletters/2022-04-20/an-underwater-hack-and-the-digital-ripple-effects

## 3.2 Sea Trade and Maritime Cyber Security

### *Italy and the Mediterranean as crossroads of maritime trade*

In addition to submarine energy pipelines and internet, the Wider Mediterranean is a fundamental crossroads for Italy also, and above all, for maritime trade. The maritime security of the region, therefore, constitute one of the main drivers of the Italian presence and one of Rome's major national interests. Italy has always been linked to the sea for many economic and safety aspects. It represents a historical heritage of the country, which supports the national economy and, therefore, national well-being and prosperity. As a transformation economy, which imports raw materials and semi-finished products to export "Made in Italy" finished ones, Italy is heavily dependent on transport and maritime traffic.[174] It is the first country in Europe for the quantity of goods imported by sea; it imports about 80% of the oil it needs by sea and it has the 11th merchant fleet in the world and the 3rd fishing fleet in Europe. Only the national maritime cluster, excluding coastal tourism, generates about 3% of GDP, with an economic multiplier of 2.9 times the invested capital. In 2018, 79.3% of Italian goods exported to the world travelled by sea, a percentage that rises to 95.9% considering only non-EU countries.[175] In June 2022, import-export by sea of Italy was close to 184 billion euros with an increase of 42% on an annual basis.[176]

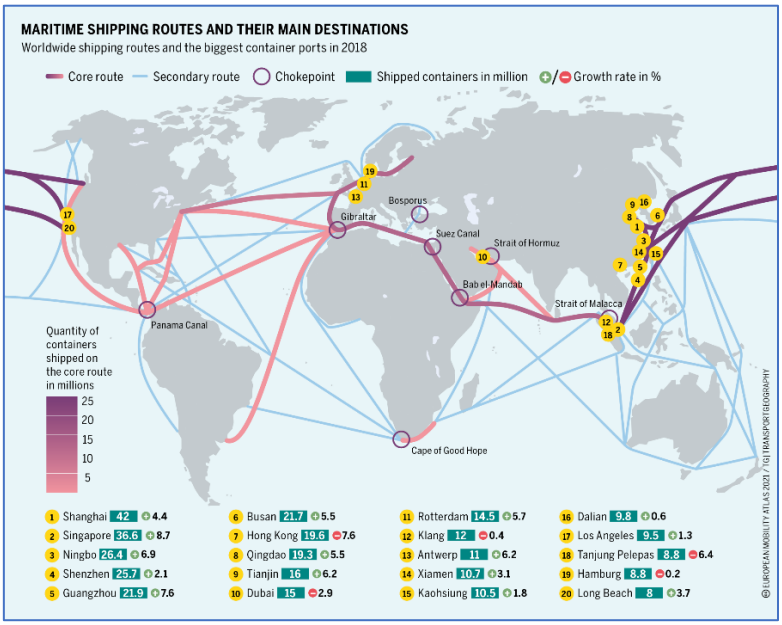


*Figure 19: Maritime Shipping Routes. Source: European Mobility Atlas 2021*

[174] Italian Ministry of Defense (2022), Strategia di Sicurezza e Difesa per il Mediterraneo 2022
[175] Circolo di Studi Diplomatici (2020), "Sicurezza e gestione delle crisi. La dimensione marittima", *Dialoghi Diplomatici*, n. 250
[176] SRM (2022), Italian Maritime Economy Report 2022

This context clearly shows how Italy vitally depends on the Mediterranean and on the communication routes that cross it. This basin - although representing only 1% of the global water surface - is affected by 20% of world maritime traffic, which rises to 30% for oil, which arrives almost entirely with specialized ships from the Persian Gulf, from the two African ocean sides, the eastern Mediterranean and the Black Sea through the crucial passages of Suez, Hormuz and Bab El Mandeb. Italian geographical position, central to the two choke points of Gibraltar and Suez, places the national ports at an important strategic crossroads which intersects the huge commercial traffic coming from the Indian Ocean, the Gulf Region and the Far East towards the Atlantic, the Middle East and the Continental Europe, which is the industrial heart of the Union.[177] This centrality of Italy and the Mediterranean, as already underlined in the previous chapter, has increased following the expansion of the Suez Canal, which has meant a strong increase in commercial traffic in the area and strong foreign investments in Mediterranean ports. While on the one hand the new routes and current trends represent a great development opportunity for the powers of maritime trade, for Italy it is an opportunity to regain centrality in the context of the dynamics and evolution of global traffic.[178]

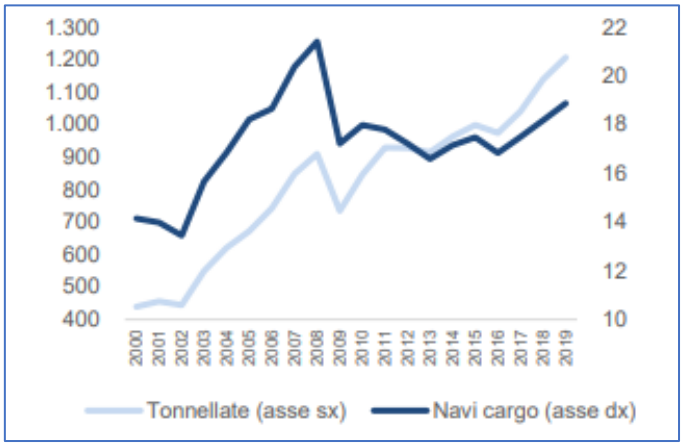


*Figure 20: Number of vessels and tons in transit through the Suez Canal (2000-2019, '000). Source: Suez Canal Authority*

### *Ports and the growing digital transformation*

An essential condition for Italian centrality in maritime trade is the strengthening of national port infrastructures. The European Union has identified ports as critical infrastructures in Directive 2005/65/EC. Ports play a crucial role at different levels for many sectors and have been the successful pioneers in Europe for interconnecting the different types of transport. As a main vehicle for European

[177] Circolo di Studi Diplomatici (2020), "Sicurezza e gestione delle crisi. La dimensione marittima", *Dialoghi Diplomatici*, n. 250

[178] Camerano S. et al. (2021), *Suez e le rotte alternative: il futuro dell'Italia nel commercio marittimo*, CDP Think Tank

imports and exports (food, commodities, etc.) with the rest of the world, ports enable also trade and contacts between all European nations. Moreover, they are important nodes for passengers and vehicles transportation (inter and extra-EU) and play a key role in European fishing activity. Therefore, ports, as submarine energy and internet cables, constitute particularly strategic critical infrastructures for Italy in the Mediterranean. Their protection has an important role in the Italian security strategy and policy in the region.[179]

Although the main threat comes from the attempts of non-EU actors, mainly from China, to acquire stakes or the entire control of the main European and Mediterranean terminals, another fundamental aspect remains the protection of these infrastructures from attacks by state and non-state actors. The European Maritime Security Strategy (EUMSS) identifies among the main maritime security risks and threats "*terrorism and other intentional unlawful acts at sea and in ports against ships, cargo, crew and passengers, ports and port facilities and critical maritime and energy infrastructure, including cyber-attacks*".

In recent years cybersecurity have indeed acquired particular relevance following the growing digitalization of the sector. As a logistics center and linkages with shipping lines becomes digitalized, container ports have integrated cybertechnologies into port activities, such as cargo handling and navigation, environment and pollution prevention, risk management, and port security. A turning point in this digitalization process was the definition of nine standardized forms to be used to exchange information within the maritime ecosystem by SOLAS (Safety of Life at Sea) and FAL (Facilitation of International Maritime Traffic) conventions. Since 2019, electronic exchange of required information is mandatory, especially using "Single Window" systems offset up by public authorities. This standardisation of data exchanges has a strong impact on port IT ecosystems and poses new IT security challenges.

In 2011, European Network and Information Security Agency was one of the first to identify a lack of awareness of cybersecurity in maritime transport and ports. In the following years, the increasing dependence of ports and maritime traffic on the digital sphere has helped to highlight this aspect even more. In 2015, the United States Coast Guard introduced its Cyber strategy for critical maritime infrastructure. The next year, the Baltic and International Maritime Council (BIMCO), the International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO and the Cruise Lines International Association (CLIA) published "Guidelines on Cyber Security Onboard Ships". In the same year, IMO released the "Interim Guidelines on Maritime Cyber Risk Management", which

[179] Senato della Repubblica (2022), *Relazione Annuale COPASIR febbraio 2022*

underlines that cyber-risk management should be complementary to existing security and safety risk management requirements, like ISM and ISPS Codes. At the European level, the NIS Directive, at the recitals number 10 and 11, provides specific cybersecurity requirements for companies, ships, port facilities, ports and vessel traffic services in the Union.

***Ports' cyber-vulnerabilities and threats***

As mentioned in the previous paragraph, critical infrastructure, including ports, constitutes a likely target for cyberattacks given its significance on the functionality of societies. In addition, what makes ports particularly vulnerable to cyberthreats relates to their basic characteristics. One of the greatest weaknesses is the complexity of the port ecosystem due to the number and diversity of stakeholders taking part in port operations (up to 900 for the biggest ports). This ecosystem is built from companies of various sizes, with various levels of cybersecurity capabilities and which can even be direct competitors among themselves. This makes the overall cybersecurity control at port level difficult with heterogeneous level of controls within the port. Added to this is a technical complexity of port IT and OT systems, which can be developed, managed and maintained by different teams or entities. This represents a significant problem considering the IT and OT convergence and interconnection in ports. Usually OT systems, more vulnerable than IT systems, are protected because they are separated from IT systems and networks, but, increasingly, IT and OT systems and networks become more and more dependent and interconnected, exposing OT systems to higher risks. The vulnerability is then aggravated by the strong interdependencies between port systems and external services from other sectors (e.g. energy) that introduce interdependency cybersecurity risks.[180]

Shipping and port operators might be targeted by five categories of cyberthreats, namely, hacktivism, cybercrime, cyber espionage, cyber terrorism, and cyber war.[181]

- Hacktivism means the operation in cyberspace using different hacking techniques (e.g. malware) to invade into web pages and on computers, and create pressure on a certain object. The aim for conducting hacktivism varies from gaining attention to disrupting business through the vulnerable gaps in the cyberspace.

- Cyber criminality refers to criminal activities that are deemed injurious to the public welfare and are legally prohibited. The motivation to conduct cyber criminality is normally to exploit human

[180] Drougkas A. et al. (2019), *Port Cybersecurity: Good practices for cybersecurity in the maritime sector*, European Union Agency for Cybersecurity

[181] Ahokas J. et al. (2017), "Cybersecurity in ports: A conceptual approach", in Blecker T., Kersten W. and Ringle C.M. (Eds.), *Digitalization in Supply Chain Management and Logistics*, epubli GmbH, Berlin, pp. 343-359

or security vulnerabilities in order to gain financial benefits, inflict personally motivated harm, endanger confidentiality and availability of data and systems, or violating a firm's reputation and brand.

- Cyber espionage is the illegal access to secret and delicate information (e.g. company strategy, private information, or intellectual capital). It aims to gain competitive advantages rather than create pressure and business disruption. Thus, the consequences might be the loss of intellectual property, business profits and efficiency, and customer information, additional costs thanks to the interrupted business plan, and damage to company reputation.

- Cyber terrorism is a politically motivated attack using various tools (e.g. computer viruses, computer worms, phishing, and other malicious software) to violate the information, computer systems, computer software, and databases of important organizations or global networks in order to accomplish the political or ideological gain. Thus, the cyber terrorism normally causes serious consequences, such as massive damage to government systems and national security programs, or loss of life or significant bodily harm.

- The last category of cyberthreats is cyber war, which is a part of the modern information war between nations. Apart from the military, the cyber war might be done by the state-sponsored actor (e.g. terrorist groups, companies, political, or ideological extremist groups) to attack the opponent's computer networks. In cyber war, the computers and satellites might be used to disturb critical infrastructures with the aim to lead to disastrous consequences. This infrastructures could include ports as they are the key node of global trade holding substantial amounts of data and monetary transactions among stakeholders. This makes ports attractive for cyberattacks.

The European Union Agency for Cybersecurity in the "Good practices for cybersecurity in the maritime sector" identified four possible cyber-attack scenarios in correlation with the sources of threats and the possible impacts on port assets.[182]

The first involves the compromission of critical data to steal high value cargo or allow illegal trafficking through a targeted attack. In this case attackers must have in-depth knowledge of port

[182] Ahokas J. et al. (2017), "Cybersecurity in ports: A conceptual approach", in Blecker T., Kersten W. and Ringle C.M. (Eds.), *Digitalization in Supply Chain Management and Logistics*, epubli GmbH, Berlin, pp. 343-359

systems and networks (social engineering, network scan), port processes and port infrastructure (physical intrusion) to perform cargo and container theft. An example of such an attack occurred at one of Antwerp's port terminals in Belgium, when a drug cartel took control of containers movement and retrieved the data needed to collect it before legit owner.

Another scenario could be the propagation of ransomware leading to a total shutdown of port operations. This can be a targeted or a non-targeted attack (as collateral damage of targeted attack on other companies through the ransomware propagation). The hackers can develop a ransomware exploiting different vulnerabilities to spread it into the port networks and encrypt the different systems and devices (workstations, servers, etc.), leading to the destruction of the infected systems and the potential loss of backups (within servers which could be encrypted). An example of a destructive ransomware-like malware attack was the large-scale incident affecting the operations of the Maersk terminal in Rotterdam, with high risks of security and safety incidents, and port terminal operations managed manually for more than two weeks.

A cyber-attack could also compromise Port Community System for manipulation or theft of data. This is a targeted attack on the systems used for the exchanges between all stakeholders (usually the Port Community Systems). The objectives are to falsify the information on port services to disrupt the operations or to modify some operations in the systems (implying financial loss for the port). This scenario is particularly realistic because those systems are exposed to all port stakeholders by different ways (usually using different networks and systems, through VPN access, or through the Internet, most of the time via machine-to-machine interconnections). Those systems are increasingly automatically interconnected with external systems (via API, EDI exchanges, etc.) which become an additional attack surface to reach port systems.

Finally, there is the possibility to compromise OT systems creating a major accident in port areas. This scenario is specific to the OT world and the ICS specificities and is considered to be realistic even no such attacks in ports are publicly known. Indeed, similar attacks occur in other critical sectors, especially in the energy one. This kind of attack doesn’t need to be generally sophisticated to be impactful and the major risks remain the connection with external networks and systems, especially the Internet. The specificities of such attacks are the close link between the physical and logical world: the attack usually begins in the logical world (from the IT component) and has impacts in the physical world (damage to OT systems and end-devices, safety and security incidents, etc).

### *Ports' cybersecurity in the Wider Mediterranean*

For Italy, it is increasingly topical to guarantee the cybersecurity of its national ports, especially in the light of the growing threat affecting the sector. In recent years, there have been several cases of cyberattacks on European ports: to those already mentioned in Antwerp and Rotterdam are added the ransomware attack on the port of Barcelona in 2018 and the cyberattack on the port of Lisbon in 2023. In 2022, cyberattacks also hit Hamburg as well as at least six oil terminals in Belgium and the Netherlands, preventing tankers from delivering energy supplies.[183] According to the President of Federlogistica-Conftrasporto (the Italian Federation of Logistics Companies) the risk of cyberattacks is not a random hypothesis, but "*terribly concrete*". The leaders of the Italian maritime and transport sectors have therefore asked for greater state involvement in guaranteeing the cybersecurity of Italian ports, allocating part of the resources of the NRRP in this sense. The 2022 NIS 2 European directive, on the security of networks and information systems, extends the range of action in many delicate sectors including transport and ports and not only to large companies but also to medium-sized ones. In this context, the resources of the NRRP should be used to help businesses but also the Port System Authorities to structure themselves and comply with European obligations.[184]

In addition to having to protect national port infrastructures, however, in order to guarantee Italy's national interests in maritime trade, it is also necessary to take into account the security of other ports which are fundamental for Italian trade routes. Indeed, the impact of cyber threats may sometimes extend far beyond a particular vessel, a port facility, or even a country. The University of Cambridge's Centre for Risk Studies found that an attack targeting cargo database logs at major ports in the Asia-Pacific region could result in $110 billion in damages. It estimated that an event of such magnitude could have a devastating impact on countries and companies connected to the target, yet weren't the intended victim.[185]

For example, Italy, as well as many European countries, is closely related to security of the Middle Eastern ports in the Persian Gulf and in the Strait of Hormuz, from which most of the oil and gas ships essential for energy supplies come. The danger of cyberattacks in the area has already been shown in two attacks on Iranian ports: that of the Islamic Republic of Iran Shipping Lines in 2011 and the most recent in 2020 on the Shahid Rajaee port terminal, when computers that regulate the flow of vessels, trucks and goods all crashed at once, creating massive backups on waterways and

[183] N.A. (2022), "Oil terminals disrupted after European ports hit by cyberattack", *Euronews*, https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack
[184] N.A. (2022), "Cyber security nei terminal portuali: "Lo Stato deve contribuire"", *Shipping Italy*, https://www.shippingitaly.it/2022/02/15/cyber-security-nei-terminal-portuali-lo-stato-deve-contribuire/
[185] Reva D. (2021), *Maritime cyber security: Getting Africa ready*, Institute for Security Studies, Africa Report 29

roads leading to the facility. The attack, which snarled traffic around the port for days, was carried out by Israeli operatives, presumably in retaliation for an earlier Iranian attempt to penetrate computers that operate rural water distribution systems in Israel.[186]

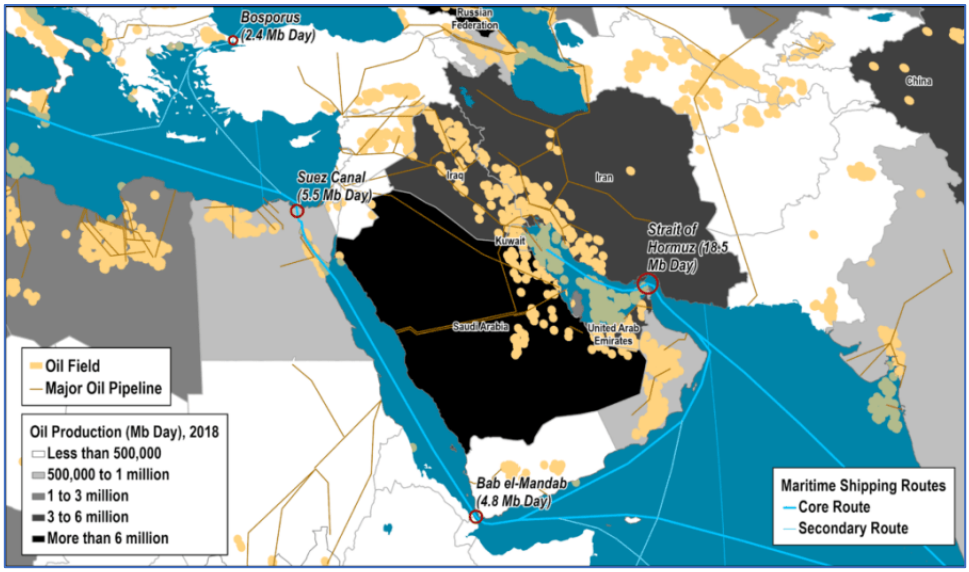


*Figure 21: Shipping Routes and Oil Production in the Middle East. Source: Port Economics, Management and Policy*

Albeit to a lesser extent, even African ports, especially those in the Gulf of Guinea, are important for Italy's energy supply. As maritime technological solutions are becoming cheaper and more accessible, these will play an ever-increasing role within the maritime sector in the continent. Therefore, given this growing reliance on information technology into maritime activities, African ports will be increasingly vulnerable to cyber threats, mainly due to the low levels of cybersecurity infrastructure.[187] An example of this happened in July 2021, when Transnet, the company that runs South Africa's ports infrastructure, became a victim of a ransomware attack, which caused huge slowdowns not only to South African national traffic but also to regional one.[188]

These cases show how an attack on a logistic hub, such as a port, could quickly disrupt a supply chain network with tremendous financial damages extending far beyond the point of the attack. This strong interdependence, added to the variety of stakeholders involved in the operations of a port, make it necessary to adopt a collective approach based on cooperation and harmonisation of responses and common standards. It therefore becomes essential for a country as closely dependent on maritime

[186] Nakashima E. & Warrick J. (2020), "Officials: Israel linked to a disruptive cyberattack on Iranian port facility", *The Washington Post*, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html
[187] Reva D. (2021), *Maritime cyber security: Getting Africa ready*, Institute for Security Studies, Africa Report 29
[188] Heiberg T. & Shabalala Z. (2021), "Cyber-attack disrupts major South African port operations", *Reuters*, https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/

traffic as Italy to ensure that minimum cybersecurity standards are set for ports at an international level and to collaborate with other countries sharing informations and best practices. The International Maritime Organization (IMO) has a central role to play, as in the case of the adoption of the Maritime Cyber Risk Management in Safety Management Systems (MSC.428(98)) in 2017. The resolution requires shipowners and managers to include cyber risk management into their Safety Management Systems under the International Safety Management Code. In addition to acting at the level of international organizations, another possibility could be to provide, also in collaboration with private companies, cyber-capacity building in the most backward contexts in this sector, such as sub-Saharan Africa. As underlined by Jens Meier, CEO of the Port of Hamburg, "*the price of not improving our collective cyber resilience can mean the loss of infrastructure of critical systems, delays in the logistics chain, as well as having economic, organizational and environmental repercussions*".[189]

***Protection of maritime trade routes***

In addition to ports, the stability of maritime trade mainly depends on the safety of commercial routes and ships. As stated in Art. 5 of the NATO Maritime Strategy, "*global trade relies upon secure and low-cost international maritime transportation and distribution networks that are vulnerable to disruption, to the extent that even short interruptions would seriously impact international trade and Allies' economies"*. The maintenance of the freedom of navigation and sea-based trade routes are in Allies' security interest.[190] Even the EU Maritime Security Strategy identifies among the strategic maritime security interests of the Union and its Member States "*the preservation of freedom of navigation, the protection of the global EU supply chain and of maritime trade, the right of innocent and transit passage of ships and the security of their crew and passengers*".[191] While both documents identify cross-border organized crime, and in particular maritime piracy, among the main threats, the European strategy, formulated two years later, also underlines the danger of acts of external aggression, including those related to maritime disputes. In fact, these remain the two main threats to the security of commercial shipping lanes.

The phenomenon of maritime piracy peaked in 2011, with 439 incidents[192], mainly due to attacks by Somali pirates in the Horn of Africa. Since then, the international community has intervened to stem

[189] N.A. (2021), "Resilience and collaboration, the best defense of ports against cyberattacks", *Pier Next*, https://piernext.portdebarcelona.cat/en/governance/resilience-and-collaboration-the-best-defense-of-ports-against-cyberattacks/
[190] NATO (2012), *Alliance Maritime Strategy*, https://www.nato.int/cps/en/natohq/official_texts_75615.htm
[191] Council of the European Union (2014), *European Union Maritime Security Strategy*, https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf
[192] Data from International Maritime Bureau

the phenomenon. In particular, the EU has launched various operations in areas deemed of strategic interest for the Union. By participating with its assets in these operations, the Italian Navy has played an important role in guaranteeing the maritime security of these areas.

In 2008 the first EU naval operation, EUNAVFOR ATALANTA, was launched with the task of helping the Somali Navy in guaranteeing the maritime security of the Horn. The mission has been a success, protecting more than 2,000 vessels, ensuring the delivery of more than three million tons of food and aid to the region. A total of 171 pirates have been transferred to the local authorities while 12,720 kilos of narcotics have been impounded.[193] Today the number of piracy attacks in the area has drastically decreased so much that since January 2023 this is no longer considered by the EU as a High Risk area. Capitalizing on the successes of suppressing piracy off the coast of the Horn of Africa, the overall mandate of Operation Atalanta was consolidated following a strategic review of the EU's role in the Horn of Africa. With this mandate, Operation Atalanta is now in a better position to contribute to the implementation of the UN arms embargo on Somalia, reduce drug traffic, support the ongoing fight against Al Shabaab and its funding stream, and the progress of the Somali government.[194]

With the progressive reduction of the numbers of attacks in the Horn of Africa, the main piracy hotspot in the world has become the Gulf of Guinea. Here too, EU action has proved particularly successful. If the ICC International Maritime Bureau's annual report recorded 115 incidents of piracy and armed robbery against ships in 2022, the lowest figure since 1994, much of this achievement is due to an overall decrease of piratical activity in the highly risky waters of the Gulf of Guinea. The EU launched the Coordinate Maritime Presence (CMP) concept in the Gulf of Guinea in January 2021 and its implementation was extended in February 2022. CMP can be implemented in any maritime area of the world determined by the Council of the EU as a Maritime Area of Interest and uses existing EU Member States naval and air assets present or deployed on a voluntary basis in these Maritime Areas of Interest. It relies on enhanced coordination of naval and air assets, which remain under national command and provides continuity, complementarity and synergy between EU Members States' actions, enhancing awareness, analysis and information sharing through the Maritime Area of Interest Coordination Cell (MAICC).[195]

[193] Data from EUNAVFOR ATALANTA Official Website, https://eunavfor.eu/
[194] European Council (2022)," Operation ATALANTA, EUTM Somalia and EUCAP Somalia: mandates extended for two years", Press Release, https://www.consilium.europa.eu/en/press/press-releases/2022/12/12/operation-atalanta-eutm-somalia-and-eucap-somalia-mandates-extended-for-two-years/
[195] EAAS (2022), Factsheet: Coordinated Maritime Presences, https://www.eeas.europa.eu/eeas/factsheet-coordinated-maritime-presences_en

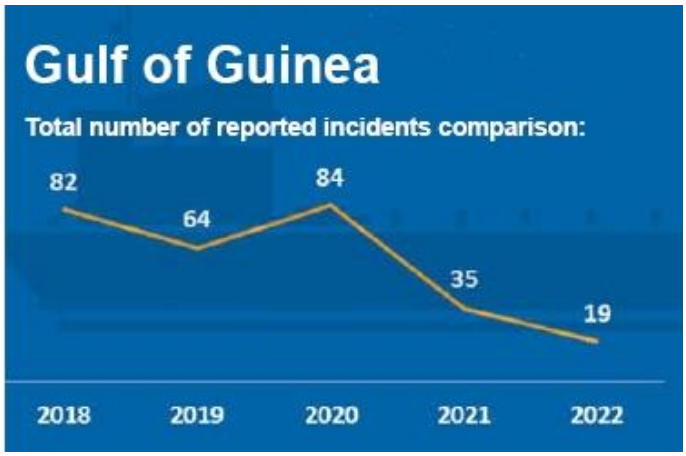


*Figure 22: Decrease in piratical attacks in the Gulf of Guinea: Source: IMB*

Building on this positive example, the EU decided to launch the implementation of the CMP concept even in the North-Western Indian Ocean by establishing a Maritime Area of Interest covering the maritime area from the Strait of Hormuz to the Southern Tropic and from the North of the Red Sea towards the centre of the Indian Ocean. The implementation of the CMP concept in the North-Western Indian Ocean complement both the EU's and EU member states' activities in the region, while respecting the mandate and chain of command of EUNAVFOR Operation ATALANTA. The EU should enhance coordination and cooperation with the European Maritime Awareness in the Strait of Hormuz (EMASOH) surveillance mission.[196] It was set up in January 2020 by Belgium, Denmark, France, Germany, Greece, Italy, the Netherlands, and Portugal in response of the Iranian attacks on tankers and commercial ships in UAE waters and the strikes on the Abqaiq and Khurais oil facilities in Saudi Arabia in 2019, arguing that such incidents were undermining freedom of navigation in the Gulf and the safety of ships in the Strait of Hormuz.[197]

There is a long line of Iranian acts of "state piracy" in the region. The IRGC navy has long used its fleet of speedboats to harass commercial shipping and military vessels in the region and Teheran has also repeatedly threatened to blockade the strait if it is attacked. Even the Iran-backed Houthi militia in Yemen has launched repeated attacks on ports and ships in recent years, routinely planting marine

[196] European Council (2022), *Coordinated Maritime Presences: Council extends implementation in the Gulf of Guinea for two years and establishes a new Maritime Area of Interest in the North-Western Indian Ocean*, Press Release, https://www.consilium.europa.eu/en/press/press-releases/2022/02/21/coordinated-maritime-presences-council-extends-implementation-in-the-gulf-of-guinea-for-2-years-and-establishes-a-new-concept-in-the-north-west-indian-ocean/#:~:text=The%20CMP%20concept%20in%20the,as%20a%20maritime%20security%20provider.

[197] Bianco C. & Moretti M. (2022), "Europe's role in Gulf maritime security", *Middle East Institute*, https://www.mei.edu/publications/europes-role-gulf-maritime-security

mines in the southern Red Sea and in the Bab Al-Mandab Strait in the path of commercial shipping.[198] In May 2022, Iran's Revolutionary Guards seized two Greek oil tankers in Arabian Gulf probably as a "punitive action" against Athens over the confiscation of Iranian oil by the United States from a tanker held off the Greek coast.[199]

These threats are particularly relevant especially following the Russian invasion of Ukraine and the European attempts to strengthen its energy ties with Middle Eastern suppliers to overcome its dependence on Russian oil and gas. Indeed, if the seas around the Arabian Peninsula become a conduit for a growing share of vital energy shipments to Europe, Gulf maritime security will become a strategic interest for the EU. Furthermore, the CMP in the waters of the Gulf allows the Union to achieve even more strictly geopolitical objectives. Gulf countries are not in a position to provide maritime security around the Strait of Hormuz and the Arabian Sea on their own and they continue to argue that the area is of global interest and therefore they should not be the sole actors responsible for maritime security. Given this, the risk is that Gulf actors will invite more and more international partners — including rivals of the U.S. and Europe, such as China and Russia — to patrol the waters. A more significant European presence may deter regional actors from such moves.[200]

***Cyber piracy***

Despite the declining numbers and efficiency of international anti-piracy missions, commercial ships still remain a risky target. Pirates have in fact demonstrated their ability to revise their modes of operation in response to maritime industry behaviour and the strategies of coastal states. In this perspective, the Gulf of Guinea is a perfect example. Before 2010, piracy in the Gulf was limited to coastal area less than 30 nautical miles from shore. As ships kept their distance from shore, the pirates improved theirs range of operation with the use of mother vessels but also, very quickly, with new capacity to operate their skiffs without mother vessels out to 100-120 nautical miles from shore, improving their endurance, safe sailing ability and communication to connect with their targets.[201]

It is therefore probable that the adaptability of pirate techniques will also extend to the cyber domain, especially considering the growing digitization and digital dependence of vessels. A clear indication

[198] Edwards R. (2021), "Iran's strategy of state piracy menaces Middle East oil lanes", *Arab News*, https://www.arabnews.com/node/1788396/middle-east
[199] N.A. (2022), "Iranian forces seize two Greek tankers in the Gulf: State media", *Al Jazeera*, https://www.aljazeera.com/news/2022/5/27/greece-protests-piracy-after-tankers-seized-in-gulf
[200] Bianco C. & Moretti M. (2022), "Europe's role in Gulf maritime security", *Middle East Institute*, https://www.mei.edu/publications/europes-role-gulf-maritime-security
[201] Morizur F. (2020), "Sea Piracy in 2025: Piracy 2.0 ?", *The Maritime Executive*, Sea Piracy in 2025: Piracy 2.0? (maritime-executive.com)

in this sense is the April 2020 attack to the container ship Fouma when sailing inbound to Guayaquil, Ecuador. The pirates opened around 15 containers that were loaded onboard looking for high value goods.[202] Today, there is no official record on the total number of cyberattacks on the industry as shipping companies are reluctant to reveal data due to potential reputational damage. Despite this, it is clear that the prevalence of cyber piracy is growing; even the US coast guard has issued safety alerts for a number of cyber threats. As said by Newman, "*most maritime pirates are no longer just sailing the seas looking for vessels to board and rob. Instead, they are sitting at computers in some office thousands of miles away*".[203]

Vessels are equipped with a whole range of electronic navigation, command-and-control systems interconnected to the global internet via satellite so there are many access routes on a vessel for cyber pirates to access, pillage data, and take control of systems. These include all the points where connected devices and systems intersect and interact with employees using employer's laptops, tablets and mobile phones to share operational manuals and chart updates. These access points radiate via many devices to application groups and onwards to service sectors and locations, affecting supply chains, headquarters, ports, terminals and ships.[204]

ECDIS (Electronic Chart Display and Information System) can be compromised to modify files and insert malicious content in order to take over the whole INS (Integrated Navigational System) or display the vessel in a false position. In this way, a cyberattack can mislead a ship as, for example, in 2016 when two naval ships were misdirected in the Persian Gulf. Another example happened in February 2017 when cybercriminals took control of the navigation systems of a German-owned 8250 TEU container vessel. The crew attempted to regain control and had to bring IT experts on board to solve the situation. The case serves as a "pre-warning" about hackers' abilities to gain control over the vessels to carry out, for instance, kidnap and ransom.[205]

The Global Navigation Satellite System (GNSS) is vulnerable to jamming and spoofing activities of state and non-state actors. Jamming is the deliberate transmission of signals on frequencies used by GNSS in an effort to prevent receivers from locking-on to authentic GNSS Signals. It requires relatively little technical knowledge and can be conducted by merely drowning out genuine signals with random or disruptive noise. Spoofing refers to the transmission of simulated false GNSS satellite

[202] Morizur F. (2020), "Sea Piracy in 2025: Piracy 2.0 ?", *The Maritime Executive*, Sea Piracy in 2025: Piracy 2.0? (maritime-executive.com)
[203] Newman N. (2019), "Cyber pirates terrorising the high seas", *Institution of Engineering and Technology*, https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/
[204] *Ibidem*
[205] Androjna A. et al. (2020), "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering*, 8,776

ephemeris and timing information which coerces the victim receiver into calculating incorrect positioning and, in some cases, timing information. While navigation systems sound alarms when they recognize jammers, spoofing systems create false signals that confuse even state-of-the-art GNSS systems, leading to more severe consequences.[206]

In 2017, the incident at Gelendzhik Airport received attention in international media. At least 20 vessels in the vicinity of the Black Sea Novorossiysk Commercial Sea Port reported that their AIS traces erroneously showed their position as Gelendzhik Airport, around 32 km inland. That led to informed speculation that the incident could be attributed to Russian testing of satellite navigation spoofing technology.[207]

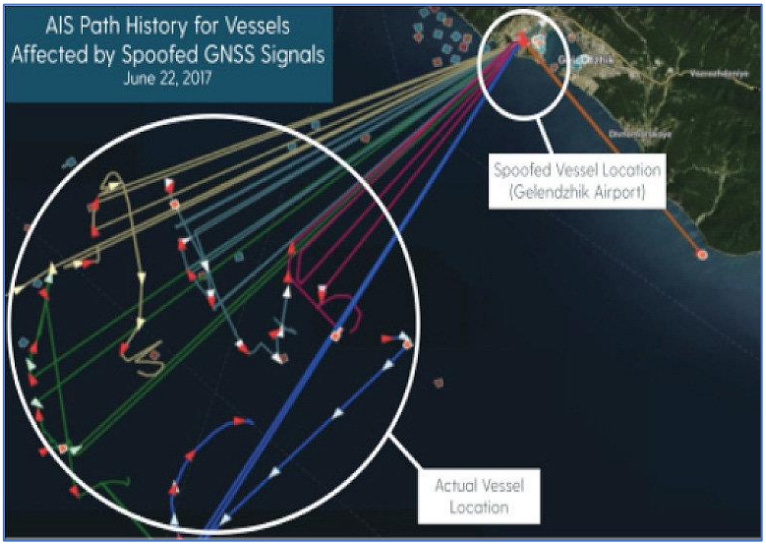


*Figure 23: GNSS Spoofing at Gelendzhik Airport. Source: C4ADS*

In another event, in July 2019, a British oil tanker, the Stena Impero, was seized by Iranian forces after being spoofed to cause the vessel to shift its course into Iranian waters. Today, many of the shipping companies operating in the region have also instructed their vessels to transit Hormuz only at high speed and during the daylight hours.[208]

[206] Androjna A. et al. (2020), "Assessing Cyber Challenges of Maritime Navigation", *Journal of Marine Science and Engineering*, 8,776
[207] Hambling D. (2017), "Ships fooled in GPS spoofing attack suggest Russian cyberweapon", New Scientist, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/
[208] Wiese Bockmann M. (2019), "Seized UK tanker likely 'spoofed' by Iran", *Lloyd's List*, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

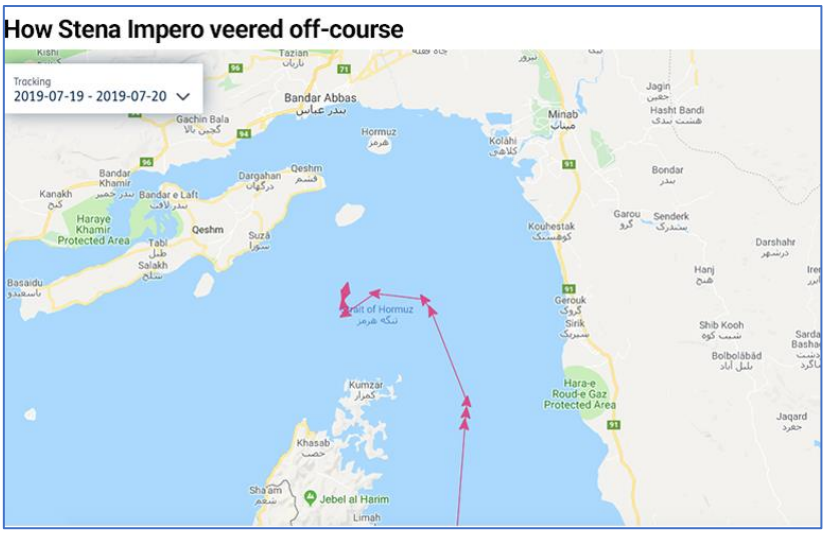


*Figure 24: GNSS Spoofing Stena Impero. Source: Lloyd's List*

Even in Italy an AIS (a critical safety system designed to provide a ship's position and course to neighbouring ships to prevent collision ) base station experienced a ship-spoofing situation near Elba Island, when 870 different vessels appeared in an area of 28 × 21 nautical miles with different routes and speeds, rendering the monitoring of the maritime traffic in the area impossible and impacting real vessel transmissions.

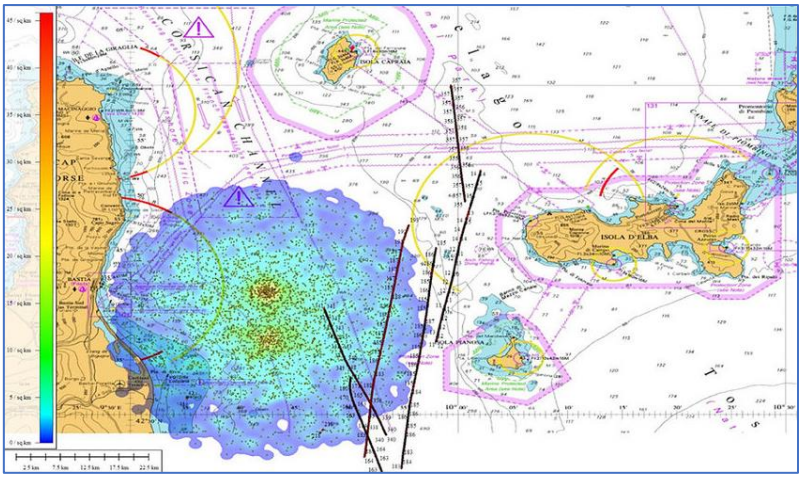

*Figure 25: AIS spoofing -shipping density near Elba Island. Source: Androjna et al.*

### *Information sharing and Maritime Situational Awareness*

Due to their low-level and dispersed nature, hybrid threats such as those just described can only be fully recognized by bringing together the information about occurrences of disruptions, which individually may seem minor but are part of a larger whole, creating situational awareness. The EU Maritime Security Strategy defines the integration of different data sources in the maritime domain on the basis of existing national and international law as a key task, resulting in a better understanding

of what is happening at sea. "*The more information is aggregated and integrated, the more complete is the maritime picture created and more value is delivered to the operational end-users, in a cost efficient way*".[209]

The concept of Coordinated Maritime Presence that the Union is implementing in the Gulf of Guinea and in the Western Indian Ocean is based precisely on the sharing of information and the achievement of Maritime Situational Awareness among the Navies involved. At the European level, in addition to this successful example, there is another initiative in this perspective. In 2010 the European Commission launched the Common Information Sharing Environment (CISE) initiative with the aim of creating an organizational and legal environment to allow the sharing of maritime information between seven sectors (transport, environmental, fisheries control, border control, general law enforcement, customs and defence). Since 2019, CISE has been in a transition phase in which various stakeholders (EDA, EEAS, EFCA, EMSA, Frontex and SatCen) have been in charge of ensuring a coherent evolution of the project and gradually reaching a fully operational network. In this regard, with the funding of Horizon 2020, some stakeholders, including the Italian Navy, have developed the ANDROMEDA project to unlock the capabilities of the CISE, improving the models for the exchange of maritime data and extending its scope to the land component.[210]

In parallel with the European initiative, the Italian navy has also developed its own software for sharing information, called "Service-oriented infrastructure for MARitime Traffic tracking (SMART)", currently evolving to the SMART FENIX release (as of 2018), with more tools and an advanced user interface. The software is at the basis of the Virtual Regional Maritime Traffic Centre (V-RMTC), a virtual network connecting Maritime Operation Centers of member which make possible to share among participants selected unclassified information related to merchant shipping.

The V-RMTC initiative was launched by the Italian Navy at the 5th Venice Regional Seapower Symposium edition (2004), recording the common will and urge to improve the situational awareness of the maritime domain and merchant traffic in the Mediterranean Region. Based on this wide support, the Italian Navy started a technical analysis to find out a way to connect all Navies through a dedicated network, where to exchange unclassified information and data about merchant shipping, on a "push/pull" policy. In 2006, seventeen Navies (Albania, Croatia, Cyprus, France, Greece, Italy, Israel, Jordan, Malta, Montenegro, Portugal, Romania, Spain, Slovenia, Turkey, UK, USA), belonging to

[209] Council of the European Union (2014), *European Union Maritime Security Strategy*, https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf
[210] Marina Militare, *Progetti Europei*, https://www.marina.difesa.it/cosa-facciamo/per-la-difesa-sicurezza/operazioni-in-corso/Pagine/progetti_europei.aspx

the Mediterranean and the Black Sea, adhered to the Initiative and signed the Operational Arrangement (OA). In 2009, the Community agreed unanimously to federate with compatible Maritime Surveillance Systems, the Brazilian Navy Surveillance System (SISTRAM) and the Singapore Navy Surveillance System (OASIS), so in 2010, evolving in a Trans-Regional Maritime Network (T-RMN).[211]

The V-RMTC, through the years, has proved to be an effective instrument that, while enhancing the Maritime Situational Awareness, also strengthens mutual trust, builds confidence among shareholders and allow to create synergies by sharing information and resources. The most valuable achievement is that the Operational Arrangement guarantees that the information shared would remain within the Community and cannot be released outside this circle; furthermore, the members have no obligation on what, and when to share their own information and data, but everybody can receive back the full maritime picture. The V-RMTC model has indeed become an actual model for maritime traffic data exchange, being also applied from 2007 (on dedicated servers, managing different stockpile of data) within the "5+5" community (North Mediterranean countries: France, Italy, Malta, Portugal, Spain; South Mediterranean countries: Algeria, Libya, Mauritania, Morocco, Tunisia) and off the Lebanon coast (thanks to a dedicated agreement, V-SRMTC).[212]

Developing Situational Awareness as a prerequisite for decision-making superiority is one of the six points identified to fully implement the Italian Mediterranean Defense and Security Strategy. In this sense, it is appropriate to capitalize on what is already available at the government level and proceed to achieve the full operation of the Integrated Interministerial Device for Maritime Surveillance (DIISM). This is a project launched in 2007 by the Presidency of the Council of Ministers in order to have an integrated organization of Maritime Surveillance for the management of all the information, collected on the sea by the various dicasteries, and through a single Operations Center - located at the Military Operations Center (COMM), used up to now, albeit with excellent results, only in specific cases and for inter-agency operations limited in time.[213]

[211] Marina Militare, *Virtual Regional Maritime Traffic Centre & Trans Regional Maritime Network*, https://www.marina.difesa.it/EN/facts/Pagine/vrmtc_trmn.aspx
[212] *Ibidem*
[213] Italian Ministry of Defense (2022), Strategia di Sicurezza e Difesa per il Mediterraneo 2022

## 3.3 Illegal immigration and borders control: the role of digital technologies and AI

***The relevance of the management of illegal migratory flows for Italy and the EU***

Alongside the protection of critical submarine infrastructures and the security of maritime trade, the waters of the Mediterranean present another fundamental element for Italian and European foreign policy, namely the fight against illegal immigration. In this context, the macro-region of the enlarged Mediterranean is strategic not only because the phenomenon occurs mainly in the waters of the Mare Nostrum but also because, as can be seen from the figure 26, the majority of migrants arriving on the Italian coasts come from the countries of the region.

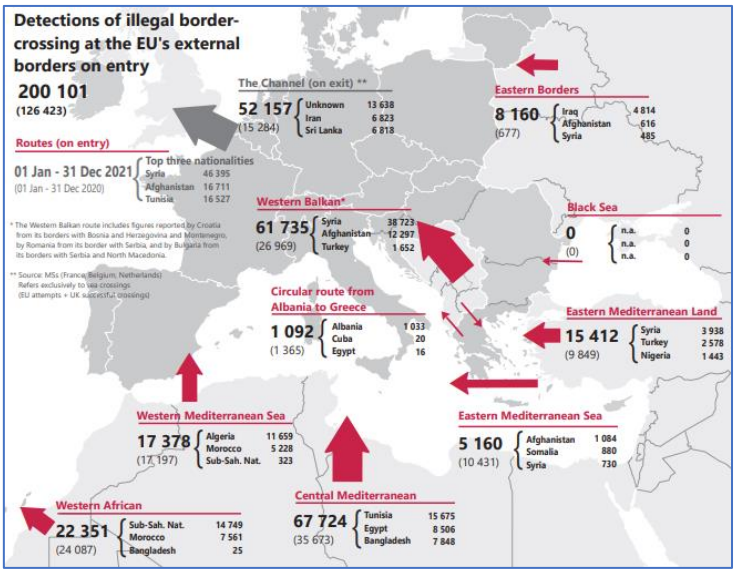


*Figure 26: EU Illegal border-crossing in 2021. Source: FRONTEX*

Migration, asylum and border control policies and systems have been gradually integrated across the EU over at least the last two decades. The roles of the European Commission and the European Parliament as co-decision makers on migration policy have grown since the enactment of the Maastricht Treaty in 1993 and the introduction of the pillar structure. This initiated an ongoing 'communitarization' process in regards to migration that was further strengthened by the Treaty of Amsterdam, entered into force in 1999, and the Treaty of Lisbon, entered into force in 2009.

Regarding the European border regime, the Dublin Conventions represent the current cornerstones. Dublin system established the principle that asylum applications and the legal status of 'third-country nationals apprehended in connection with the irregular crossing of an external border' must be managed in the first country of entry. The system just described, despite the establishment and

strengthening of the mandate of FRONTEX to help and coordinate member states in border policies, therefore puts particular pressure on border countries, including Italy, for which the issue in recent years has also become increasingly central to domestic politics.[214]

***EUROSUR, drones and maritime border surveillance***

As previously mentioned, border control is one of the areas on which information is shared in the CISE. Situational Awareness constitutes one of the founding elements of the European approach to the management of borders and illegal immigration. The clearest example in this sense is EUROSUR. Established in 2013, the European Border Surveillance system (EUROSUR) is a framework for information exchange and cooperation between Member States and Frontex to improve situational awareness and increase reaction capability at the external borders. It aims to prevent cross-border crime and irregular migration and to contribute to protecting migrants' lives. Each Member State has a National Coordination Centre (NCC), which coordinates and exchanges information among all the authorities responsible for external border surveillance, as well as with other NCCs and Frontex. The NCC maintains the national situational picture providing an overview of the situation at its external border, including the events taking place and assets deployed, as well as relevant background information and analysis. Through this informations, integrated with the ones collected from satellites and other surveillance tools used by the European Maritime Safety Agency and the EU Satellite Centre, Frontex maintains a European situational picture on the situation at European borders and the pre-frontier area. This way, EUROSUR enables the Member States to rapidly exchange information, ensure necessary cooperation and offer a joint response to challenges.[215]

A large part of the information that contributes to EUROSUR's situational awareness comes from the use of drones. Since 2016, there has been a huge increase of the use of UAVs in maritime surveillance activities by Frontex in order to control pre-frontier areas and enhance situational awareness to prevent the migratory flows by acting as an early warning mechanism. Drones have operational advantages as they are able to lower personnel costs and are more expandable as they can stay airborne much longer than a human crew, as well as carrying the necessary technology for monitoring areas and detecting suspicious vessels, for example, infrared cameras, mobile phone jammers, thermal

[214] Fragapane S. & Minaldi G. (2018) "Migration policies and digital technologies in Europe: a comparison between Italy and Spain", *Journal of European Integration*, 40:7, 905-921

[215] European Commission, *Eurosur*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/border-crossing/eurosur_en

imagining devices and video cameras.[216] In 2021, Frontex signed contracts to enhance aerial surveillance amounting to a total of € 84.5 million and conducted 468 aerial surveillance flights.[217]

In parallel to this investment and deployment of drones, the EU Member States decided to cease the maritime patrols, as it happened in the case of the EUNAVFOR MED Operation Sophia, which has replaced them with the use of long-range drones (the agency commenced to use Italian Air Force Predator drones for this mission in 2018). The operations involving drones are deployed in cooperation with third countries from the south of the Mediterranean which are normally migrants' place of origin or transit countries, such as Libya and Turkey. The agreements and policies implemented to contain migrants imply the interception of vessels by the coastguard of these third countries, who send back the migrants to the coast from where they have departed. The informations arrived at these countries through the Seahorse Mediterranean Network, a cooperation programme to exchange information in the Mediterranean area, signed by Spain, Italy, France, Malta, Cyprus, Portugal and by North African countries within the European Border Surveillance System (EUROSUR) framework. In this way, the agency externalizes the actions and interventions linked to the interception and return of migrants.[218]

The growing use of drones by FRONTEX also has an economic and strategic impact for Italy, which holds 30% of the shares in the defense company Leonardo through the Ministry of Economy and Finance. Unmanned surveillance is a core business for Leonardo, currently one of the only (if not the only) companies in Europe offering a complete UAV surveillance service package, including the self-developed aircraft, adapted sensor payload and a mission control system with a fully equipped and manned ground station. One of the most used drones in maritime surveillance operations is Leonardo's Falco EVO, which is a tactical system, with about a 12-meter wingspan and close to 700-kilogram maximum takeoff weight. This is a proven system with lots of redundancy and a robust data link, which can include imagery and video. Its data dissemination system allows to immediately share the collected information with the ground team and the relevant authorities. Leonardo is also working to not be outdone by the recent demand for MALE (Medium Altitude Long Endurance) drones. These drones can fly at altitudes up to 30,000 feet (9,000 meters) and have a range of more than 200 kilometres, making them highly suitable for the types of surveillance missions embarked upon over large bodies of open water. In 2020 Frontex signed a framework contract with Germany's Airbus DS

[216] Marin, L., & Krajcíková, K. (2016), "Deploying drones in policing European borders: constraints and challenges for data protection and human rights", In A. Zavrsnik (Ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance,* pp. 101-127

[217] Puntas I.B. (2022), *The use of drones for maritime surveillance and border control*, Centre Delàs d'Estudis per la Pau, Working Paper

[218] *Ibidem*

Airborne Solutions GmbH and Israel's Elbit Systems Ltd. to provide aerial surveillance support with MALE RPAs. For this reason, Leonardo is developing the "Skydweller", which will be a solar-powered UAV with unprecedented endurance and capable of carrying large payloads.[219]

On the other hand, despite the operational and economic advantages, the use of drones in maritime surveillance operations in support of EUROSUR poses many challenges from a humanitarian point of view. Indeed, vessels that are capable of helping migrants and asylum seekers are replaced by drones that can only observe. Many analysts have seen this as a deliberate move by FRONTEX in order to not have the obligation to intervene neither rescue them. Furthermore, the collaboration with the North African authorities in intercepting and bringing back the boats of migrants before they enter European waters is considered a violation of Article 33 of the Geneva Convention Relating to the Status of Refugees, which states the principle of *non-refoulement*.[220]

***IT systems in border management***

Alongside EUROSUR, the European border control framework makes use of a series of IT systems that allow the immediate sharing of information between Member States. One of them that mostly concern Italy, as a first arrive country, is EURODAC. The European Dactyloscopie is the European database of fingerprints for asylum seekers and people apprehended while illegally crossing an external border of the European Union. By comparing fingerprints, Member States can verify whether an asylum seeker or a foreign national who is illegally on their territory has already lodged an application in another Member State or whether an asylum seeker has entered EU territory illegally.

The two other large-scale IT systems on which the European border regime is based are the Schengen Information System (SIS) and the Visa Information System (VIS). The SIS is a common centralized information system that was established in 1995 and renewed in 2006. The second-generation Schengen Information System (SIS II) has been operational since 2013 registering biometric information as well as personal data and data on goods and possessions. Although the objectives of the system are related to public order and security in general, its main purpose is easily identified as combatting irregular immigration. Indeed, most of information stored in the system concerns third

[219] Gutierrez P. (2022), "Putting Unmanned Systems on Task Over the Mediterranean", *Inside Unmanned Systems*, https://insideunmannedsystems.com/putting-unmanned-systems-on-task-over-the-mediterranean/

[220] Puntas I.B. (2022), *The use of drones for maritime surveillance and border control*, Centre Delàs d'Estudis per la Pau, Working Paper

country nationals to be refused entry to, or the right to stay in, the Schengen Area, and lost and/or stolen identity documents.[221]

SIS II is linked to the Visa Information System which is the primary instrument of the common visa policy. VIS contains information, including biometric information, on visa applications by citizens of third countries who need a visa to enter the Schengen area. The VIS makes it possible to check if fingerprints scanned at the frontier-crossing match those recorded at the consular posts where the visa was issued.[222]

Furthermore, in November 2017, the Council adopted a regulation for an entry/exit system. This system, operative since 2023, will register information on the entry, exit and refusal of entry of non-EU nationals crossing the external borders of the Schengen area, automatically calculating the authorised stay of each traveller, ensuring systematic and reliable identification of overstayers and strengthening internal security and the fight against terrorism and other serious crime by allowing law enforcement authorities access to travel history records.

In May 2019, the Council adopted two regulations establishing a framework for interoperability between these EU information systems. This new interoperability should become operational by the end of June 2024 and provide a single interface for searches, as well as a biometric matching service to facilitate identification.[223]

Despite, according to the Schengen Code, Member states are required to systematically check all people crossing the EU's external borders in the relevant databases to ensure that those people are not a threat to public policy, internal security or public health, a study by Fragapane and Minaldi clearly shows how in the past years Italy and Spain have used this IT systems based on their own, diverging, strategic priorities in migration and border policies. In regard to EURODAC, both countries pursued similar goals in an attempt circumvent a system that they deemed unfairly burdensome, as demonstrated by the very low numbers of Eurodac entries connected to irregular border-crossers. In response to the Commission's recommendations to conduct systematic checks using VIS data in order to identify visa overstayers for the purpose of return, Italy and Spain confirm they do not aim to reduce the overall presence of irregular residents who are mostly absorbed into the flourishing informal economy. On the contrary, the high rate of implementation of SIS II in both countries represents the securitization of migration policy, as SIS II aims to not only effectively manage borders

[221] Fragapane S. & Minaldi G. (2018) "Migration policies and digital technologies in Europe: a comparison between Italy and Spain", *Journal of European Integration*, 40:7, 905-921
[222] *Ibidem*
[223] European Council, *Strengthening the EU's external borders*, https://www.consilium.europa.eu/en/policies/strengthening-external-borders/

but also to prevent and counteract crime and terrorism.[224] For the purposes of this study, this demonstrates how the use of digital systems in the management of illegal immigration is a relevant aspect in relation to Italian national interests and Italian domestic and foreign policy.

## 3.4 Counterterrorism and international security: Cyber-Jihad and the digital evolution of counterterrorism strategies

***An evolving terrorist threat in the Wider Mediterranean***

The fight against international terrorism is one of the most underlined points in the Italian Security and Defense Strategy for the Mediterranean. With regard to Islamic terrorism, the 2021 report of the Italian intelligence services paid particular attention to the decentralization of the command and control structures of the Islamic State and Al Qaeda. In this perspective, in addition to highlighting the restructuring of the Islamic State in Iraq and Syria, the document confirmed the African continent as an information priority. According to the International Institute for Counterterrorism, "*Africa is radical Islam's new heaven*". The reasons for the prosperity of radical Islamic organizations are varied: the existence of large influential Muslim communities, lack of governability, weak and corrupt security services, weak intelligence infrastructure in most countries, mostly poor populations susceptible to Islamic propaganda regarding social mobility and radicalization.[225] The main threats to Italian national interests come from the conflict between the two main Sahelian terrorist groups linked to Al Qaeda and Daesh, from the expansion of these groups towards the Gulf of Guinea and from the Al Shabaab's consolidation of the control on Somali rural areas. These developments are accompanied by a still worrying picture regarding the viral spread of jihadist propaganda and the mechanisms for financing terrorism. In both fields, terrorists have shown a high ability to adapt to new technologies and, therefore, cyberspace has become a new battleground with governments all over the world in search of a solution with adequate cyber intelligence to confront and destabilize terror infrastructures. [226]

[224] Fragapane S. & Minaldi G. (2018) "Migration policies and digital technologies in Europe: a comparison between Italy and Spain", *Journal of European Integration*, 40:7, 905-921
[225] Azani E. & Doukhan D. (2021), *Global Jihad in Africa: Danger and Challenges*, International Institute for Counterterrorism, p. 2
[226] Sistema di Informazione per la Sicurezza della Repubblica (2022), Relazione Annuale sulla Politica dell'Informazione per la Sicurezza, pp. 77-82

### *Cyberspace as a field of action for terrorist groups*

While at first sight the collapse of the "caliphate" in Syria and Iraq, the death of Abu Bakr al-Baghdadi in 2019, and the decrease in the number of jihadist attacks in the West since 2017 could suggest violent extremism has entered a phase of relative decline, the web remains a crucial means for radical propaganda, mobilisation, planning attacks and financing. Even though the jihadist threat has seemingly declined, the danger exists of the internet being an environment where radical messages can survive and even prosper. Online militants and sympathisers are still difficult to counter and continue to represent a critical part of the extremist threat.[227] Indeed, cyberspace can perform different functions of varying nature and degree of violence for extremists and terrorists.

The most direct threat could be a cyberattack launched trough the Web. So far terrorist groups have shown neither the intention nor the capability to launch destructive cyberattacks, but it is perhaps natural to consider the possibility that terrorist groups such as the so-called Islamic State (IS) or al-Qaeda could launch these type of attacks, even on a large scale, in the future.[228]

Beyond the direct attack through cyberspace however the digital sphere provides a variety of more indirect but equally dangerous threats.

- One of them is the use of the internet for the provision of operational instructions: information for carrying out attacks with explosive devices or with other weapons or tools, but also instructions about operational security (in particular, on how to avoid detection offline and above all online). In this field, Telegram, generally criticised for its reluctance to regulate extremist content, has played a major role in recent years. On this free platform, unlike in other messaging services, users can benefit from encrypted messages, remarkable file-sharing capabilities, and the opportunity to publish material in various file formats.[229]

- Another significant threat is represented by hacking and so-called "doxing" (or "doxxing"), that is the practice of gathering and disclosing an individual's personally identifiable information (PII) online for different purposes, particularly with the intent of inflicting harm. For instance, in April 2015 Ardit Ferizi provided support to the jihadist organisation by transmitting PII of US and

[227] Magri P. (2019), "Introduction", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan
[228] Marone F. (2019), "Violent Extremism and the Internet, Between Foreign Fighters and Terrorist Financing", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan
[229] Clifford B. (2018), "Trucks, Knives, Bombs, Whatever': Exploring Pro-Islamic State Instructional Material on Telegram", *CTC Sentinel*, vol. 11, no. 5, pp. 23-29

Western European citizens he had obtained by illegally accessing customer records databases of a US company.

- Cyberspace can also play a key role in the recruitment of extremists and terrorists. Indeed, despite offline interactions in physical networks are often still essential especially in the most advanced stages of the processes of radicalisation, today the role of the Web for extremist radicalisation and recruitment is crucial. Extremist "virtual planners" (also known as "virtual entrepreneurs") can target and guide unaffiliated radical sympathizers remotely, via the Web, in particular through the use of encrypted application.[230]

- Finally, the internet can play a significant role in financing terrorist activities mainly thanks to its relatively high level of anonymity and ease of use. On one hand, extremist or terrorist groups can solicit funds directly from their supporters through electronic transfers of money, such as online fundraising activities or the participation of non-profit organisations and charities.[231] In 2021, Spain reported that most of the funds channelled from the country to jihadist groups was raised through online crowdfunding campaigns.[232] On the other hand, other methods do not imply the consent of the source provider (whether it is informed or based on deception). Cybercrime can be a relevant method in this respect. For example, part of the funding for the devastating jihadist attacks in London on July 2005 derived from credit card fraud.

***Jihadism and Social Media***

In addition to these threats, the primary use that jihadist terrorist groups make of cyberspace is for propaganda, especially following the rise of social media. As emphasized by Hoffman Bruce, terrorism and media are joined together in an intrinsically symbiotic relationship, each feeding off, and utilizing the other for its purposes. Any terrorist operation without the media has limited effects on the targeted audience and one significant objective of terror groups is to get maximum publicity for their terrorist activities. The terrorist always wants to communicate the revolutionary or divine messages to a broad audience, and, for this reason, they have recognized the potential of new mass

[230] Vidino L., Marone F., Entenmann E. (2017), *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West*, , ISPI in partnership with the International Centre for Counter-Terrorism – The Hague (ICCT) and the Program on Extremism at George Washington University

[231] Başaranel B.U. (2017), "Online Terrorist Financing", in M. Conway, L. Jarvis, O. Lehane, S. Macdonald and L. Nouri (eds.), *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam, IOS Press, pp. 95-108

[232] Europol (2022), *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg

communication technology.[233] For instance, a study, published by the Journal of Terrorism Research in 2014, clearly explains how the adoption of social media technology has been the main factor in facilitating the overall rise of the terrorist web presence in Sub Saharan Africa. The figure 27 shows how the advent of social media was immediately identified by sub-Saharan terrorist groups as a strategic asset that could be exploited. While the trend for the creation of new HTML sites remained almost unchanged from 1994 to 2013, the rate of creation of social media has soared since 2008, significantly contributing to the growth of the virtual presence of terrorist groups.[234]

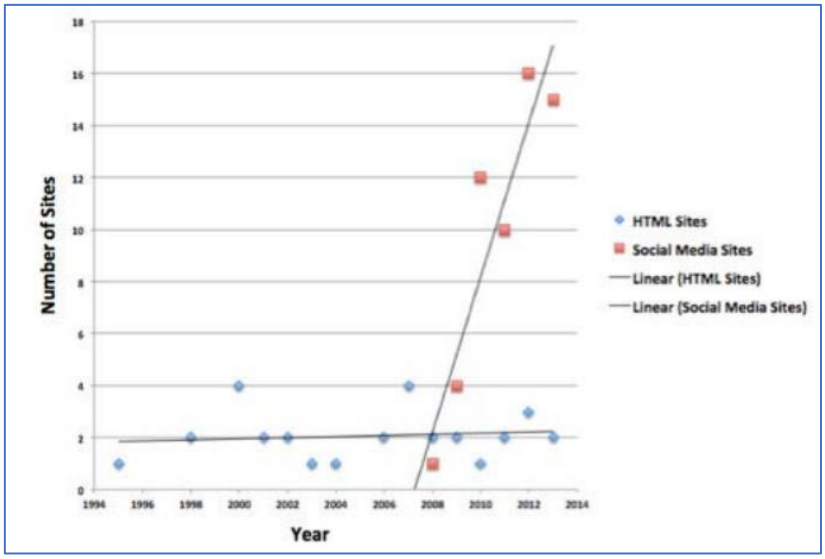


*Figure 27: Number of HTML and Social Media sites linked to jihadist terrorism created from 1994 to 2013 in Sub Saharan Africa. Source: Journal of Terrorism Research*

Social media have proved particularly well-suited for terrorist propagandizing and recruiting for several reasons. First, social media enables terrorists to communicate radicalizing messages to a far wider circle of potential adherents than they could have reached with traditional media. If, previously, radicalization required personal contact with someone who could provide materials, ideological grooming, and connections to wider jihadist networks, today, social-media platforms like Twitter, Instagram, Facebook, and YouTube, offer the ability to instantaneously convey one's message to users around the world, often in the form of captivating images or video. In this perspective, social media allows terrorists to recruit and propagandize across borders, in a way that 20th-century technology never allowed.[235]

[233] Ogunlana O.S. (2019), "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies", *Journal of Strategic Security*, Vol. 12, No. 1
[234] Bertram S. & Ellison K. (2014), "Sub Saharan African Terrorist Groups' use of the Internet", *Journal of Terrorism Research*, vol. 5, n. 1 (Special Issue)
[235] Hamilton L.H. & Kean T.H. (2018), *Digital Counterterrorism: Fighting Jihadists Online*, Bipartisan Policy Centre, Task Force on Terrorism and Ideology

Furthermore, on social-media platforms all content looks more or less the same. Production value serves as the most readily available indicator of quality, and terrorists have grown adept at using desktop software to turn out propaganda materials that are as polished as traditional media. In this perspective, a salient example is provided by the Islamic State. As underlined by an analysis by the Program on Extremism at George Washington University, IS differs from previous jihadist organizations for its professional-quality productions and its ability to disseminate this content through social media.[236] Its level of sophistication has proven unprecedented. Thanks to the technological and communication skills of some of his militants, it has built and institutionalised a vast and complex propaganda machine capable of attracting at least spectators, if not active sympathizers and militants, all over the world.[237]

Another advantage is that social media enables terrorist to engage directly, and publicly, with more credible figures, hijacking those figures' visibility to amplify the terrorists' own messages. For example, responding to a post by an influential Western politician allows them to both exploit his entire audience and interact with him in a way that is impossible in the real world.[238]

The final reason why social media is such an effective amplifier for terrorists is the power with which platforms' algorithms connect users to content that resonates with their existing inclinations and preferences. Users are ensconced in a "filter bubble", created by algorithms designed to give them what they want, and they may rarely, if ever, encounter any opinion with which disagree. This effect tends to become more pronounced over time: As the platforms acquire more information about the user's exact preferences, the algorithms become progressively better at anticipating the user's desires. "*Users become enmeshed in feedback loops that confirm, and therefore strengthen, their pre-existing beliefs about the world—their hatreds, their fears, their preferred accounts of the causes of their grievances, and their sense of what is to be done*."[239]

[236] Hamilton L.H. & Kean T.H. (2018), *Digital Counterterrorism: Fighting Jihadists Online*, Bipartisan Policy Centre, Task Force on Terrorism and Ideology
[237] Marone F. (2019), "Violent Extremism and the Internet, Between Foreign Fighters and Terrorist Financing", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan
[238] Hamilton L.H. & Kean T.H. (2018), *Digital Counterterrorism: Fighting Jihadists Online*, Bipartisan Policy Centre, Task Force on Terrorism and Ideology
[239] *Ibidem*

### *Jihadist online propaganda in the Wider Mediterranean*

In the MENA region, jihadist propaganda can count on a vast audience of young people dissatisfied with the outcome of the 2011 Arab Spring and with regional political and economic instability.[240] In this context, the Islamic State focuses many of its online propaganda efforts on the two Middle Eastern theaters where the group is still present in the field, i.e. Iraq and Syria. In Iraq pro-Islamic State media not only described the Iraqi state as a disunited entity (contrasted with the alleged unity of the IS) but even as a malicious actor intent on harming Sunnis. Jihadist media referred to two instances of high civilian casualties in Sunni areas, claimed to be the result of operations by Iraqi security forces, pro-Iranian militias, and allied tribes. This sectarian messaging is meant to drive a wedge between the Sunni constituency from which the Islamic State wants to recruit and general society.[241] In Syria, on the other hand, the efficiency of the Islamic State's propaganda was clearly seen in the case of the IS attack to the Ghuwayran Prison in al-Hasaka, in January 2022. This Syrian offensive was accompanied by close media coverage, specifically by the official Islamic State news media outlet Amaq. Disinformation about the status of the prison was used to undermine trust in the official narrative and to increase solidarity with the prisoners attempting to escape. The profile also called Syrian supporters to arms and asked them to target the SDF (Syrian Democratic Forces) in diversionary attacks throughout eastern Syria. These calls reached an ever increasing audience as followership of all the monitored profiles, accounts, pages, and channels soared during this time period.[242]

In June 2022, researchers found 30 public Facebook pages promoting official al-Shabaab and Islamic State propaganda, resharing "news" updates and promoting central al-Shabaab and Islamic State narratives in the Horn of Africa. This set of Facebook pages classified themselves as blogs, publishers, media personalities and media outlets. They shared al-Shabaab and the Islamic State contents in Somali, Kiswahili and Arabic and posted 850 videos over the two-year period of the ISD investigation, generating some 450,000 views on content. Furthermore, researchers tracked 44,522 profiles supportive of al-Shabaab and the Islamic State which re-shared the content of these Facebook pages across several platforms, including decentralized messaging applications such as Element and RocketChat, and encrypted messaging platforms such as Telegram. This complex network spread key narratives such as al-Shabaab and the Islamic State being an anti-imperial and anti-colonial force

[240] Schori Liang C. (2015), "Cyber Jihad: Understanding and Countering Islamic State Propaganda", *Geneva Centre for Security Policy*, n.1
[241] Al-Tamimi A., Ayad M., Khan N. (2022), *The Terror Times: The Depth and Breadth of the Islamic State Alternative News Outlet Ecosystem Online*, Institute for Strategic Dialogue, pp. 13-15
[242] *Ivi*, p. 18

protecting the interests of Muslims in Somalia, Ethiopia, Uganda, and notably, Kenya. Central to these narratives is a foundational set of tropes that relies on calling out the illegitimacy of the governments currently in power across East Africa, while championing taking up arms to fight their "democracy" and their "elections".[243]

Even in the Sahel and in particular in Mali radicalisation and recruitment by extremist groups is also taking place through social media and messaging platforms. For instance, Katiba Macina's leader, Amadou Koufa, has become known for using channels such as WhatsApp, Facebook, and Telegram to call for members of the Peul (Fulani) community to rise up against the Malian Armed Forces, the G5 Sahel countries, and France's Barkhane forces. Ansar Dine, now part of Jama'at Nasr al-Islam wal Muslimin (JNIM), has adopted social media and messaging technologies to advance their messages. Using Telegram, the group has pushed a narrative of framing itself as the 'good guys', by fighting off foreign oppression, including through releasing photographs such as ones of suicide bombers who carried out an attack on the Timbuktu Airport in 2018.[244]

The risk of jihadist online propaganda obviously does not follow the geographic boundaries of the Islamic world, but also reaches Italy and the European continent. Indeed, social and political events outside the EU have a strong influence on jihadist narratives circulating among European radicalised audiences. For instance, the fate of prisoners linked to IS in Iraq and Syria strongly resonated with jihadists and their supporters.[245] In April 2022, an appeal by the alleged new spokesman of the IS, Abu-Omar al Muhajir, urged the organization's militiamen to ride the wave of the war in Ukraine to carry out attacks in Europe and avenge its long line of slain leaders. Under this perspective, the European scene continues to remain exposed to the threat of those who mobilize autonomously in support of the so-called "global jihad" and the exponential increase in jihadist propaganda activity, both by al-Qaeda and IS, in the aftermath of the Taliban takeover in Afghanistan, assumes particular relevance.[246] In the current scenario, in which social media and the web play a key role in spreading hate messages and fuelling extremist tendencies, the risk is that jihadist propaganda could favor the transition to action of radicalized subjects also on European soil.[247] Countries such as France,

[243] Abdullah M.A., Ayad M., Harrassy A. (2022), *Under-Moderated, Unhinged and Ubiquitous: Al-Shabaab and the Islamic State Networks on Facebook*, Institute for Strategic Dialogue,
[244] Coleman J., Dal Santo E., Vermeesch E. (2020), *The Role Of Social Media In Mali And Its Relation To Violent Extremism: A Youth Perspective*, UN Interregional Crime and Justice Research Institute
[245] Europol (2022), *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg
[246] Sistema di Informazione per la Sicurezza della Repubblica (2022), *Relazione Annuale sulla Politica dell'Informazione per la Sicurezza*, pp. 77-82
[247] Fruganti L. (2022), "Lo Stato islamico torna a minacciare l'Europa?", *ISPI*, https://www.ispionline.it/it/pubblicazione/lo-stato-islamico-torna-minacciare-leuropa-34764

Germany and Britain, in addition to having already been hit by terrorist attacks, also host structured jihadist online activities in their respective languages. Even Italy, albeit with a less worrying picture, records a sleeping but present cyber activity that must be monitored, as evidenced by the IS-related propaganda content in Italian, shared within some telegram channels such as Ghulibati a Rum ("The Conquest of Rome").[248]

***The increasing role of AI and online surveillance systems in counterterrorism***

One element of governments' response to jihadist online propaganda has been counter-messaging: attempting to refute or undercut the messages propagated by terrorist groups and their sympathizers. Those efforts, while laudable in theory, have struggled in practice. The difficulty was linked to a broader challenge in post-9/11 efforts to counter Islamist ideology: Western governments' lack of fluency in the languages, ideas, traditions, history, and mores of the Islamic world. In the Cold War, the battle of ideas was fought largely within the West, between economic and governmental systems that were both the products of Western thought. In the struggle against Islamist terrorism, the arguments that move public opinion draw upon traditions that few Westerns understand, often expressed in languages that few Westerns have mastered.[249] Another defect in this approach lies in the specific nature of the IS. The Islamic State, in contrast to al Qaeda, is less concerned with building support and consent among Muslim populations. Indeed, as underlined by McCants, IS's strategy is to use fear and violence to cow populations into submission, not to win hearts and minds. For that reason, highlighting IS's violence against other Muslims, as the US State Department did in YouTube videos like "Welcome to ISIS Land," did not necessarily undermine the Islamic State's message among its target audiences, but on the contrary furthers the purpose of the Islamic State.[250]

More recently, governments and the social-media platforms themselves have shifted their focus away from competing with terrorists in the marketplace of ideas toward denying terrorists the ability to use prominent platforms for recruiting and propaganda. In the wake of horrific terrorist attacks in Europe in 2015 and 2016, Facebook, Twitter, and Google responded to European pressure by stepping up efforts to remove extremist content from their platforms. They created the "Global Internet Forum to Counter Terrorism," intended to "share technical solutions for removing terrorist content, commission research to inform their counter-speech efforts and work more with counter-terrorism

[248] Mazzoni V. (2019), "Sleeping, but Present: The Cyber Activity Inspired by the Islamic State in Italy", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan

[249] Hamilton L.H. & Kean T.H. (2018), *Digital Counterterrorism: Fighting Jihadists Online*, Bipartisan Policy Centre, Task Force on Terrorism and Ideology, p. 8

[250] McCants W. (2015), The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State, St. Martin's Press, New Yorkp. 137

experts." Facebook relies on different tools, including AI language models to understand text that might be advocating for terrorism, which is often language and group-type specific. Other popular platforms like Twitter and YouTube also rely on AI to quickly remove comments that violate the companies' rules. Twitter reported that three quarters of the 300,000 accounts removed between January and June 2017 were deleted before posting their first Tweet. According to YouTube, more than 150,000 videos have been removed between June and December 2017.[251]

Despite these efforts social media companies are failing to tackle the spread of such content and several countries have sought to adopt national legislation aimed at compelling companies to do more. For example, this can be achieved by regulating how fast content must be taken down and by setting incentives and punishing non-compliance. Germany´s Network Enforcement Act is one of the first examples of national legislation in this sense, followed by the EU regulation on addressing the dissemination of terrorist content online, which compels removal of terrorist content within one hour of receipt of removal notices. Furthermore, law enforcement and counter-terrorism agencies in several countries, as well as within Europol, have begun to using AI to independently identify content related to terrorist propaganda and then report it to online platforms as violations of their terms. For instance, the UK Home Office and ASI Data Science announced in 2018 the development of new technology that leverages machine learning to analyze audio-visual content online to determine whether it could be ISIL propaganda. According to the Home Office, tests have shown the tool can automatically detect such content with 99.995% accuracy.[252]

Beyond just identifying vulnerable individuals, AI can play an even more proactive role in countering terrorism online analyzing users' behaviour and directing them to specific content conducive to countering terrorist narratives. In this perspective, Moonshot, with its innovative "Redirect Method", which was piloted in 2016 with Google's Jigsaw, uses automated risk assessment and NLP to identify vulnerable audiences based on their online search behaviour. For instance, if people are searching for specific content that matches pre-defined indicators, advertisements with positive, de-radicalizing content are triggered and users are redirected to ads and curated videos on a YouTube channel designed to refute IS propaganda. Even the Institute for Strategic Dialogue uses AI-driven social media advertisement tools to counter ISIL narratives online and in 2015 launched a curated counter-

[251] European Commission (2017), *Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda*, Press Release

[252] N.A. (2021), *Countering Terrorism Online With Artificial Intelligence: An Overview For Law Enforcement And Counter-Terrorism Agencies In South Asia And South-East Asia*, Joint Report by UNICRI and UNCCT, p. 31

narrative campaign targeting vulnerable people especially at risk of being involved by ISIL propaganda.[253]

AI can help intelligence activities even offline, as in enhancing the capabilities of national authorities to process large quantities of data in an effective manner, optimizing the necessary amount of human and financial resources allocated for any specific situation. More specifically, AI can be used to extract relevant information, filter, and triage data to help prioritize the analysis of vast sets of data that may identify vital investigative leads. One sector where the application of AI can bring significant benefits is the audio-visual sector. In this context, facial recognition, is one technology that offers considerable promise in terms of being able to analyze video footage to identify persons of interest. INTERPOL operates a facial recognition system that contains facial images received from more than 179 countries.[254] Sources of the Israeli Security Services (Shin Bet) have underlined how the use of AI and Big Data could also significantly help in the identification of the so-called "lone wolves", who carry out terrorist attacks without any connection to terrorist organizations. Artificial intelligence makes it possible to analyze additional information, which is not taken into consideration in the traditional HUMINT and OSINT, which could be fundamental in identifying anomalous behavior indicative of an impending threat.[255]

At the same time, in addition to providing various advantages, AI also poses a series of risks. The accuracy of the forecasting models developed in the field of terrorism remains in doubt as there are multiple different roles in terrorism, and multiple pathways to fulfilling those roles. This means that it is impossible to list definitive indicators of involvement or exclusion from terrorist activities. Accuracy of predictive models can be progressively improved by increasing the quantity of data but, in this case, government agencies, are constrained by several limits based on national regulations, international human rights laws or physical access and technical capabilities, such as the difficulties in the information sharing with foreign countries.[256]

Furthermore, the mass collection and retention of domestic data, needed to use AI, remains a hotly contested point in terms of privacy. The right to data privacy is protected most specifically under Article 8 of the EU Charter and by Article 8 of the European Convention on Human Rights. For both institutions, interference must meet a three-fold criterion of fulfilling a legitimate aim, being

[253] N.A. (2021), *Countering Terrorism Online With Artificial Intelligence: An Overview For Law Enforcement And Counter-Terrorism Agencies In South Asia And South-East Asia*, Joint Report by UNICRI and UNCCT, p. 31
[254] *Ivi*, p. 32
[255] Ganor B. (2019), *Artificial or Human: A New Era of Counterterrorism Intelligence?*, Studies in Conflict & Terrorism, pp. 5-8
[256] McKendrick K. (2019), *Artificial Intelligence Prediction and Counterterrorism*, International Security Department, Chatham House, pp. 13-20

undertaken within a legal framework and satisfying conditions of necessity and proportionality. Predictive AI would rely on analysis of data belonging to the general public to distinguish suspicious from normal behaviour, or to discern trends that might help predict attacks. In this context, the vast majority of data under analysis would be generated by people who are not of interest to intelligence services, and this would render it indiscriminate and therefore inherently disproportionate.[257]

In general, the power to access, collect and store citizens' data brought about by the information age could represent a change in the relationship between states and citizens. In 2014, the report of the Office of the United Nations High Commissioner for Human Rights (OHCHR) on the right to privacy in the digital age observed that "*examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure*". As analyst James Shires argues, the "*ambiguity, imprecision and multivalence" of the term "cybersecurity – particularly the lack of consensus about what constitutes a legitimate security threat in the digital domain – has helped authoritarians legitimise various strategies for achieving their political goals*".[258] This happened with particular rapidity in the Wider Mediterranean, given the vagueness of the legal framework in this regard. In particular, the phenomenon has rapidly taken hold following the Arab Spring of 2011, when local governments have acquired foreign technologies, especially online surveillance software, justifying themselves with the need to prevent the rise of terrorism. Digital surveillance, on the other hand, has been systematically used as a tool to repress dissent and, according to many analysts, has contributed to further strengthening the authoritarian character of those governments.[259]

China is a major supplier of AI surveillance, with a considerable overlap between China's Belt and Road Initiative and AI surveillance — thirty-six out of eighty-six BRI countries also contain significant AI surveillance technology. Experts claim that Chinese companies are working directly with Chinese state authorities to export "authoritarian tech" to like-minded governments in order to spread influence and promote an alternative governance model, but AI surveillance is not solely going from one authoritarian country (China) to other authoritarian states. Rather, transfers are happening in a much more heterogeneous way. China is exporting surveillance tech to liberal democracies as

[257] McKendrick K. (2019), *Artificial Intelligence Prediction and Counterterrorism*, International Security Department, Chatham House, pp. 13-20
[258] Lynch J. (2022), *Iron Net: Digital Repression In The Middle East And North Africa*, European Council on Foreign Relations
[259] *Ibidem*

much as it is targeting authoritarian markets. Likewise, companies based in liberal democracies are actively selling sophisticated equipment to authoritarian regimes.[260]

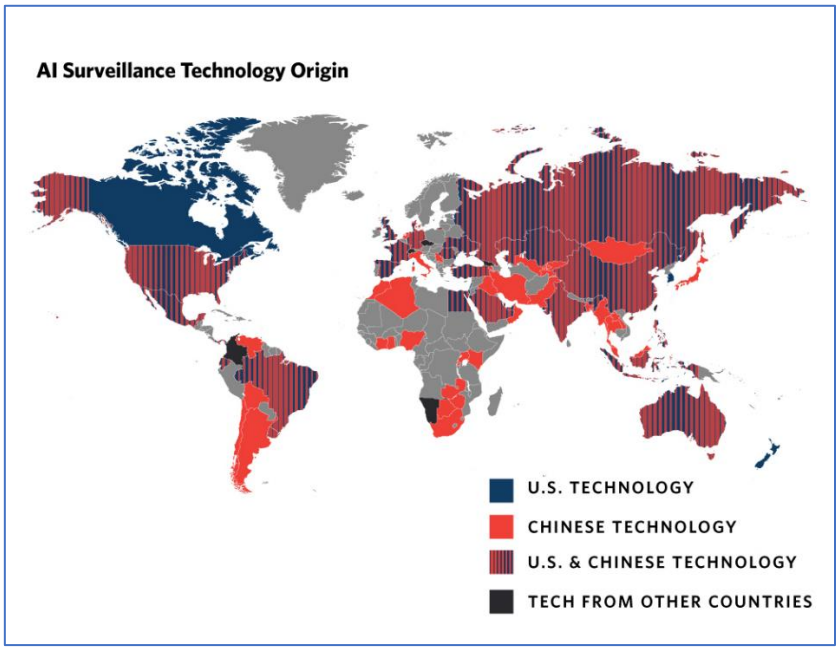


*Figure 28: AI Surveillance Technology Origin : Carnegie Endowment for Peace*

In this context, indeed, the EU acts with a certain ambiguity and "*still has to decide whether tackling digital repression is a core geopolitical interest at the highest political level*".[261] On the one hand, it condemns the repression of dissent and the use of these software for authoritarian purposes, but, on the other, it actively contributes to strengthening the region's digital surveillance ecosystem.[262] This trend is not only limited to AI-related surveillance systems, but rather extends to several initiatives and funding, which have contributed to the repression of dissent in various countries of the Wider Mediterranean. An example is the EU/MENA Counterterrorism Training Partnership 2, which led the European agency CEPOL to collaborate with the authorities of Algeria, Jordan, Lebanon, Morocco, Tunisia and Turkey on cyber security and on the fight against online extremism and terrorism. The skills acquired in this occasion would have been crucial in the repression of internal dissent on several occasions, for instance in street protests against Algerian President Bouteflika in 2019.[263]

[260] Feldtein S. (2019), *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, Working Paper
[261] Głowacka D. et al. (2021), *Digital technologies as a means of repression and social control*, Policy Department for External Relations, Directorate General for External Policies of the Union
[262] Lynch J. (2022), *Iron Net: Digital Repression In The Middle East And North Africa*, European Council on Foreign Relations
[263] Zorloni L. (2021), "L'Europa finanzia anche con aiuti umanitari sorveglianza digitale in Africa e nei Balcani", *Wired*, https://www.wired.it/attualita/tech/2021/10/19/europa-sorveglianza-digitale-africa-balcani-cepol/

The problem of providing such surveillance tools to the countries of the region has also concerned Italy on several occasions. In the early 2010s, Canadian NGO Citizen Lab revealed that several Arab governments were employing Italian firm Hacking Team to track the activities of their political opponents, human rights activists, and others. This spyware has also been employed by the Ethiopian government against dissidents[264] and Egyptian authorities may have used this software to surveil Italian PhD student Giulio Regeni prior to his torture and murder in January 2016.[265] In the same year, Italy barred the company from exporting its products outside the EU but, by 2019, the owner of Hacking Team was marketing KRAIT, a surveillance tool described as "a match made in heaven for human rights abusers" which can take over Android devices to surveil them without requiring their owners to click on a link.[266] In this context, Italy has the need to coordinate with European partners and stakeholders to arrive at a legal framework useful for regulating more precisely the digital surveillance, to prevent the fight against terrorism from being used as a pretext for limiting individual freedoms.

***Drones: strategic assets but even dangerous threats***

Another tool deriving from digital transformation that proves to be particularly useful for the fight against terrorism, but, at the same time, has negative sides are drones. The use of drones in counter-terrorism operations in the Middle East and Sub-Saharan Africa has become increasingly frequent in recent years. The drone contributes to the counterterrorism mission by providing pervasive intelligence and aggressive strike capabilities. Both of these, combined and unified in a single aircraft platform, hinder the operational capacity of the terrorist organization by eliciting fear, fracturing communication, and decimating command and control.

On one hand drones are highly effective intelligence assets. USAF testimonials indicate that around 97% of mission time is dedicated purely to reconnaissance. The aircraft contributes to the intelligence cycle because it continuously and simultaneously collects and distributes information. Specifically, it collects intelligence efficiently via advanced visual equipment and long loiter capabilities. It can easily distribute these information to other entities and as the entire process is electronic, intelligence feeds can be stopped, played, rewound, and fast-forwarded from virtually anywhere in the world that has a connection to the satellite link. The intelligence-gathering capabilities of drones were

[264] N.A. (2015), "Ethiopia: Hacking Team Lax on Evidence of Abuse", *Human Rights Watch*, Ethiopia: Hacking Team Lax on Evidence of Abuse | Human Rights Watch (hrw.org)
[265] Hassib B. & Shires J. (2021), "Manipulating uncertainty: cybersecurity politics in Egypt", in *Journal of Cybersecurity*, Oxford University Press
[266] Lynch J. (2022), *Iron Net: Digital Repression In The Middle East And North Africa*, European Council on Foreign Relations

fundamental to identifying the location of top leaders of prominent terrorist organizations such as Abu Musab al-Zarqawi or Osama bin Laden.[267]

On the other hand, UAVs are particularly effective at lethally eliminating top terrorist leadership. According to Price, removing these leaders from a position of authority is the most significant variable in the downfall of a terrorist organization, because they have significant influence over the creation of norms within the organization and leadership succession is often difficult. In this regard, in July and August 2022 respectively, US drone airstrikes killed the leader of IS in Syria, Maher al-Agal, and the leader of al-Qaeda, Ayman al-Zawahiri.[268]

The marked functionality of drones and their cost-efficiency compared to field operations, in economic terms and in terms of risk of military personnel, have therefore led to a growing use in contemporary counterterrorism operations. In Afghanistan and other areas where the United States lacks a persistent, physical presence, the Biden administration announced a pivot to "over-the-horizon" counterterrorism operations (OTHCT) that rely heavily on stand-off assets, such as overhead satellite technology and airpower, in the absence of eyes and ears. The use of "remotely piloted aircraft" (RPAs)—to target potential terrorist threats, however, has come under increasing pressure from human rights and humanitarian organizations, and others for their effects on civilian populations. RPAs have caused collateral civilian casualties, eroding U.S. legitimacy and providing cause for recruitment into extremist organizations. Notably, a 2013 study by Larry Lewis from the Center for Naval Analyses (CNA) found that drones were ten times more deadly to civilians than crewed aircraft during one year in Afghanistan. Furthermore, without an on-the-ground presence, the possibility of inadequate intelligence and misanalysis could further undermine the accuracy and efficiency of the airstrikes.[269]

Alongside the US, other NATO partners have also made increasing use of drones in counter-terrorism operations in recent years. France has repeatedly used RPAs to strike the leaders of Sahelian jihadist organizations and, probably, the use of "remote warfare" will be even more marked following the gradual withdrawal of French troops from the region.[270] This growing practice raises the need for greater international cooperation to increase regulatory clarity, transparency and accountability in this regard. If RPAs are to be relied upon more heavily, they should be treated as transparently as other

[267] Farrow A. (2014), "Drone Warfare as a Military Instrument of Counterterrorism Strategy", *Air & Space Power Journal*, pp. 6-7
[268] *Ivi*, pp. 8-9
[269] Yayboke E. & Reid C. (2022), *Counterterrorism from the Sky? How to Think Over the Horizon about Drones*, Center for Strategic and International Studies
[270] Tull D.M. (2021), *Operation Barkhane and the Future of Intervention in the Sahel*, Stiftung Wissenschaft und Politik German Institute for International and Security Affairs, Comment n. 5

military operations that have a high chance of civilian impacts. Indeed, as warfighting technology advances rapidly, the public will demand more accountability.[271]

Estimated Casualties of Drone Attacks in Pakistan, Libya, Yemen, and Somalia

| Country | Total Drone Strikes | Estimated Civilian Casualties (lower bound) | Estimated Civilian Casualties (upper bound) | Estimated Total Casualties (lower bound) | Estimated Total Casualties (upper bound) |
|---|---|---|---|---|---|
| Pakistan (2004–2018) | 414 | 245 | 303 | 2,366 | 3,702 |
| Libya (2012–2020) | 4,606 | 637 | 930 | 1,867 | 2,482 |
| Yemen (2009–2021) | 376 | 125 | 151 | 1,390 | 1,779 |
| Somalia (2003–2022) | 267 | 33 | 120 | 1,483 | 1,965 |
| | 5,663 | 1,040 | 1,504 | 7,106 | 9,928 |

*Figure 29: Estimated Casualties of Drone Attacks in Pakistan, Libya, Yemen and Somalia. Source: CSIS*

In addition to the danger to civilians in counter-terrorism operations, drones are particularly dangerous as increasingly used by terrorist groups themselves to achieve a variety of goals. First, they may be deployed to collect information about sites' weak points, with the intention to subsequently exploit the detected vulnerabilities by launching a conventional or drone-based attack. In case of attack, they may be directed to crash against a target or used to discharge explosive devices or release chemical, biological, radiological or nuclear agents. Furthermore, jihadist could use them for propaganda purposes, which has been a hallmark of Daesh's UAS strategy, filming their attacks on crowded or vulnerable sites and maximizing the media impact of their actions.[272]

Since 2014, the use of commercial drones for terrorist purposes has emerged in the Middle East, especially by the Islamic State which has repeatedly used them in attacks in Syria and Iraq. In this case, the IS strategy envisaged the online purchase of commercial drones, taking advantage of the low costs and the high modifiability of the products, which can easily be transformed into explosive weapons to be used in battle.[273] The trend has also spread to Africa, where, although the adaptation of commercial drones into strike platforms is yet to happen, there is evidence of their use by armed groups for surveillance and precision targeting. As underlined by Herbert, the Middle East experience does not necessarily mean that drones may be used in the same way in Africa and "*their tactical utility may be limited as a weapon; however, strategically they could be of use for wider intelligence gathering, for collection of footage and propaganda materials and for precision targeting*.' Indeed,

[271] Yayboke E. & Reid C. (2022), *Counterterrorism from the Sky? How to Think Over the Horizon about Drones*, Center for Strategic and International Studies
[272] UN Office of Counterterrorism (2022), *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)*, Global Programme on Countering Terrorist Threats against Vulnerable Targets
[273] Rassler D. (2018), *The Islamic State and Drones: Supply, Scale and Future Threats*, Combatting Terrorism Center at West Point, United States Military Academy

in the Democratic Republic of the Congo, insurgents have recently used unmanned aerial systems to locate targets for attacks and, in Somalia, al-Shabaab has deployed drones for surveillance and propaganda purposes.[274]

In this context the main mean to avoid the use of commercial drones for terrorist purposes is the international cooperation between states and industry stakeholders to regulate both the use and export of commercial drones. In this sense, an example is the Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems, which condenses the takeaways and experiences shared by governments, law enforcement agencies, multilateral organizations, private industry and other subject matter experts. The Memorandum identifies 26 good practices in four broad areas: 1) Assessing the risk and vulnerabilities and raising awareness; 2) Enhancing information-sharing, engaging with relevant stakeholders and educating the public; 3) Implementing policies and regulations, establishing crisis planning; 4) Developing tactical countermeasures and technical solutions.[275]

Regarding the use of drones for terrorist purposes in war zones, an useful measures from private companies could be the implementation of geo-fencing systems. An example dates back to 2017 when, to the news that the IS was predominantly using DJI's Phantom drones, the company has quietly initiated an update to its geo-fencing system, which was supposed to render its drones no longer operable in "most of Iraq and Syria". The biggest incentive for companies to implement such systems lies in the bad publicity that the use of their products in war zones brings. Indeed, drones for photography and videography, while on the one hand are booming in sales due to their reliability, could see their popularity decline as they become increasingly associated with terrorist groups.[276]

[274] Allen K. (2021), "Drones in the hands of insurgents: how Africa can prepare", *Institute for Security Studies Africa*, https://issafrica.org/iss-today/drones-in-the-hands-of-insurgents-how-africa-can-prepare
[275] UN Office of Counterterrorism (2022), *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)*, Global Programme on Countering Terrorist Threats against Vulnerable Targets
[276] Fontana G. (2018), "Droni civili per terrorismo, quali soluzioni al problema", *Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/droni-civili-a-scopo-offensivo-problemi-e-soluzioni/

## 3.5 Technological independence: the race to critical raw materials for digital transformation

***European growing demand and growing foreign dependence***

The growing digital transformation is making more and more sectors highly digitized and is consequently increasing the need for raw materials for the construction of digital products. In particular, with regard to some non-ferrous metals, a further strong growth in demand is expected in the coming years as they play a fundamental role in various components of the digital network, in displays, in fibre optic cables and for automated control in microchips. The main problem, however, lies in the fact that today these resources are mainly extracted outside the European sphere of influence.

For many years, the EU and its member states, or rather, its companies have successfully met their high demand for raw materials on the global market by relying on imports from abroad. This has made it possible to largely externalize negative side effects, such as environmental damage from mining and processing, but on the other hand has led to high levels of dependence on raw materials. In recent decades, the EU has consistently recorded a trade deficit in this sector. This deficit is highest among metals and minerals (€32 billion) and particularly high for several raw materials critical to the EU economy. Since 2008, given the volatility of commodity prices on the international market, the problem of excessive European dependence has begun to emerge more clearly. The EU Raw Materials Initiative of 2008, for example, aimed to set the right framework conditions to foster supply from European sources, reduce consumption, and decrease relative import dependency through efficiency increases and recycling. However, this was not enough to increase raw material security. In 2011, EU published the first list of critical raw materials, are those raw materials which are economically and strategically important for the European economy, but have a high-risk associated with their supply. It included 14 raw materials, while the fourth list, published 2020, included 30 critical raw materials.[277] This growth represents an increase in quantity and variety of materials needed for modern high-tech products (figure 30), which was not matched with efforts to increase EU raw material security.

[277] Langsdorf S., Morotomi K., Rechlin A. (2022), *Tackling the EU's Dependency on Raw Materials from China: A Case Study on Rare Earth Elements and Potentials of the Circular Economy*, Friedrich Naumann Foundation for Freedom, European Dialogue Programme

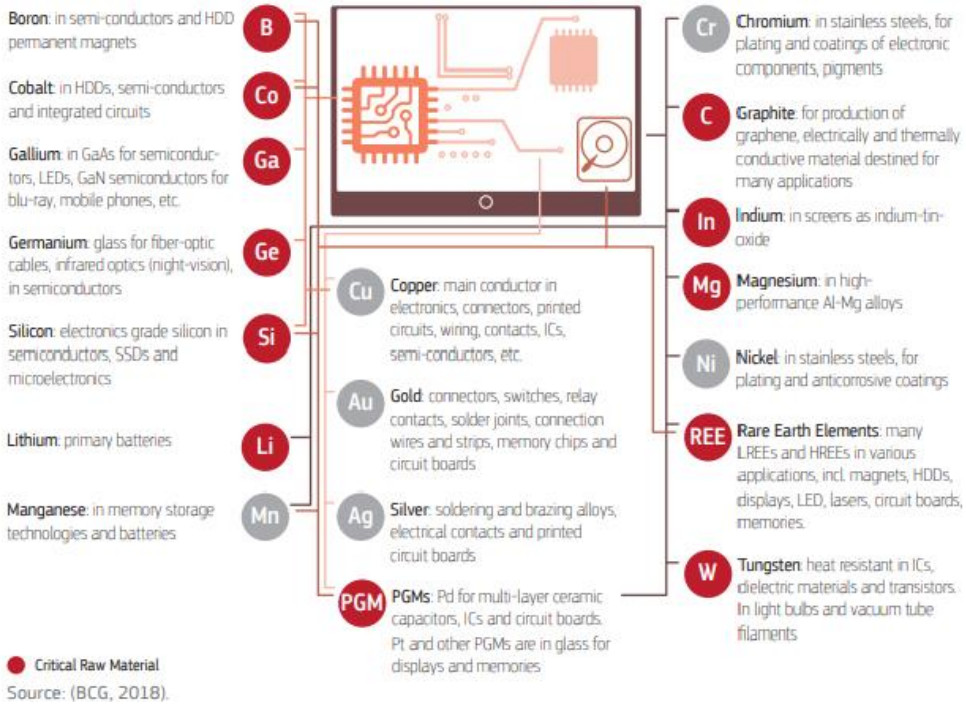


*Figure 30: Raw Materials Digital Technologies. Source: European Commission*

In September 2020, to make the supply of critical raw materials more reliable, secure and sustainable, the European Commission published a Communication containing the Action Plan for Critical Raw Materials. This is centred on three strategic axes: 1) Reducing the dependence on primary critical raw materials through the circular use of resources, sustainable products and innovation; 2) Strengthen the internal supply of raw materials in the European Union; 3) Diversify supplies from third countries and remove distortions of international trade.

Furthermore, the European Commission has launched the European Raw Material Alliance (ERMA). This has the task of bringing together different stakeholders, strengthening the resilience and strategic autonomy of the Union, identifying obstacles, opportunities and investment possibilities in all stages of the critical raw materials value chain, addressing at the same time environmental and social sustainability. Italy joined the initiative and, in 2021, the "Ministry of Enterprises and Made in Italy" launched a Critical Raw Materials Technical Table, with the purpose of mapping the needs of critical raw materials at the Italian level, cross-referencing these data with their availability and using them as a basis for defining a national strategy for critical raw materials. To this end, four thematic Working Groups were set up with the aim of systematizing prospective supply and demand by sector and by geographical area.[278]

[278] Italian Ministry of Enterprises and Mande In Italy, *Materie Prime Critiche*, https://www.mise.gov.it/index.php/it/impresa/competitivita-e-nuove-imprese/materie-prime-critiche/materie-prime-critiche

***China's monopoly in the sector***

Of the 30 raw materials that the EU classifies as critical, 19 are predominantly imported from China. Indeed, China, pursuing a policy on raw materials practically opposite to the European one, can now count on large raw material deposits and a strong mining industry. Between 2002 and 2018, Beijing kept 14.5% of the total global extraction of eight different types of base metals. During the same time, the EU's own percentage shrunk from 4.1 to 2.6%. China's production efforts become even more impressive when looking at its refining capacities: for the abovementioned raw materials, refinery production rose from 17.7 to 44.5% between 2002 and 2018. Meanwhile, the EU's decreased from 15.9 to 9.1%. Today, China holds around half of the world's refinery capacities.[279] From Figure 31 it is clear that China is the largest supplier of several of the seven materials defined by UNCTAD as "ICT elements", producing 95% of global gallium, 89% of germanium, 7% of tellurium, 47% of indium, 25% of selenium and 5% of tantalum.[280] This dominance holds especially true for rare earths, where the supply risk is considered by the Commission to be the highest, as EU imports from China 98% of these materials. REEs are an example of the different mining policies between the West and China in the last decades. Indeed, in the 1970s and 1980s, the United States dominated global rare earth production and still today the reserves of rare earths discovered in Europe in the 18th century could meet the needs of Europeans. However, the process to extract and separate the rare earths from the ore is difficult because the REEs are chemically very similar to each other and the process can also be heavily polluting. When environmental demands grew, new investments were necessary to reduce emissions, production costs increased and profitability dwindled. Therefore, in the 1990s, most countries in the world undertook, for economic and environmental reasons, to relocate the extraction and dirty processing of rare earths to China, which today provides nearly 85% of world production.[281]

[279] Langsdorf S., Morotomi K., Rechlin A. (2022), *Tackling the EU's Dependency on Raw Materials from China: A Case Study on Rare Earth Elements and Potentials of the Circular Economy*, Friedrich Naumann Foundation for Freedom, European Dialogue Programme

[280] Division On Technology And Logistics Science, Technology and ICT Branch, ICT Policy Section (2020), *Digital Economy Growth And Mineral Resources Implications for Developing Countries*, UNCTAD Technical Notes on ICT for Development, n.16

[281] Fabry E. (2021), "Reducing the EU's Dependence on Chinese Imports of Rare Earths and other Strategic Minerals", in Bermann S. & Fabry E. (eds.), *Building Europe's Strategic Autonomy Vis-À-Vis China*, Institut Jacques Delors, Report n. 124


*Figure 31: Production of seven ICT elements 2018 (millions of US dollar): Source: UNCTAD*

This dependency "*may at any time become a political weapon in case of a conflict*". Already in 2010, some analysts accused Beijing to use its raw materials monopoly to exert political pressure when, following a dispute with Japan, it limited the export of rare earths for two months. The move was later examined by the World Trade Organization and China had to reverse its export cuts, but several times in the following years Beijing feared the possibility of a reduction or a ban on REE exports. In 2020, China introduced its "Export Control Law" for sensitive materials and technologies, which was widely understood to be a response to the expanding export controls of the USA. In 2021 this law was followed by a draft regulation on the management of rare earth elements, which led the European Commission to submit comments "recalling that any measures to be taken should comply with China's obligations and commitments under the World Trade Organisation". However, since 2010 the WTO has been weakened and its dispute settlement is currently not fully functioning. This makes conflict settlement via the WTO a lot less likely. In this context, "*without doubt, dependencies would become a significant problem for the EU and the entire Western world in a possible major conflict over Taiwan*".[282]

Beyond any geopolitical clashes, the level of Chinese exports of critical raw materials is destined to decrease also due to Beijing's internal policies. In its latest five-year plan, China made it clear that exports would be cut to satisfy growing domestic demand. Indeed, China hopes to become climate-neutral by 2060 and needs more critical raw materials for itself. Much of this new demand is being driven by rapid growth of the renewable energy and electric vehicle industries, which utilize large quantities of rare earth permanent magnets. From 2007 to 2017, China's production of renewable and

[282] Langsdorf S., Morotomi K., Rechlin A. (2022), *Tackling the EU's Dependency on Raw Materials from China: A Case Study on Rare Earth Elements and Potentials of the Circular Economy*, Friedrich Naumann Foundation for Freedom, European Dialogue Programme

nuclear energy more than tripled, accounting for roughly 51% of the global increase in production over this period. China's electric vehicle market is growing even faster. Between 2014 and 2019, the number of electric vehicles in China swelled from approximately 90,000 to nearly 3.4 million. As China's domestic consumption of critical raw materials grows, the country will be increasingly reliant on imports. China already became the world's largest importer of rare earths in 2018, and it is expected to become a net importer by the middle of the decade.[283] In a strategic move, Beijing has already secured vital imports from Africa and elsewhere through large-scale investments and long-term contracts.

***The race to African cobalt and tantalum***

Africa is strategic mainly with regard to two critical materials for the digital industry: cobalt and tantalum. Cobalt is essential for the production of lithium-ion batteries, increasingly used in new digital technologies, while the ability of tantalum to store and release electrical energy makes it ideally suited for use in certain types of capacitors that are widely used in modern electronics. The key exporting country for these materials is the Democratic Republic of the Congo. DRC currently supplies 70% of the world's cobalt and about a third of tantalum mined globally. The crucial importance of the two materials has contributed to reinforcing the country's instability, exacerbating the struggle between paramilitary groups and guerrillas for control of the extraction territories and increasing foreign influence. In particular, China has dominated the Congolese mining industry for years. The DRC and China have negotiated various 'resources-for-infrastructure' deals since the early 1970s. Most have linked road and dam construction to mineral extraction. The most prominent, the 2008 Sicomines Agreement, links US$ 6.2 billion in concessional loans from the Export-Import Bank of China to a joint venture between the DRC state-owned Gécamines and a consortium of Chinese firms (with 32% and 68% ownership, respectively). The deal gives predominantly Chinese mining companies tax-free access to around 627,000 tonnes of cobalt over 25 years, until the mining profits repay the loan.[284] In 2021, according to The Times and Benchmark Mineral Intelligence, 15 of the 19 cobalt-producing mines in Congo were owned or financed by Chinese companies.

In addition to China, Russia is also showing growing attention to the DRC and its mineral resources. In Moscow's geopolitical calculations, aimed at gaining leverage over global competitor countries, Congolese mineral wealth and Western dependence on the country's mineral exports (half of the

[283] China Power Team (2020), "Does China Pose a Threat to Global Rare Earth Supply Chains?", *Center for Strategic and International Studies*, https://chinapower.csis.org/china-rare-earths/

[284] Bolin A. et al. (2019, *Chinese investment in DRC: a view from the forest*, International Institute for Environment and Development,

coltan needs of the United States' military-industrial complex is covered by imports from the DRC) are seen by Russian observers as an element Moscow should capitalize on. The strengthening of relations with the Congo is mainly taking place following two channels. On the one hand, Moscow is investing in some important infrastructure projects in the country, such as in the development of the Grand Inga Dam, which, if completed, will be the largest hydro-electric dam in the world[285]; on the other hand, the Kremlin is intensifying relations in the security field, given that various analysts report the involvement of the Wagner group in the conflict between the Kinshasa government and the M23 rebels.[286] In 2019, the Congolese government underscored its willingness to use the Russian experience in natural resource extraction (primarily in the realm of mining) and the Russian side confirmed "some large joint projects in geological exploration, extraction and transportation of mineral resources".[287]

This context, despite the strong Russian and especially Chinese influence, still presents opportunities for Italy and its European partners to enter the Congolese mining market and secure supplies of cobalt and tantalum. Indeed, with financial help from the American government as part of its broader anti-corruption effort, Congolese officials are carrying out a broad review of past mining contracts, examining whether foreign companies are fulfilling their contractual obligations.[288] In particular, the Congolese government is starting to question the contractual agreement with Beijing, because this does not seem to bring enough benefits to the country.[289] Since one of the three strategic assets on which the European Action Plan on Critical Raw materials is based is the diversification of imports from third countries and the removal of distortions of the international market, it is necessary for Europe and for Italy to enter this space and forge cooperation with DRC for mining, focusing, unlike its competitors, on reliability and respect for human rights.

In addition to the DRC, the diversification of the supplies can be achieved by exploiting other potential hubs for cobalt and tantalum present in the Wider Mediterranean area. Morocco is emerging as a new cobalt exporter and Rabat is showing a willingness to expand extractions of the material to

[285] Sukhankin S. (2020), "Russian Inroads Into Central Africa", *Eurasia Daily Monitor*, The Jamestown Foundation, Vol. 17, Issue 56
[286] N.A. (2023), "Wagner Group expands influence in DRC, Africa", *Robert Lansing Institute for Global Threats and Democracies Studies*, https://lansinginstitute.org/2023/01/13/wagner-group-expands-influence-in-drc-africa/
[287] Sukhankin S. (2020), "Russian Inroads Into Central Africa", *Eurasia Daily Monitor*, The Jamestown Foundation, Vol. 17, Issue 56
[288] Lipton E., Forsythe M., Searcey D. (2021), "A Power Struggle Over Cobalt Rattles the Clean Energy Revolution", *The New York Times*, https://www.nytimes.com/2021/11/20/world/china-congo-cobalt.html
[289] Do Rosario J. & Strohecker K. (2023), "Exclusive: Congo sees deal on $6 bln China mining contract overhaul this year -FinMin", *Reuters*, https://www.reuters.com/markets/commodities/congo-sees-deal-6-bln-china-mining-contract-overhaul-this-year-finmin-2023-01-18/

meet the country's ecological transition plan.[290] On the other hand, as regards the demand for tantalum, some potential hubs are located in the Gulf of Guinea and in the Horn of Africa. In particular, Nigeria and Ethiopia are respectively the fourth and sixth world producers of tantalum and seem to have large potential in this field. Although Beijing is the main destination for a large part of the extractions of these countries, these new markets represent an important opportunity for European countries to diversify their imports of the two critical materials and reduce their dependence on China. The foreign policy choices of Rome and Brussels, therefore, are called to favor a dialogue with these countries regarding this sector and to ensure stable cooperation agreements according to the growing demand for cobalt and tantalum that the digital transformation will bring.

## 3.6 Digital transformation and Italian national interests

The analysis made in this chapter has clearly shown how nowadays there is a strong link between the digital transformation and Italian national interests in the Wider Mediterranean. The new digital technologies and the challenges that their growing application brings have greatly changed the strategies and contexts in which Italy has to operate to guarantee its interests.

In the case of the protection of critical submarine infrastructures, energy and internet cables, the need for greater attention to cybersecurity has increasingly emerged. The very nature of these infrastructures, which cross several countries and whose construction involves a large number of stakeholders, makes it impossible to guarantee security without a cooperative approach with the countries and private firms involved. As for submarine internet cables, which form the country's digital backbone, both the physical threat, coming from Russia, and the economic one, linked to Chinese investments in the sector, need to be addressed.

Cybersecurity also plays an increasingly central role in guaranteeing the security of maritime trade, on which Italy is closely dependent. The analysis showed that the cyber threat is already very current towards ports, where a cyberattack can cause enormous damage to the entire supply chain and therefore have very negative economic effects which spread far beyond the single port and affected country. Furthermore, the examples provided confirm that the cyber threat is rapidly expanding on the routes of commercial ships, as evidenced by the cases of GNSS spoofing in various maritime contexts. To counter this type of threat, an essential element is the Maritime Situational Awareness, obtained through the exchange of information. In this sense, the Italian Navy has proved to be at the

[290] Gomez C. (2022), "Morocco wants to increase its cobalt production for the manufacture of rechargeable batteries", *Atalayar*, https://atalayar.com/en/content/morocco-wants-increase-its-cobalt-production-manufacture-rechargeable-batteries

forefront with the development of its SMART FENIX software for sharing information with other Navies and the V-RMTC initiative.

Information sharing and situational awareness are also fundamental in the approach to border control and the fight against illegal immigration. In this context, European legislation imposes an increasing use of IT systems such as EUROSUR, EURODAC, SIS II and VIS. Particularly relevant for Italy is the growing use of drones in FRONTEX missions, as in the case of the Operation Sophia in the waters of the Central Mediterranean. The use of UAVs in these contexts has important economic and strategic implications for Italy since the defense company Leonardo, of which the state is the major shareholder, plays a key role in the UAVs industry. At the same time, however, the use of drones poses serious problems of a humanitarian and legal nature and therefore requires a greater regulatory effort at an international and European level.

The fight against jihadist terrorism, which is booming especially in the Sahel, is another case where Italian strategies to defend its national interests are strongly conditioned by the rise of digital transformation. Over the past few years, jihadist groups have developed a solid presence in cyberspace, which has now become a thriving ground for funding, recruitment and propaganda. In particular, the problem of jihadist propaganda on social media requires great attention since it concerns all areas of the Wider Mediterranean and also has repercussions on the internal front. One of the most used means to fight online terrorism are surveillance systems, often AI-guided. However, the use of these systems poses problems from a humanitarian and democratic point of view, because often the technologies supplied by Western partners, including Italy, are used by the governments of the macro-region for the repression of dissent. This ambivalence in the use of new technologies for counterterrorism also pertains to the controversial use of drones as UAVs have demonstrated great operational advantages in counterterrorism, but at the same time have been the cause of numerous civilian deaths. Furthermore, terrorists have also demonstrated increasing use of these technologies, adapting commercial drones as both explosive weapons and intelligence gathering assets.

Finally, a particular case is represented by the race for critical materials for digital transformation. In this case, the digital aspect rather than constitute a necessary means to protect Italian national interests, contributes by itself to setting the national foreign policy agenda towards the geostrategic region. Indeed, some areas of the Wider Mediterranean are strategic for the extraction of minerals necessary for the construction of digital technologies, in particular cobalt and tantalum. Thus, attending these areas of extraction and strengthening relations with these countries assumes particular importance for Italy to reduce the dependence on digital technologies from abroad, especially from China.

# Conclusion

The elaborate analyzed the impact of the digital transformation on the geostrategic region of the Wider Mediterranean and the effects on the Italian foreign policy towards the region. The analysis revealed a strong influence of the digital aspect on the geopolitical and geoeconomic dynamics of the region and, therefore, on the foreign policy choices that Italy is called to make in this context. In particular, the digital transformation has proved to be a crucial element for three factors:

- it has significantly contributed to changing the social, economic and political context of the macro-region. This has brought out new needs and new threats for the population and governments of the area and has therefore made it necessary to adapt the traditional means of Italian foreign policy with which to approach the region;

- it has allowed new players to enter the balance of power in the region by exploiting the potential of new technologies. This is clearly seen in the strategies of both global actors, China and Russia, and regional ones, Turkey and Iran, which have exploited the opportunity to gain increasing space in a scenario of growing geopolitical competition;

- it has quickly changed the strategies needed to protect Italian national interests in the region, as the security of critical submarine infrastructures, the stability of maritime trade, the fight against terrorism and illegal immigration as well as strategic autonomy in the procurement of critical raw materials are all sectors now heavily dependent on the dynamics of digital transformation.

What emerges from the intersection of these three dynamics is the clear need for Italy to adopt an approach that takes greater account of the changes, opportunities and threats which the digital transformation has brought in the macro-region. This, as just described, becomes necessary in order to relate more properly with a rapidly evolving context, to respond effectively to the competitors' actions and to ensure adequate protection of their national interests. In this perspective, the study conducted has made it possible to identify some focal points on which Italy, both nationally and in collaboration with European partners, will necessarily have to direct its foreign policy.

One of the aspects that emerged most clearly is the growing danger of attacks from cyberspace, especially concerning the protection of Italian critical infrastructures in the Wider Mediterranean. Various actors involved in the macro-region, both state and non-state, have demonstrated an increasing willingness and ability to conduct attacks of this type against critical infrastructures. Undersea energy pipelines and internet cables, as well as port infrastructures are particularly

vulnerable in this sense due to their transnational nature and the high number of stakeholders involved. An accident that even occurs outside the Italian territory can have a serious impact on the Italian economy because it would interrupt respectively the supply of energy, the flow of internet data or the maritime supply chain. In this context, as underlined by the President of the National Cybersecurity Agency, Roberto Baldoni, countries cannot limit the scope of their preventive and counter initiatives to the domestic realm. They should act at the international level, too, promoting and contributing to universal, regional, and bilateral cooperation in the field of cybersecurity.[291] Italy should deepen governmental collaboration in the sector with regional actors at the multilateral and intergovernmental level, as in context of the New Agenda for the Mediterranean, the OSCE's Mediterranean Partnership, or the Union for the Mediterranean and the 5+5 Dialogue.[292] It should also engage in bilateral cyber-capacity building (CCB)[293] initiatives to improve the overall cybersecurity of regional and sub-regional areas. A virtuous example in this sense is USAID's recent program to enhance Kyiv's cyber capabilities against Russian cyber-attacks since, following the implementation of these actions, Ukrainian cyber capabilities have improved significantly.[294]

In some cases, however, the threats are not so direct. The Wider Mediterranean is one of the key regions where the game is being played to obtain EU digital sovereignty and strategic autonomy. As previously seen, China through the investments of the Digital Silk Road, is gradually acquiring control over the majority of digital infrastructures in the region. This, in addition to providing Beijing with an important political and economic leverage over regional countries to exploit in the global competition with the West, allows China complete access to the data flow. Furthermore, Beijing, which already owns a near-monopoly of all critical raw materials for digital components, also presides over and dominates the rare cobalt and tantalum mining areas, essential for the production of batteries and electronics. The Chinese strategy highlights the need for an integrated approach among the European partners to counter Beijing's economic expansionism. To counter Chinese investments, Italy, which has already exercised the "golden power" regulation on Telecom Sparkle Italia, should promote consortia with other leading European companies in the sector, such as the French "Orange"

[291] Baldoni R. (2022), "Cyber Capacity Building: Security, Innovation, and Growth in the Mediterranean Region", *ISPI*, http://www.ispionline.it/en/publication/cyber-capacity-building-security-innovation-and-growth-mediterranean-region-35371

[292] Ferrara P. (2022), "As Cyber Threats Target the Wider Mediterranean Region, Countries Must Act Together", *ISPI*, http://www.ispionline.it/en/publication/cyber-threats-target-wider-mediterranean-region-countries-must-act-together-35345

[293] Barbero defines CCB as: "*the development and reinforcement of processes, competences, resources and agreements aimed at strengthening national capabilities, at developing collective capabilities and at facilitating international cooperation and partnerships in order to respond effectively to the cyber-related challenges of the digital age*".

[294] Martino L. (2022), "Why Cyber Capacity-Building Is Essential to Achieving Stability", *ISPI*, http://www.ispionline.it/en/publication/why-cyber-capacity-building-essential-achieving-stability-35365

and the Spanish “Telxius”. In the wake of the EU Digital Compass, the Union could help in this sense by financing projects directly – as in the case of BELLA consortium – but also by working with states in its neighbourhood to set similar legislative standards on privacy and ownership. Concerning the supply of critical digital raw materials it is necessary for Europe and for Italy to forge cooperation for mining with Democratic Republic of Congo, which is the main producer of cobalt and tantalum, and other African potential exporters, such as Morocco, Ethiopia or Nigeria, focusing, unlike its competitors, on reliability and respect for human rights.

In addition to the dangers of cyberattacks and the Chinese monopoly on the region's digital ecosystem, the analysis then identified another crucial sector on which Italy should focus its attention: the fight against online disinformation and propaganda. Social media has emerged as a new arena of influence exploited by state actors, such as Russia and Iran, and non-state actors, such as jihadist terrorist groups, for their own interests. In this perspective, an observatory for online harms should be developed and supported in order to track and understand the depth of extremist and hateful narratives across a range of platforms. This observatory can then help shape policy and practices relating to the proliferation of harmful content online, assisting technology companies, civil society and government. At the European level, Italy should increase its support to projects such as the EEAS Strategic Communications Task Force (Stratcom), which, with its Division 2, focuses on pro-active communication and awareness raising, support to independent media, and the detection, analysis and challenge of information manipulation and interference activities by foreign states in the EU Southern Neighbourhood.

Another development that has proved to be fundamental in different contexts is the need to share and exchange information with European, Atlantic and regional partners to achieve the so-called “Situational Awareness”. This applies in particular to ensuring the security of maritime trade routes and the border control, respectively against the threat of piracy and illegal migration. In this perspective, Italy should continue in the footsteps already successfully marked by national initiatives such as the SMART FENIX software and the Virtual Regional Maritime Traffic Centre (V-RMTC), developed by the Italian Navy to share information with other Navies and to contribute obtaining a Maritime Situational Awareness in the areas of interest. In parallel, Rome should guarantee a commitment also at European level in contributing to the improvement and operativity of recently created European IT systems, such as the Common Information Sharing Environment (CISE) or the European Border Surveillance System (EUROSUR).

Finally, in the course of the elaborate an ambivalence in the use of new technologies emerged, showing that on the one hand these provide useful support but, on the other, raise various problems

of a humanitarian nature. One of the example concerns the growing use of surveillance software and AI in countering terrorist propaganda online. Surveillance software has been widely used by authoritarian regimes in the region to repress dissent and, in this sense, some analysts have underlined Beijing's role in exporting these technologies to consolidate its governance model. Italy is directly involved since it was forced to block exports of an Italian surveillance software which has been repeatedly reported as a tool for repressing dissent in many African contexts, including Egypt and Ethiopia. The same ambivalence is identifiable in the use of drones, both in counterterrorism and border control. In both contexts UAVs provide important operational advantages, but at the same time cause several humanitarian problems. Italy is particularly interested in this theme given the relevance in the UAVs production of the defense company Leonardo, of which the Italian state is the largest shareholder. The Turkish “drone diplomacy” has clearly shown how the export of drones can be a useful foreign policy tool, but, in this case, as in that of surveillance software, Rome, given the economic and strategic importance of its exports, must push for international regulation on the use of these technologies to ensure that its exports are not used for and associated with violation of human rights.

In conclusion, the analysis conducted in this work has clearly underlined how the digital aspect is now closely related to all the major political, economic and social dynamics of the Wider Mediterranean. Italian foreign policy towards the macro-region can no longer disregard the consideration of the challenges that the digital transformation has brought about in this context. In the last decade, Italy has shown the ability to adapt the geostrategic concept of the Wider Mediterranean to the evolution of the international context and Italian national interests. The next evolution should not concern geographical borders, but the enlargement to a new domain, the digital one.

# Abstract

The geostrategic concept of the Wider Mediterranean was born in the 1980s and progressively enlarged the strategic borders of the "*Mare Nostrum"*. The first "enlargement" involved the Middle East and the Persian Gulf, which have become particularly crucial areas for energy supplies and for the fight against jihadist terrorism. In the following years the geostrategic region, mainly for security reasons, expanded towards Sub-Saharan Africa, integrating the two natural extensions of the Mediterranean, the Gulf of Guinea and the Red Sea (therefore the Horn of Africa), but also the internal strip that connects them, the Sahel.

In addition to the expansion of its borders, the Wider Mediterranean has seen a progressive growth of importance within Italian foreign policy to the point of being identified as an area of main national interest. This centrality has effectively been confirmed by the reorientation of all the main Italian foreign policy instruments towards the region: almost all of the military missions abroad have been concentrated in the Wider Mediterranean; diplomacy has also followed this line with the opening of new embassies in the Sahel; and even the economic dimension has seen a concentration of development cooperation in the macro-region.

Alongside these aspects, however, the region imposes the need to take into consideration another domain, the digital one, which inevitably intersects with the previous ones. Indeed, the Wider Mediterranean is experiencing, albeit on different levels given the disparity of digital penetration in the macro-region, a growing digital transformation. The impact of digitalization and the expansion of cyberspace affects all aspects of society: from the economy, to society and politics, but also regional warfare and conflicts. This has changed both the logic with which states carry on their rivalries, for example with the emergence of cyberattacks or the disinformation operations, and the relationship between the state and citizens, affecting the amount of information available for civil society. In particular the phenomenon of cybercrime assumes a crucial relevance, because it severely slows down the growth prospects of the region.

Beijing, Moscow, Ankara and Tehran have skilfully capitalized on the opportunities opened by this evolving context, positioning themselves as new strong competitors in the Wider Mediterranean. For China, the region is highly strategic in geographical terms as it is a crucial passage to connect China to Europe. The strategic importance of the area is demonstrated by the great focus dedicated to it within the BRI global investment project, in particular as regards investments in transport such as ports or railways. However, these investments are closely linked to the digital environment, which, in fact, constitutes one of the three main drivers of the Belt and Road Initiative. The Digital Silk Road aims to digitally connect China to the rest of the world and to make China a

leader in the sector. Beijing has therefore heavily invested in the digital ecosystem of the Wider Mediterranean, both in the MENA region and in the sub-Saharan appendages. In particular, the African digital ecosystem is almost totally dependent on China, which has been investing in the sector since long before the DSR. These digital investments in the macro-region allow Beijing to achieve important strategic advantages. First, they allow China to acquire global power and international weight in the context of competition with the US. The digital dependence of the countries of the region on China could in fact be a leverage to be used to acquire consensus on Chinese policies and objectives in the international arena, in particular in deciding the international technical standards for new technologies. Second, the huge Chinese presence in the area's digital ecosystem gives China a great informational advantage, giving it access to a large variety of data. Information superiority is considered by Chinese leaders to be a crucial objective for the nation and this is also closely linked to Chinese military modernization.

Since 2015, Russia has shown a renewed interest in the region, which has distant historical and geographical origins. For centuries, due to geostrategic reasons, Russia has had the need to obtain an outlet towards the warm seas of the Black Sea and the Mediterranean. The military intervention in Syria and the support for General Haftar in Libya go in this direction. In addition to the more strictly geopolitical reasons, there is also a rationale linked to global competition with the West, as for Moscow it is crucial to expand its international alliances to promote an alternative global order. To increase its influence in the Wider Mediterranean, Moscow mainly resorts to asymmetric tactics, such as the use of proxy troops as the Wagner group or information warfare. Within this framework, the digital environment provides an important opportunity especially considering the concept of Russian information warfare, which is not limited only to times of war. Cyberspace, indeed, allows the erosion of the distinction between war and peace and the emergence of a grey zone. Russian disinformation, therefore, resorts to a mix of traditional and new media to carry forward a pro-Moscow and anti-Western narrative. Generally, the disinformation campaigns launched by the major Russian mass media RT and Sputnik are amplified and integrated by a network of social pages and profiles. This is a pattern seen in the Middle East but especially in Africa, where a vast network of disinformation social pages linked to Russian oligarch Yevgeny Prigozhin has emerged over the years. These disinformation campaigns have had positive effects on Russia's image in the region, but have also helped Moscow achieve foreign policy goals, such as increasing support for Assad in the Middle East or growing anti-French sentiment in the Sahel, which then translated into the withdrawal of French troops from Mali. In addition to online disinformation campaigns, Russian information warfare in the future could probably expand to another field, which is the exploitation of internet infrastructures such as submarine cables, from which Moscow could obtain sensitive data and information.

In the last twenty years Turkey has had a renewal of its foreign policy, which began with the rise to power of Erdogan's AKP party and is in line with Davutoglu's "Strategic Depth" doctrine. In its policies of Neo Ottomanism, Ankara has identified the Wider Mediterranean as an area of strategic interest, inevitably positioning itself as one of Italy's main competitors. In particular, Turkish expansionism has turned towards Africa by exploiting the attractiveness of its defense and security sector. In this area, Ankara has managed, through the export of its means of automated warfare, to build increasingly solid partnerships on the continent. In particular, two products of the Turkish defense industry have proved to be particularly useful: the Bayraktar TB2 drone, increasingly requested due to its limited cost compared to its efficiency, and the KORAL electronic warfare system, which increases the performance of these drones. Both of these products have proved particularly effective in recent conflicts, such as in Syria, Libya and Nagorno Karabakh. Through these exports Ankara is carrying out a real "drone diplomacy" which has allowed it to increase its influence in North Africa, in the Sahel, in the Horn of Africa and in the Gulf of Guinea.

Iran is a potential destabilizing actor in the macro-region, not only for its nuclear program but also for the asymmetrical threats it carries out, many of which take place in cyberspace. Indeed, since the 2010 Stuxnet cyber-attack, which targeted Iran's uranium enrichment centrifuges in Natanz nuclear facilities, Tehran has constantly developed defensive, but above all offensive, cyber capabilities. Iran has often used these cyber offensive capabilities as a means of deterrence and as a foreign policy tool. On several occasions, Tehran's cyber-attacks have coincided with geopolitically relevant events for the country, such as the Israeli incursions into the Gaza Strip or slowdowns in the negotiations for the JCPOA. These threats are now even more dangerous for Western countries, considering the latest attack on Albania and the growing trend of maritime cyberattacks in the Strait of Hormuz against Western ships. Finally, Iran also uses cyberspace for online propaganda. Tehran, on the one hand, restricts access to online information on the domestic front, on the other, carries out propaganda campaigns abroad. The aim is to promote a positive image for Iran, especially in the Islamic world, as evidenced by information operations in the MENA region. Also in this case, the online propaganda operations are closely linked to the relevant geopolitical events for the country, given the concomitance with the most important political implications in Lebanon, Yemen, Syria and Palestine.

It becomes clear how the digital technology has become an important and essential foreign policy asset in the Wider Mediterranean and how this has already been understood by the main competitors in the region. In this context, it is essential for Italy to consider new foreign policy tools that adapt to the new digital reality of the macro-region and allow to effectively counter the moves of global and regional competitors.

In this scenario, the protection of Italian national interests has been strongly influenced by the emergence of digital technologies. One of the fields most affected regards the protection of critical submarine infrastructures which cross the waters of the Mediterranean. In particular, the threat of an attack on energy pipelines became clear following the sabotage of Nord Stream 2 in the Baltic Sea in September 2022. The many energy pipelines crossing the Mediterranean have already been repeatedly targeted by non-state actors, as shown in various cases in the MENA region from 2011 onwards, but in recent years, the threat has shifted more to the cyber domain. In this case, the cyberattack that hit the American gas pipeline Colonial Pipeline in May 2021 is indicative. The very nature of these infrastructures, which cross several countries and whose construction involves a large number of stakeholders, makes it impossible to guarantee security without a cooperative approach with the countries and private firms involved. Even for submarine internet cables, which form the country's digital backbone, the cyber threat remains a significant danger, as evidenced by the recent cyberattack in Hawaii in April 2022, but both the physical threat, coming from Russia, and the economic one, linked to Chinese investments in the sector, need to be addressed. Russia has probably developed military technologies capable of detecting and taking information from undersea internet cables and has already demonstrated in 2014 in Crimea that it considers attacking internet infrastructure as an option. To respond to this threat, the various Western navies have increased the assets available for cable patrolling, but other measures should be considered, such as the establishment of Cable Protection Zones (CPZs) in the Mediterranean and Suez. Within the Digital Silk Road, China pays particular attention to submarine cables and plays a key role in the production of these infrastructures in the whole Wider Mediterranean. To limit the Chinese monopoly on the digital ecosystem and avoid increasing Beijing's information capacity even further, it is essential for the European partners to coordinate and create, also with EU funding, consortia between the main European companies in the sector (Telecom Italia Sparkle, Orange and Telxius) for the production of submarine cables in the region.

Cybersecurity also plays an increasingly central role in guaranteeing the security of maritime trade, on which Italy is closely dependent. The analysis showed that the cyber threat is already very current towards ports, where a cyberattack can cause enormous damage to the entire supply chain and therefore have very negative economic effects which spread far beyond the single port and affected country. Furthermore, the examples provided confirm that the cyber threat is rapidly expanding on the routes of commercial ships, as evidenced by the cases of GNSS spoofing in various maritime contexts, such as the Strait of Hormuz, where a British vessel was hit by a GNSS spoofing attack from Iranian Revolutionary Guard Corps. To counter this type of threat, an essential element is the Maritime Situational Awareness, obtained through the exchange of information. The European Union

has particularly developed this idea with the new concept of “Coordinated Maritime Presence”, in which the naval assets of the European Navies present on site share useful information to preserve the security of the "maritime areas of interest" for the Union. This concept has proved particularly successful in combating piracy in the Gulf of Guinea and has therefore also been replicated in the Western Indian Ocean. In this sense, the Italian Navy has proved to be at the forefront with the development of its SMART FENIX software for sharing information with other Navies and the Virtual Regional Maritime Traffic Centre (V-RMTC) initiative.

Information sharing and situational awareness are also fundamental in the approach to border control and the fight against illegal immigration. In this context, European legislation imposes an increasing use of IT systems such as EUROSUR, EURODAC, SIS II and VIS, even if several times in the Italian context the choice whether or not to use these software has been influenced by internal policy choices, as in the low level of application of the EURODAC and VIS systems. Particularly relevant for Italy is the growing use of drones in FRONTEX missions to acquire and share information, as in the case of the Operation Sophia in the waters of the Central Mediterranean. The use of UAVs in these contexts has important economic and strategic implications for Italy since the defense company Leonardo, of which the state is the major shareholder, plays a key role in the UAVs industry. Indeed, one of the most used drones in maritime surveillance operations by FRONTEX is Leonardo’s Falco EVO. At the same time, however, the use of drones poses serious problems of a humanitarian and legal nature, as often seen as a way to avoid SAR obligations, and therefore requires a greater regulatory effort at an international and European level.

The fight against jihadist terrorism, which is booming especially in the Sahel, is another case where Italian strategies to defend its national interests are strongly conditioned by the rise of digital transformation. Over the past few years, jihadist groups, especially the Islamic State (IS), have developed a solid presence in cyberspace, which has now become a thriving ground for funding, recruitment and propaganda. In particular, the problem of jihadist propaganda on social media requires great attention since it concerns all areas of the Wider Mediterranean and also has repercussions on the internal front. One of the most used means to fight online terrorism are surveillance systems, often AI-guided. However, the use of these systems poses problems from a humanitarian and democratic point of view, because often the technologies supplied by Western partners, including Italy, are used by the governments of the macro-region for the repression of dissent. In the early 2010s, Canadian NGO Citizen Lab revealed that several Arab governments were employing Italian firm Hacking Team to track the activities of their political opponents, human rights activists, and others. This ambivalence in the use of new technologies for counterterrorism also pertains to the controversial use of drones, in rise following the US pivot to “over the horizon”

counterterrorist operations. UAVs have demonstrated great operational advantages in counterterrorism, but at the same time have been the cause of numerous civilian deaths. Furthermore, terrorists have also demonstrated increasing use of these technologies, adapting commercial drones as both explosive weapons and intelligence gathering assets.

Finally, a particular case is represented by the race for critical materials for digital transformation. In this case, the digital aspect rather than constitute a necessary means to protect Italian national interests, contributes by itself to setting the national foreign policy agenda towards the geostrategic region. Indeed, some areas of the Wider Mediterranean are strategic for the extraction of minerals necessary for the construction of digital technologies, in particular cobalt and tantalum. Thus, attending these areas of extraction, especially the Democratic Republic of Congo but even potential new hubs as Ethiopia, Nigeria or Morocco, and strengthening relations with these countries assumes particular importance for Italy to reduce the dependence on digital technologies from abroad, especially from China, which has a near-monopoly on the extraction and refining of critical raw materials for digital transformation.

In conclusion, the digital aspect is now closely related to all the major political, economic and social dynamics of the Wider Mediterranean and has a strong influence on the foreign policy choices that Italy is called to make in this context. Italy, indeed, can no longer disregard the consideration of the challenges that the digital transformation has brought about in this geostrategic region.

# Bibliography


Abdullah M.A., Ayad M., Harrassy A. (2022), *Under-Moderated, Unhinged and Ubiquitous: Al-Shabaab and the Islamic State Networks on Facebook,* Institute for Strategic Dialogue,

Aboul-Enein S. (2017), *Cybersecurity Challenges in the Middle East*, The Geneva Centre for Security Policy, Research Series n. 22/17

Ach A. & Kurtz P. (2021), "Conduct of Code: A Historical Overview of Cyberspace in MENA", in Campbell E. & Sexton M., (Eds.), *Cyber War & Cyber Peace In The Middle East: Digital Conflict In the Cradle of Civilization*, Middle East Institute

Afterman G. (2021), *China's Evolving Approach to the Middle East: A Decade of Change*, Institute for National Security Studies, Strategic Assessment, Vol. 24, n. 1

Agbebi M. (2021), *China's Digital Silk Road and Africa's Technological Future*, Council on Foreign Relations

Agenzia Nova (2022), "Diplomazia Economica Italiana: la cabina di regia per l'Internazionalizzazione", *MAECI*, https://www.esteri.it/wp-content/uploads/2022/01/20220119-Newsletter-DEI-01_2022.pdf

Ahokas J. et al. (2017), "Cybersecurity in ports: A conceptual approach", in Blecker T., Kersten W. and Ringle C.M. (Eds.), Digitalization in Supply Chain Management and Logistics, epubli GmbH, Berlin

AICS (2021), *Documento Triennale Di Programmazione e di Indirizzo 2021 – 2023*, https://www.esteri.it/wp-content/uploads/2021/11/Schema-di-Documento-triennale-2021-2023.pdf

Allen K. (2021), "Drones in the hands of insurgents: how Africa can prepare", *Institute for Security Studies Africa*, https://issafrica.org/iss-today/drones-in-the-hands-of-insurgents-how-africa-can-prepare

Allen K. (2022), "Hybrid warfare – Africa beware", *Institute for Security Studies Africa*, https://issafrica.org/iss-today/hybrid-warfare-africa-beware

Allen N. & Opkali M. (2022), "Artificial Intelligence Creeps on to the African Battlefield", *Brookings*, https://www.brookings.edu/techstream/artificial-intelligence-creeps-on-to-the-african-battlefield/

Al-Tamimi A., Ayad M., Khan N. (2022), *The Terror Times: The Depth and Breadth of the Islamic State Alternative News Outlet Ecosystem Online*, Institute for Strategic Dialogue

Aluf D. (2022), "China's Tech Outreach in the Middle East and North Africa", *The Diplomat*, https://thediplomat.com/2022/11/chinas-tech-outreach-in-the-middle-east-and-north-africa/

Androjna A. et al. (2020), "Assessing Cyber Challenges of Maritime Navigation", in *Journal of Marine Science and Engineering*, 8,776

Antonovich P. (2011), "Cyberwarfare: Nature and Content", in *Military Thought*, No. 3, Vol. 20

Arcesati R. (2021), "China's Evolving Role in Africa's Digitalisation: From Building Infrastructure to Shaping Ecosystems", *ISPI*, https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247

Arcesati R., Eder T.S., Mardell J. (2021), "Networking the "Belt and Road" - The future is digital", *Mercator Institute for China Studies*, https://merics.org/en/tracker/networking-belt-and-road-future-digital

Atkinson M. & Oshadami O. (2022), "Closing the Digital Divide in Africa", *Equinix*, https://blog.equinix.com/blog/2022/11/02/closing-the-digital-divide-in-africa/

Attanasio Ghezzi C. & Cavalieri R. (2021), "Is the Mediterranean Sea Still the Mare Nostrum? The Belt and Road Initiative and Chinese Investments in the Region" in Corrao F.M. and Redaelli R. (eds.), *States, Actors and Geopolitical Drivers in the Mediterranean*, Palgrave MacMillan

Ayad M. (2022), "Propaganda Primping: The 'Kremlinistas' of Twitter", *Institute for Strategic Dialogue*, https://www.isdglobal.org/digital_dispatches/propaganda-primping-the-kremlinistas-of-twitter/

Azani E. & Doukhan D. (2021), *Global Jihad in Africa: Danger and Challenges*, International Institute for Counterterrorism

Bakir A. (2021), "Turkey's Electronic Warfare Capabilities: The Invisible Power Behind its UACVs", *RUSI*, https://rusi.org/explore-our-research/publications/commentary/turkeys-electronic-warfare-capabilities-invisible-power-behind-its-uacvs

Bako H., et al. (2022), *Conflict and Online Space in the Sahel: Challenges and Recommendations*, Search for Common Ground, Issue Brief

Baldoni R. (2022), “Cyber Capacity Building: Security, Innovation, and Growth in the Mediterranean Region”, *ISPI,* http://www.ispionline.it/en/publication/cyber-capacity-building-security-innovation-and-growth-mediterranean-region-35371

Başaranel B.U. (2017), “Online Terrorist Financing”, in M. Conway, L. Jarvis, O. Lehane, S. Macdonald and L. Nouri (eds.), *Terrorists’ Use of the Internet: Assessment and Response*, Amsterdam, IOS Press

Battisti G. (2017), “Le caratteristiche del “modello italiano” nelle operazioni di peacekeeping”, in Caracciolo I. & Montuoro U., *L'evoluzione del peacekeeping. Il ruolo dell'Italia*, Centro Alti Studi per la Difesa, Giappichelli Editore, Turin

Benigni D. & Ercolani A. (2017), *Digital Transformation: Nuovi Confini, Crescita e Sicurezza del Paese*, The European House – Ambrosetti

Bertram S. & Ellison K. (2014), “Sub Saharan African Terrorist Groups’ use of the Internet”, in *Journal of Terrorism Research*, vol. 5, n. 1 (Special Issue)

Bianco C. & Moretti M. (2022), “Europe’s role in Gulf maritime security”, *Middle East Institute*, https://www.mei.edu/publications/europes-role-gulf-maritime-security

Bolin A. et al. (2019), *Chinese investment in DRC: a view from the forest*, International Institute for Environment and Development,

Borsari F. (2022), *Turkey’s drone diplomacy: Lessons for Europe*, European Council on Foreign Relations

Bronk C. & Tikk-Ringas E. (2013), “The Cyber Attack on Saudi Aramco”, in *Survival: Global Politics and Strategy*, Vol. 55, no. 2

Brooking E. T. & Kianpour S. (2020), *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, Atlantic Council

Bueger C., Liebetrau T., Franken J. (2022), *Security threats to undersea communications cables and infrastructure – consequences for the EU*, Directorate General for External Policies of the Union, Policy Department for External Relations

Burrows M. et al. (2022), *Unpacking The Geopolitics Of Technology: How Second- and Third-Order Implications of Emerging Tech are Changing the World*, Atlantic Council, Geotech Centre

Bush D., DiResta R., Grossman S. (2019), *Evidence of Russia-Linked Influence Operations in Africa*, Stanford Internet Observatory

Çahmutoğlu E. (2021), *Iran's Cyber Power*, Center for Iranian Studies in Ankara (İRAM)

Camerano S. et al. (2021), *Suez e le rotte alternative: il futuro dell'Italia nel commercio marittimo*, CDP Think Tank

Carbone G. (2021), "Tra alti e bassi: l'Italia torna a guardare all'Africa", *ISPI*, https://www.ispionline.it/it/pubblicazione/tra-alti-e-bassi-litalia-torna-guardare-allafrica-29226

Caşın M.H. (2016), "Critical Infrastructures: Security and Energy Politics in the Eastern Mediterranean Region and the Role of the OSCE" in Colombo S. & Sartori N. ed., *The OSCE's Contribution to Energy Governance in the Mediterranean Region*, New-Med Research Network, IAI, Rome

Chan K. & Hungerland N. (2021), *Assessing China's Digital Silk Road: Huawei's engagement in Nigeria*, LSE Ideas, Digital IR Working Paper, n. 11

Chen Y. (2022), "African Railway Ambitions Meet China's Belt and Road", in Rolland N. (eds.), *(In)Roads and Outposts: Critical Infrastructure in China's Africa Strategy*, National Bureau of Asian Research, Special Report no. 98

China Power Team (2020), "Does China Pose a Threat to Global Rare Earth Supply Chains?", *Center for Strategic and International Studies*, https://chinapower.csis.org/china-rare-earths/

Circolo di Studi Diplomatici (2020), "Sicurezza e gestione delle crisi. La dimensione marittima", in *Dialoghi Diplomatici*, n. 250

Clifford B. (2018), "Trucks, Knives, Bombs, Whatever': Exploring Pro-Islamic State Instructional Material on Telegram", in *CTC Sentinel*, vol. 11, no. 5

Cohen S. (2019), "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests", in *Cyber, Intelligence, and Security*, Vol. 3, No. 1

Coleman J., Dal Santo E., Vermeesch E. (2020), *The Role Of Social Media In Mali And Its Relation To Violent Extremism: A Youth Perspective*, UN Interregional Crime and Justice Research Institute

Colombo M., Solfrini F., Varvelli A. (2021), *Network Effects: Europe's Digital Sovereignty In The Mediterranean*, European Council on Foreign Relations

Coralluzzo V. (2011), “Italy’s Mediterranean Policy from a Transatlantic Perspective” in Aliboni R. et al., *Southern Europe and The Mediterranean: National Approaches and Transatlantic Perspectives*, German Marshall Fund of the United States, Mediterranean Paper Series 2011

Coticchia F. (2021), “Un centro di gravità permanente? La difesa italiana e il Mediterraneo allargato”, *Formiche*, https://formiche.net/2021/04/mediterraneo-allargato-coticchia-unige/

Council of the European Union (2014), *European Union Maritime Security Strategy*, https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf

Crippa P. & Di Liddo M. (2021), *Sviluppo, Insicurezza E Volatilità Politica nel Golfo di Guinea, Osservatorio di Politica Internazionale*, Senato della Repubblica, https://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/affariinternazionali/osservatorio/approfondimenti/PI0165.pdf

Crippa P. & Di Liddo M. (2021), *Sviluppo, Insicurezza E Volatilità Politica nel Golfo di Guinea*, Osservatorio di Politica Internazionale, Senato della Repubblica

Cristiani D. (2021), “Tra Ue e Nato, così l’Italia è protagonista in Africa. L’analisi di Cristiani (Iai/Gmf)”, *Formiche*, https://formiche.net/2021/04/italia-protagonista-in-africa-cristiani/

Dancy J.R. & Dancy V.A. (2017), “Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks”, in *Oil & Gas, Nat. Resources & Energy Journal*, vol. 2, n. 6

De La Bruyere E. et al. (2021), *China As A “Cyber Great Power” Beijing’s Two Voices In Telecommunications*, Brookings, Foreign Policy Report

Dentice G. & Talbot V. (Eds) (2020), *A Geopolitical Sea: The New Scramble for The Mediterranean*, ISPI

Di Cecco V. (2004), “Un “grande Medio Oriente” o un “Mediterraneo allargato””, in *Panorama Internazionale: Informazioni della difesa*, n. 2

Division On Technology And Logistics Science, Technology and ICT Branch, ICT Policy Section (2020), *Digital Economy Growth And Mineral Resources Implications for Developing Countries*, UNCTAD Technical Notes on ICT for Development, n.16

Do Rosario J. & Strohecker K. (2023), “Exclusive: Congo sees deal on $6 bln China mining contract overhaul this year -FinMin”, *Reuters*, https://www.reuters.com/markets/commodities/congo-sees-deal-6-bln-china-mining-contract-overhaul-this-year-finmin-2023-01-18/

Donelli F. (2022), *UAVs and beyond: Security and defence sector at the core of Turkey's strategy in Africa*, Megatrends Afrika, Policy Brief, n. 2

Drougkas A. et al. (2019), *Port Cybersecurity: Good practices for cybersecurity in the maritime sector*, European Union Agency for Cybersecurity

EAAS (2022), *Factsheet: Coordinated Maritime Presences*, https://www.eeas.europa.eu/eeas/factsheet-coordinated-maritime-presences_en

Edwards R. (2021), "Iran's strategy of state piracy menaces Middle East oil lanes", *Arab News*, https://www.arabnews.com/node/1788396/middle-east

Elswah M. & Alimardani M. (2021), "Propaganda Chimera: Unpacking the Iranian Perception Information Operations in the Arab World", in *Open Information Science*, vol. 5, p. 167

European Commission (2017), *Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda*, Press Release

European Commission (2020), *Proposal for a Directive of The European Parliament and of the Council on the resilience of critical entities*

European Commission, *Eurosur*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/border-crossing/eurosur_en

European Council (2022), *Coordinated Maritime Presences: Council extends implementation in the Gulf of Guinea for two years and establishes a new Maritime Area of Interest in the North-Western Indian Ocean*, Press Release, https://www.consilium.europa.eu/en/press/press-releases/2022/02/21/coordinated-maritime-presences-council-extends-implementation-in-the-gulf-of-guinea-for-2-years-and-establishes-a-new-concept-in-the-north-west-indian-ocean/#:~:text=The%20CMP%20concept%20in%20the,as%20a%20maritime%20security%20provider.

European Council (2022)," *Operation ATALANTA, EUTM Somalia and EUCAP Somalia: mandates extended for two years*, Press Release, https://www.consilium.europa.eu/en/press/press-releases/2022/12/12/operation-atalanta-eutm-somalia-and-eucap-somalia-mandates-extended-for-two-years/

European Council, *Strengthening the EU's external borders*, https://www.consilium.europa.eu/en/policies/strengthening-external-borders/

Europol (2022), *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg

Fabian E. (2022), "Gantz: Iran's maritime activity in Red Sea is 'most significant' in a decade", *Times of Israel*, https://www.timesofisrael.com/gantz-irans-maritime-activity-in-red-sea-is-most-significant-in-a-decade/

Fabry E. (2021), "Reducing the EU's Dependence on Chinese Imports of Rare Earths and other Strategic Minerals", in Bermann S. & Fabry E. (eds.), *Building Europe's Strategic Autonomy Vis-À-Vis China*, Institut Jacques Delors, Report n. 124

Fardella E. & Ghiselli A. (2019), "Introduction" in Fardella E. & Ghiselli A. (eds.), *China's New Role in the Wider Mediterranean Region*, Torino World Affairs Institute, ChinaMed Report 2019

Farrow A. (2014), "Drone Warfare as a Military Instrument of Counterterrorism Strategy", *Air & Space Power Journal*

Feldtein S. (2019), *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, Working Paper

Ferrara P. (2021), "As Cyber Threats Target the Wider Mediterranean Region, Countries Must Act Together", *ISPI*, https://www.ispionline.it/en/pubblicazione/cyber-threats-target-wider-mediterranean-region-countries-must-act-together-35345

Fontana G. (2018), "Droni civili per terrorismo, quali soluzioni al problema", *Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/droni-civili-a-scopo-offensivo-problemi-e-soluzioni/

Fragapane S. & Minaldi G. (2018) "Migration policies and digital technologies in Europe: a comparison between Italy and Spain", in *Journal of European Integration*, 40:7,

Franchetti Pardo L. (2020), *Sicurezza e gestione delle crisi. La dimensione marittima*, Circolo Studi Diplomatici, Dialoghi Diplomatici n. 250

Freyrie M. & Leoni R. (2022), "Come la Russia minaccia i gasdotti nel Mediterraneo", *Affari Internazionali*, https://www.affarinternazionali.it/come-la-russia-minaccia-i-gasdotti-nel-mediterraneo/

Fruganti L. (2022), "Lo Stato islamico torna a minacciare l'Europa?", *ISPI*, https://www.ispionline.it/it/pubblicazione/lo-stato-islamico-torna-minacciare-leuropa-34764

Gagliardone I. (2016), *The Politics of Technology in Africa. Communication, Development, and Nation-Building in Ethiopia*, Cambridge University Press

Ganor B. (2019), *Artificial or Human: A New Era of Counterterrorism Intelligence?*, Studies in Conflict & Terrorism

Giles K. (2016), *Handbook of Russian Information Warfare*, NATO Defense College, Rome

Giles K. (2016), *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence

Gili A. (2022), "Cavi: interessi di Stato in gioco", *ISPI*, https://www.ispionline.it/it/pubblicazione/cavi-interessi-di-stato-gioco-36487

Giroux J. (2015), *Energy Infrastructure Targeting in the Mediterranean: a Shifting Threat*, IEMed Mediterranean Yearbook 2015

Głowacka D. et al. (2021), *Digital technologies as a means of repression and social control*, Policy Department for External Relations, Directorate General for External Policies of the Union

Gomez C. (2022), "Morocco wants to increase its cobalt production for the manufacture of rechargeable batteries", *Atalayar*, https://atalayar.com/en/content/morocco-wants-increase-its-cobalt-production-manufacture-rechargeable-batteries

Gray I.W. (2016), "Cyber Threats to Navy and Merchant Shipping in the Persian Gulf", *The Diplomat*, https://thediplomat.com/2016/05/cyber-threats-to-navy-and-merchant-shipping-in-the-persian-gulf/

Gutierrez P. (2022), "Putting Unmanned Systems on Task Over the Mediterranean", *Inside Unmanned Systems*, https://insideunmannedsystems.com/putting-unmanned-systems-on-task-over-the-mediterranean/

Hambling D. (2017), "Ships fooled in GPS spoofing attack suggest Russian cyberweapon", *New Scientist*, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

Hamilton L.H. & Kean T.H. (2018), *Digital Counterterrorism: Fighting Jihadists Online*, Bipartisan Policy Centre, Task Force on Terrorism and Ideology

Hanley M., VanSant K., Pildegovičs T. (2021), *Russia's Activities In Africa's Information Environment Case Studies: Mali and Central African Republic*, NATO Strategic Communications Centre of Excellence

Hassan E. & Schaer C. (2022), "How Russia is winning the Mideast information war", *Deutsche Welle*, https://www.dw.com/en/russia-is-winning-the-information-war-in-the-middle-east/a-62900269

Hassib B. & Shires J. (2021), "Manipulating uncertainty: cybersecurity politics in Egypt", in *Journal of Cybersecurity*, Oxford University Press

Haynes D. (2021), "Iran's Secret Cyber Files", *Sky News*, https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871

Heiberg T. & Shabalala Z. (2021), "Cyber-attack disrupts major South African port operations", *Reuters*, https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/

IMB, annual piracy report 2020

INTERPOL (2022), African Cyberthreat Assessment Report

ISPI (2017), *La strategia italiana nel Mediterraneo*, MAECI, https://www.ispionline.it/sites/default/files/media/img/rapporto_med_maeci_2017_internet_1.pdf

ISPI (2021), *Dal Sahel al Mozambico: Insorgenze Jihadiste in Africa Subsahariana*, Osservatorio di Politica Internazionale, Senato della Repubblica, n. 175

Italian Ministry of Defense (2002), Libro Bianco 2002

Italian Ministry of Defense (2015), Libro Bianco 2015

Italian Ministry of Defense (2020), *Documento Programmatico Pluriennale della Difesa per Il Triennio 2020-2022*, https://www.difesa.it/Content/Documents/DPP/DPP%202020-2022.pdf

Italian Ministry of Defense (2022), Defense Policy Document 2022-2024

Italian Ministry of Defense (2022), *Strategia di Sicurezza e Difesa per il Mediterraneo 2022*

Italian Ministry of Enterprises and Made In Italy, Materie Prime Critiche, https://www.mise.gov.it/index.php/it/impresa/competitivita-e-nuove-imprese/materie-prime-critiche/materie-prime-critiche

Italian Parliament (2022), *Autorizzazione e proroga missioni internazionali nell'anno 2022*

Italian Parliament (2022), *Relazione Annuale COPASIR 2021-2022*

Janadze E. (2021), "Russia and the digital Middle East: An old game made new?", *Middle East Institute*, https://www.mei.edu/publications/russia-and-digital-middle-east-old-game-made-new

Kardon I. (2022), "China's Ports in Africa", in Rolland N. (eds.), *(In)Roads and Outposts: Critical Infrastructure in China's Africa Strategy*, National Bureau of Asian Research, Special Report no. 98

Kasapoglu C. (2022), *Techno-Geopolitics and the Turkish Way of Drone Warfare*, Atlantic Council, Issue Brief

Khazan O. (2013), "The Creepy, Long-Standing Practice of Undersea Cable Tapping", *The Atlantic*, https://www.theatlantic.com/international/archive/20

Koka A. (2022), "The Gulf Submarine Network amid Sabotage and Mine Warfare Threats", *The Euro-Gulf Information Centre*, https://www.egic.info/gulf-submarine-network-amid-sabotage-mine-warfare

Langsdorf S., Morotomi K., Rechlin A. (2022), *Tackling the EU's Dependency on Raw Materials from China: A Case Study on Rare Earth Elements and Potentials of the Circular Economy*, Friedrich Naumann Foundation for Freedom, European Dialogue Programme

Limonier, K. (2019), *The Dissemination of Russian-Sourced News in Africa*, Institut de Recherche Stratégique de l'École Militaire, Research Paper No. 66

Lipton E., Forsythe M., Searcey D. (2021), "A Power Struggle Over Cobalt Rattles the Clean Energy Revolution", *The New York Times*, https://www.nytimes.com/2021/11/20/world/china-congo-cobalt.html

Loft P. (2022), *Iran's influence in the Middle East*, House of Commons Library, Research Briefing

Lynch J. (2022), *Iron Net: Digital Repression In The Middle East And North Africa*, European Council on Foreign Relations

Magri P. (2019), "Introduction", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan

Makory J. et al. (2022), *Combating Cybercrime on Critical Infrastructure in the Region*, ALN Kenya Anjarwalla & Khanna

Marin, L., & Krajcíková, K. (2016), "Deploying drones in policing European borders: constraints and challenges for data protection and human rights", In A. Zavrsnik (Ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*

Marina Militare, *Progetti Europei*, https://www.marina.difesa.it/cosa-facciamo/per-la-difesa-sicurezza/operazioni-in-corso/Pagine/progetti_europei.aspx

Marina Militare, *Virtual Regional Maritime Traffic Centre & Trans Regional Maritime Network*, https://www.marina.difesa.it/EN/facts/Pagine/vrmtc_trmn.aspx

Marone F. (2019), "Violent Extremism and the Internet, Between Foreign Fighters and Terrorist Financing", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan

Martini L. et al. (2022), *Crises in the Mediterranean. The Italian pivot: a new strategy for European and US engagement in the MENA region*, European Council on Foreign Relations

Martino L. (2022), "Why Cyber Capacity-Building Is Essential to Achieving Stability", *ISPI*, http://www.ispionline.it/en/publication/why-cyber-capacity-building-essential-achieving-stability-35365

Mazzoni V. (2019), "Sleeping, but Present: The Cyber Activity Inspired by the Islamic State in Italy", in Marone F. (ed.), *Digital Jihad: Online Communication and Violent Extremism*, ISPI, Milan

McCants W. (2015), *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*, St. Martin's Press, New York

McKendrick K. (2019), *Artificial Intelligence Prediction and Counterterrorism*, International Security Department, Chatham House

McPherson-Smith O. (2022), "Transparency is derailing China's debt trap diplomacy", *The Hill*, https://thehill.com/opinion/international/3738211-transparency-is-derailing-chinas-debt-trap-diplomacy/

Middleton R. & Quartapelle L. (2010), *Le conseguenze della pirateria nel Corno d'Africa*, Osservatorio di Politica Internazionale, Senato della Repubblica, n.11

Morizur F. (2020), "Sea Piracy in 2025: Piracy 2.0 ?", *The Maritime Executive*, https://maritime-executive.com/blog/sea-piracy-in-2025-piracy-2-0

Muti K. & Tessari P. (2021), *Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations*, European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union

N.A. (2015), "Ethiopia: Hacking Team Lax on Evidence of Abuse", *Human Rights Watch*, https://www.hrw.org/news/2015/08/13/ethiopia-hacking-team-lax-evidence-abuse

N.A. (2021), "Resilience and collaboration, the best defense of ports against cyberattacks", *Pier Next*, https://piernext.portdebarcelona.cat/en/governance/resilience-and-collaboration-the-best-defense-of-ports-against-cyberattacks/

N.A. (2021), *Countering Terrorism Online With Artificial Intelligence: An Overview For Law Enforcement And Counter-Terrorism Agencies In South Asia And South-East Asia*, Joint Report by UNICRI and UNCCT

N.A. (2022), "Cyber security nei terminal portuali: "Lo Stato deve contribuire"", *Shipping Italy*, https://www.shippingitaly.it/2022/02/15/cyber-security-nei-terminal-portuali-lo-stato-deve-contribuire/

N.A. (2022), "Iranian forces seize two Greek tankers in the Gulf: State media", *Al Jazeera*, https://www.aljazeera.com/news/2022/5/27/greece-protests-piracy-after-tankers-seized-in-gulf

N.A. (2022), "Oil terminals disrupted after European ports hit by cyberattack", *Euronews*, https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack

N.A. (2022), "Understanding Africa's Emerging Cyber Threats", *Africa Center for Strategic Studies*, https://africacenter.org/programs/cyber/

N.A. (2023), "Wagner Group expands influence in DRC, Africa", *Robert Lansing Institute for Global Threats and Democracies Studies*, https://lansinginstitute.org/2023/01/13/wagner-group-expands-influence-in-drc-africa/

N.A., "Dal Libro Bianco 1985 al Golfo Persico", *Marina Militare*, Ministero della Difesa, https://www.marina.difesa.it/noi-siamo-la-marina/storia/la-nostrastoria/storianavale/Pagine/librobiancoMarina.aspx

Naeni A. (2021), "Iran and Africa: Why Tehran will boost its ties with the continent under the Raisi administration", *Middle East Institute*, https://www.mei.edu/publications/iran-and-africa-why-tehran-will-boost-its-ties-continent-under-raisi-administration

Nakashima E. & Warrick J. (2020), "Officials: Israel linked to a disruptive cyberattack on Iranian port facility", *The Washington Post*, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

NATO (2012), Alliance Maritime Strategy, https://www.nato.int/cps/en/natohq/official_texts_75615.htm

Nelson J. & Romero A. (2022), Why Europe's energy industry is vulnerable to cyberattack, European Council on Foreign Relations

Newman N. (2019), "Cyber pirates terrorising the high seas", *Institution of Engineering and Technology*, https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/

Nocera L. (2021), "Perspectives on the New Centrality of the Mediterranean States: The Role of Turkey in a Changing Region" in F. M. Corrao and R. Redaelli (eds.), *States, Actors and Geopolitical Drivers in the Mediterranean*, Palgrave MacMillan

Nocetti J. (2019), *Dazed And Confused: Russian "Information Warfare" And The Middle East – The Syria Lessons*, EuroMesc Policy Brief, n. 93

Ogunlana O.S. (2019), "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies", in *Journal of Strategic Security*, Vol. 12, No. 1

Perfetti F. (2011), "Mediterraneo e Medio Oriente nella politica estera italiana", in *La Comunità internazionale*, fasc.2

Picard R. (2022) , "Cybersecurity in Energy Markets: Challenges and Opportunities", in MEDREG Consumer Working Group, *The Digitalization of Energy Markets And The New Role Of Consumers*, Association of Mediterranean Energy Regulators

Puntas I.B. (2022), *The use of drones for maritime surveillance and border control*, Centre Delàs d'Estudis per la Pau, Working Paper

Rassler D. (2018), *The Islamic State and Drones: Supply, Scale and Future Threats*, Combatting Terrorism Center at West Point, United States Military Academy

Reva D. (2021), *Maritime cyber security: Getting Africa ready*, Institute for Security Studies, Africa Report 29

Riccardi L. (2020), “Italy’s foreign policy and the Palestinian question”, in Monzali L. & Soave P. (eds.), *Italy and the Middle East*, Bloomsbury Publishing

Rossi E. (2021), “Indo-Pacifico? L’Europa si concentri sul Mediterraneo Allargato. Il monito di Lloyd Austin”, *Formiche*, https://formiche.net/2021/07/indo-pacifico-lloyd-austin/

Rumer E. & Sokolsky R. (2021), *Russia in the Mediterranean: Here to Stay*, Carnegie Endowment for International Peace

Schori Liang C. (2015), “Cyber Jihad: Understanding and Countering Islamic State Propaganda”, *Geneva Centre for Security Policy*, n.1

Sherman J. (2022), “Internet Security Under the Ocean: EU-US Must Cooperate on Submarine Cable Security”, *ISPI*, https://www.ispionline.it/en/pubblicazione/internet-security-under-ocean-eu-us-must-cooperate-submarine-cable-security-35471

Siegle J. (2021), “Russia and Africa: Expanding Influence and Instability”, in Graeme P. Herd, (ed.), *Russia's Global Reach: a Security and Statecraft Assessment. Garmisch-Partenkirchen*: George C. Marshall European Center for Security Studies

Sistema di Informazione per la Sicurezza della Repubblica (2022), *Relazione Annuale sulla Politica dell’Informazione per la Sicurezza*

Sistema di Informazione per la Sicurezza della Repubblica (2022), Relazione Annuale sulla Politica dell’Informazione per la Sicurezza

Spadoni G. (2019), *IRGC Cyber-Warfare Capabilities*, International Institute for Counterterrorism

SRM (2022), Italian Maritime Economy Report 2022

Stavridis J. (2015), “A New Cold War Deep Under the Sea?”, *Huffington Post*, https://www.huffpost.com/entry/new-cold-war-under-the-sea_b_8402020

Sukhankin S. (2020), “Russian Inroads Into Central Africa”, in *Eurasia Daily Monitor*, The Jamestown Foundation, Vol. 17, Issue 56

Sunak R. (2017), *Undersea Cables: Indispensable, insecure*, Policy Exchange, Westminster, London

Szkarłat M. & Katarzyna M. (2016), *New Technologies as a Factor of International Relations*, Cambridge Scholars Publishing

Tarabay J. (2022), “An Underwater Hack and the Digital Ripple Effects”, *Bloomberg*, https://www.bloomberg.com/news/newsletters/2022-04-20/an-underwater-hack-and-the-digital-ripple-effects

Tugendhat H. & Voo J. (2021), *China’s Digital Silk Road in Africa and the Future of Internet Governance*, School of Advanced International Studies, Johns Hopkins University, China Africa Research Initiative, Working Paper n. 50

Tull D.M. (2021), *Operation Barkhane and the Future of Intervention in the Sahel*, Stiftung Wissenschaft und Politik German Institute for International and Security Affairs, Comment n. 5

Turato M. (2022), “La difesa europea delle infrastrutture sottomarine”, *Formiche*, https://formiche.net/2022/10/difesa-europea-sottomarina/

UN Office of Counterterrorism (2022), *Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS)*, Global Programme on Countering Terrorist Threats against Vulnerable Targets

UNODC (2012), *Contribution to the United Nations Integrated Regional Strategy for the Sahel*

Venturi, B. (2018), “Africa and Italy’s Relations After the Cold War”, In: Nagar, D., Mutasa, C. (eds) *Africa and the World*. Palgrave Macmillan

Vidino L., Marone F., Entenmann E. (2017), *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West* , ISPI in partnership with the International Centre for Counter-Terrorism – The Hague (ICCT) and the Program on Extremism at George Washington University

Wiese Bockmann M. (2019), “Seized UK tanker likely ‘spoofed’ by Iran”, *Lloyd’s List*, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

Yayboke E. & Reid C. (2022), *Counterterrorism from the Sky? How to Think Over the Horizon about Drones*, Center for Strategic and International Studies

Zaimi G. (2022), “Iran’s Balkan front: The roots and consequences of Iranian cyberattacks against Albania”, *Middle East Institute*, https://www.mei.edu/publications/irans-balkan-front-roots-and-consequences-iranian-cyberattacks-against-albania

Zayani M. (2018), “Mapping the Digital Middle East: Trends and Disjunctions”, In Zayani M. (ed.), *Digital Middle East: State and Society in the Information Age*, Oxford University Press

Zorloni L. (2021), “L'Europa finanzia anche con aiuti umanitari sorveglianza digitale in Africa e nei Balcani”, *Wired*, https://www.wired.it/attualita/tech/2021/10/19/europa-sorveglianza-digitale-africa-balcani-cepol/