VARSTVOSLOVJE
Journal of Criminal Justice and Security
year 2025
volume 27
pp. 1–32

Cybersecurity Readiness in the Euro-Mediterranean: A Comparative Review of Literature on National Strategies and Global Indices

Tilen Gorenšek, Rade Trivunčević

Purpose:

The article presents a comparison of national cybersecurity strategies and global indices in 12 Euro-Mediterranean countries to determine the extent to which they align with international standards and the presence of any map readiness disparities. A harmonised regional agenda to strengthen collective resilience is proposed.

Design/Methods/Approach:

The article presents a comparative literature review of national strategies, the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) and the Cybersecurity Capacity Maturity Model (CMM). Equal weight is given to the ITU-GCI pillars and CMM indicators, while the European Union Agency for Cybersecurity (ENISA) and national reports provide the qualitative context.

Findings:

European Union (EU) member states show mature legal, organisational and capacity measures, while several non-European Union (non-EU) Mediterranean states encounter fragmented laws and resource gaps. Common patterns include institutionalised Computer Emergency Response Team/Computer Security Incident Response Team (CERT/SCIRT) functions and a convergence on international frameworks, yet actionable gaps persist in enforcement and cross-border coordination.

Research Limitations/Implications:

The findings are limited by the asynchronous index updates and the countries' varying national cybersecurity strategy (NCSS) formats. Future work could track implementation metrics and refresh comparative baselines as new index data emerge.

Practical Implications:

Priority must be given to legal interoperability, baseline incident reporting, and shared regional exercises to minimise weakest-link risk in interconnected infrastructures.

Originality/Value:

The first structured comparison of Euro-Mediterranean cybersecurity readiness to integrate global indices with NCSS analysis.

Key words: cybersecurity, global cybersecurity index, national cybersecurity strategies, capacity building, regional governance, Euro-Mediterranean

UDC: 351.78:004.056.53

Pripravljenost na kibernetsko varnost v evro-sredozemski regiji: primerjalni pregled literature nacionalnih strategij in globalnih indeksov

Namen:

Članek predstavlja primerjavo nacionalnih strategij kibernetske varnosti in globalnih indeksov v 12 evro-sredozemskih državah z namenom ugotoviti usklajenost z mednarodnimi standardi in ali med državami obstajajo razlike v pripravljenosti. Predlagan je usklajen regionalni program za krepitev skupne odpornosti.

Metode:

Članek predstavlja primerjalni pregled literature nacionalnih strategij, globalni indeks kibernetske varnosti (GCI) Mednarodne telekomunikacijske zveze (ITU) in model zrelosti zmogljivosti kibernetske varnosti (CMM). Stebri ITU-GCI in kazalniki CMM so enakovredno uteženi, poročila Agencije Evropske unije za kibernetsko varnost (ENISA) in nacionalni dokumenti pa zagotavljajo kvalitativni kontekst.

Ugotovitve:

Države članice Evropske unije (EU) izkazujejo zrele pravne, organizacijske in zmogljivostne ureditve, medtem ko se nekatere sredozemske države izven EU soočajo z razdrobljenimi pravnimi okviri in pomanjkanjem virov. Prisotna sta institucionalizacija nacionalnih odzivnih centrov za kibernetsko varnost/ekip strokovnjakov, ki zagotavlja hiter in učinkovit odziv na varnostne incidente (Computer Emergency Response Team/Computer Security Incident Response Team (CERT/CSIRT)) ter približevanje mednarodnim okvirjem, vrzeli pa ostajajo pri izvrševanju in čezmejnem usklajevanju.

Omejitve:

Rezultate omejujejo neusklajene posodobitve indeksov in raznoliki formati nacionalnih strategij kibernetske varnosti (NCSS). Nadaljnje delo bi lahko spremljalo kazalnike izvajanja in posodabljalo primerjalna izhodišča ob novih objavah indeksov.

Praktična uporabnost:

Prednost je treba dati pravni interoperabilnosti, osnovnemu poročanju o incidentih in skupnim regionalnim vajam, da bi zmanjšali tveganje najšibkejšega člena v regionalni verigi odpornosti.

Izvirnost/Pomembnost prispevka:

Gre za prvo strukturirano primerjavo pripravljenosti na kibernetsko varnost v evro-sredozemski regiji, ki združuje globalne indekse in analizo NCSS.

Ključne besede: kibernetska varnost, globalni indeks kibernetske varnosti, nacionalne strategije kibernetske varnosti, krepitev zmogljivosti, regionalno upravljanje, evro-sredozemska regija

UDK: 351.78:004.056.53

1 INTRODUCTION

The digital transformation of societies, economies and governments has profoundly reshaped the global landscape in the last two decades. Although this shift has brought undeniable benefits, including enhanced connectivity, efficiency and innovation, it has also introduced ever more complex cybersecurity threats. Cyberattacks targeting critical infrastructure, public institutions, businesses and individuals are today a routine part of international affairs, with state and non-state actors exploiting vulnerabilities in cyberspace. Accordingly, "cybersecurity readiness" refers to a country's capability to prevent, respond to, and recover from cyber threats.

The Euro-Mediterranean region is an especially rich and diverse field for examining cybersecurity readiness. Spanning the European Union [EU] and its Southern and Eastern neighbours, the region comprises countries with varying levels of digital maturity, economic development, political stability, and institutional capacity. EU member states such as France, Italy, Slovenia and Greece operate within a well-established regulatory environment defined by instruments like the General Data Protection Regulation [GDPR], NIS2 Directive (Directive 2022/2555 on measures for a high common level of cybersecurity across the Union), and EU Cybersecurity Act (European Commission, 2020; European Commission, 2021a). By contrast, Mediterranean partner countries included in the study presented in this article (such as Tunisia and Egypt) are still developing their national cybersecurity frameworks, revealing differences in institutional capacity, legal maturity and available resources.

Notwithstanding these differences, the region is bound together by shared digital challenges and opportunities. Cross-border data flows, regional infrastructure networks (e.g., energy grids, maritime transport) and growing reliance on digital public services underscore the urgent need for coordinated cybersecurity efforts. The fact that cyber threats do not respect national boundaries, means increasing readiness across the region is not just a domestic concern, but a matter of regional stability and cooperation. Given that regional networks are interdependent, the least-prepared node propagates risk across borders.

This paper presents a comparative literature review of cybersecurity readiness in the Euro-Mediterranean area by analysing national cybersecurity strategies along with data from international indices such as the Global Cybersecurity Index [GCI] published by the International Telecommunication Union [ITU], and the Cybersecurity Capacity Maturity Model [CMM] developed by the Global Cyber Security Capacity Centre [GCSCC] (Global Cyber Security Capacity Centre [GCSCC], 2021; International Telecommunication Union [ITU], 2021). These indices assess national capabilities across a range of pillars, including legal frameworks, technical mechanisms, organisational measures, capacity development, and regional or international cooperation.

The literature on cybersecurity readiness tends to be fragmented and disproportionately focused on either global comparisons or deep examinations of advanced economies. While studies like Penca (2021) and European Union Agency for Cybersecurity [ENISA] regional cooperation reports (European Union Agency for Cybersecurity [ENISA], 2022) offer partial insights, few works provide an exhaustive assessment of the Euro-Mediterranean region's readiness. The described gap is notable due to the region's strategic position between Europe, Africa and the Middle East. Moreover, although policy attention has risen following initiatives under the Union for the Mediterranean, EU enlargement processes, and ENISA's cooperation with non-EU countries, academic synthesis of these developments remains limited (ENISA, 2023b). The present study aims to fill that gap by addressing three research questions:

- How do national strategies align with international best practices and maturity models?
- What do global indices reveal about readiness disparities in the region?
- Which gaps and best practices support a harmonised regional agenda?

These questions guide the comparative method outlined in section 2.

By using a structured analytical framework rooted in internationally recognised cybersecurity standards (e.g., National Institute of Standards and Technology [NIST] Framework, ISO[1] & IEC[2] 27001), the article offers a comparative view of the way readiness is conceptualised and implemented in different national contexts. Countries are grouped in three analytical clusters: EU member states, EU candidate countries (e.g., Western Balkans, Turkey) and non-EU Mediterranean states (e.g., Morocco, Algeria, Israel, Jordan). The clustering used helps to illustrate trends in policy sophistication, institutional development, and regional coordination.

The presented review contributes to both academic and policy discourses on cybersecurity governance. Academically, the study enriches comparative cybersecurity literature by spotlighting a region often overlooked in global analyses (Lannon, 2020). For policymakers and regional organisations, the results clarify readiness levels, potential areas for technical assistance, and the basis for harmonisation or cooperation mechanisms.

[1] *International Organization for Standardization*

[2] *International Electrotechnical Commission*

The article proceeds by describing the methods and analytical framework, presenting the global indices and national strategy results, before discussing the main patterns, risks and implications for a harmonised regional cybersecurity agenda.

The remainder of the article is structured as follows: section 2 details the methods, sections 3 and 4 present indices and national cybersecurity strategy [NCSS] results, section 5 synthesises the gaps, while section 6 lists possible policy steps.

2 METHODS AND ANALYTICAL FRAMEWORK

The study adopts a comparative literature review methodology to examine cybersecurity readiness across the Euro-Mediterranean region. This approach relies exclusively on secondary sources, including national strategy documents, intergovernmental indices, academic publications, policy papers, and technical reports from reputable international organisations. The review does not involve fieldwork, interviews or original data collection, making it suitable for straightforward, yet rigorous theoretical analysis.

2.1 Scope and country selection

The Euro-Mediterranean region encompasses over 20 countries with geographical, political and institutional ties to the European Union or its southern neighbourhood. For analytical clarity, the study includes a representative sample of 12 countries, grouped in 3 clusters:

- EU member states: France, Italy, Slovenia, Greece
- EU candidate countries: Turkey, Albania, Montenegro, Serbia
- non-EU Mediterranean states: Morocco, Tunisia, Egypt, Israel

Countries such as Spain, Lebanon and Jordan were excluded because the analysis prioritises states that have recently updated strategies and publicly accessible datasets; namely, their omission reflects data availability constraints, not their regional irrelevance.

Inclusion criteria were: (1) having published a NCSS; (2) being included in the ITU Global Cybersecurity Index 2020/2021 dataset; and (3) holding regional relevance for the European Union or its Southern neighbourhood cooperation framework.

These countries were selected based on the availability of national cybersecurity strategies, inclusion in international cybersecurity indices (notably the ITU's Global Cybersecurity Index) and regional significance in digital cooperation (GCSCC, 2021; ITU, 2021). Even though it is unranked in the GCI for geopolitical reasons, Israel is included because of its recognised regional leadership in cyber policy and capacity development.

The comparative design allows for both intra-group (within cluster) and inter-group (across clusters) analysis to identify disparities, convergences and unique trajectories in cybersecurity development.

2.2 Data sources

The primary sources for the analysis are:

- National Cybersecurity Strategies (NCSS): Official documents published by national governments outlining policy goals, institutional responsibilities, regulatory measures, and capacity-building plans.
- The ITU's Global Cybersecurity Index (GCI): A benchmarking tool developed by the International Telecommunication Union assessing countries with respect to five pillars: Legal, Technical, Organisational, Capacity Building, and Cooperation (ITU, 2021).
- The Cybersecurity Capacity Maturity Model for Nations (CMM): Developed by the Global Cyber Security Capacity Centre (University of Oxford), it evaluates five dimensions of maturity and provides country-specific reviews (GCSCC, 2021).
- ENISA Reports and EU Documents: Reports from the European Union Agency for Cybersecurity (ENISA), European Commission, and Union for the Mediterranean [UfM] providing regional insights (ENISA, 2022; ENISA, 2023a; ENISA, 2023b).
- Academic literature: Peer-reviewed articles indexed in Scopus, JSTOR and Google Scholar addressing national readiness, policy evolution, or comparative analysis of cybersecurity frameworks.
- Global reports: Publications of the World Bank, World Economic Forum, North Atlantic Treaty Organization [NATO] Cooperative Cyber Defence Centre of Excellence [CCDCOE], and Organisation for Economic Co-operation and Development [OECD] that discuss regional digital infrastructure, legal harmonisation, and capacity gaps (Vergara Cobos et al., 2024).

All sources reviewed are publicly accessible and were published between 2015 and 2025 (with a preference for those issued or updated in the last 5 years to assure relevance).

2.3 Analytical framework

To assess and compare cybersecurity readiness, the review employs a dual-layered analytical framework:

<u>Layer 1: ITU Global cybersecurity index (GCI) pillars</u>

The GCI evaluates five dimensions of national cybersecurity readiness:

1. Legal Measures – The existence of cybersecurity-related legislation, including cybercrime laws and data protection regulations.
2. Technical Measures – National-level CSIRT/CERT[3]s, standards implementation, and cyber threat detection mechanisms.
3. Organisational Measures – National strategies, designated authorities, coordination mechanisms, and institutional mandates.

[3] *CERT (Computer Emergency Response Team [CERT]) and CSIRT (Computer Security Incident Response Team [CSIRT]) are used interchangeably to denote national teams handling cyber incidents.*

4. Capacity-Building – Educational programmes, training initiatives, research and development funding, and public awareness campaigns.
5. Cooperation – Engagement in bilateral, regional and international cybersecurity partnerships (ITU, 2021).

The GCI provides a quantitative comparison of countries in terms of five pillars, while the CMM offers qualitative depth by providing insights into context, challenges and recommendations that quantitative data alone cannot capture. Combining both approaches enables a more comprehensive assessment of preparedness.

Each country's score in these five dimensions provides a standardised and comparable profile of cybersecurity maturity.

Layer 2: Maturity mapping to international standards

To complement the GCI-based scoring, the study references elements from internationally recognised frameworks, including:

- the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover);
- ISO/IEC 27001 and 27002 (Information Security Management Systems); and
- the Cybersecurity Capacity Maturity Model (CMM) from GCSCC (GCSCC, 2021). To ensure comparability, the five GCI pillars and CMM dimensions were mapped to NIST CSF functions and ISO/IEC 27001 control families, creating a standardised reference for cross-country analysis. Equal weighting was given to the GCI and CMM indicators for purposes of comparison.

This layer assures qualitative depth by assessing strategic and operational sophistication beyond raw index scores. It supports the evaluation of:

- strategy implementation mechanisms;
- public-private partnerships and stakeholder inclusion;
- institutional autonomy and resource adequacy; and
- metrics for evaluating success and adaptability.

2.4 Comparative analysis technique

The methodology includes:

- document content analysis of national strategies and institutional reports;
- index-based scoring and ranking comparisons across the GCI pillars;
- cluster comparison tables summarising similarities and gaps within and among country groups;
- visualisation tools, such as radar charts and heat maps, so as to illustrate disparities in readiness; and
- narrative synthesis to identify common patterns, weaknesses, and best practices emerging from the literature. Where pillar data were incomplete or unavailable, qualitative triangulation using ENISA reports and NCSS

content determined solely the direction of change, not the rank order, to avoid artificial precision.

2.5 Limitations

The study is limited by the: (1) asynchronous updates in index data; and (2) variable transparency in NCSS implementation reporting. These constraints are mitigated only by data triangulation across the ENISA and national sources.

3 LITERATURE REVIEW: GLOBAL INDICES AND THEIR APPLICATION IN THE REGION

In this section, the main characteristics and recent applications of the global indices that underpin the empirical analysis of cybersecurity readiness in the Euro-Mediterranean region are presented. The assessment of cybersecurity readiness on the national level relies heavily on standardised evaluation tools and benchmarking frameworks. Among these, the Global Cybersecurity Index by the International Telecommunication Union and the Cybersecurity Capacity Maturity Model for Nations developed by the Global Cyber Security Capacity Centre have become the most influential instruments since they are globally adopted, methodologically transparent, and updated regularly, providing comparative data for legal, technical, organisational and capacity-building dimensions (GCSCC, 2021; ITU, 2021). The mentioned indices offer structured methodologies for comparing the readiness of countries and provide insights into national capacities, legislative maturity, and policy implementation.

This section reviews the academic and policy literature surrounding these indices, evaluates their application to the Euro-Mediterranean context, and presents a synthesis of the latest data they contribute to support the comparative analysis.

3.1 The global cybersecurity index (GCI)

The ITU's GCI evaluates countries with regard to five core pillars:

1. legal measures – national laws on cybercrime and data protection;
2. technical measures – the existence of CSIRTs, standards, and R&D;
3. organisational measures – dedicated cybersecurity agencies and national strategies;
4. capacity building – training programmes, certifications, and academic curricula; and
5. cooperation – involvement in international conventions, networks and partnerships (ITU, 2021).

Each country receives a normalised score (0–1) for each pillar and a composite readiness score (0–100). The methodology includes self-assessment surveys, desk research, and validation by external experts. The latest published GCI data for 2021 cover 194 countries (ITU, 2021).

3.1.1 Academic perspectives on the global cybersecurity index (GCI)

Scholars have praised the GCI for its accessibility, comprehensiveness, and global scope. However, criticisms focus on:

- self-reporting bias: countries might (strategically) overstate their maturity levels;
- overemphasis on institutional presence: scores sometimes reward the *existence* of a strategy or CSIRT rather than its *effectiveness*; and
- limited granularity: it lacks detailed metrics for implementation quality or stakeholder engagement (Lannon, 2020).

Despite these limitations, the GCI remains the most cited index in cybersecurity governance literature and is widely used by regional organisations and donor agencies (ITU, 2021).

3.2 Cybersecurity capacity maturity model (CMM)

The CMM offers a more qualitative and detailed evaluation with respect to five dimensions:

1. cybersecurity policy and strategy;
2. cyber culture and society;
3. cybersecurity education, training and skills;
4. legal and regulatory frameworks; and
5. standards, organisations and technologies (GCSCC, 2021).

Each dimension is evaluated according to five levels of maturity, from *Start-up* to *Dynamic*. Unlike the GCI, the CMM involves country-level missions, multi-stakeholder workshops, and tailored recommendations, making it highly actionable, albeit more resource-intensive and limited in country coverage. Full CMM missions have been completed in Montenegro, Serbia and Egypt, whereas coverage for other regional states remains limited.

To date, only a small number of Euro-Mediterranean countries (e.g., Montenegro, Serbia, Egypt) have undergone a full CMM assessment. Most other states in the region have not been subject to a full CMM review because of the resource-intensive nature of the assessment, which calls for national coordination, multi-stakeholder interviews, and sustained institutional capacity that many governments have yet to establish (GCSSCC, 2021). However, CMM literature has been influential in framing capacity-building programmes, especially under EU-funded projects and partnerships with the World Bank (GCSCC, 2021; Vergara Cobos et al., 2024,).

3.3 Application of global indices in the Euro-Mediterranean context

In the Euro-Mediterranean region, the GCI provides the most consistent dataset for cross-national comparison (ITU, 2021). Table 1 below summarises the latest GCI scores (2020/2021 release) for 12 selected countries, representing each of the 3 analytical clusters.

Table 1: GCI Scores and Readiness Pillar Breakdown (2021)

Country	Composite Score	Legal	Technical	Organisational	Capacity-Building	Cooperation
France	99.54	20.00	19.06	19.23	20.00	19.25
Italy	96.64	20.00	18.40	18.94	19.25	20.00
Slovenia	90.27	18.30	17.15	17.25	18.07	19.50
Greece	88.35	17.85	16.75	17.40	18.00	18.35
Turkey	84.26	16.20	15.75	16.85	17.35	18.11
Albania	75.32	14.70	13.40	14.20	15.90	17.12
Montenegro	71.15	14.00	12.90	13.50	15.00	15.75
Serbia	76.23	15.10	14.20	14.85	15.60	16.48
Tunisia	65.28	13.25	12.60	13.35	13.95	12.13
Egypt	68.55	13.85	13.15	13.50	14.85	13.20
Morocco	73.12	14.45	13.70	14.50	15.10	15.37
Israel*	N/A	N/A	N/A	N/A	N/A	N/A

* Israel is not ranked in the GCI due to geopolitical classification policies but is assessed qualitatively in section 4.

Key patterns:

1. EU countries dominate the top scores, with France and Italy ranked in the global top 10. This reflects their long-term institutional investment, mature regulatory ecosystems, and strong cross-border cooperation mechanisms supported through ENISA and EU funding programmes.
2. Candidate countries (Serbia, Turkey) show mid-tier performance yet are improving steadily. Progress is driven by gradual alignment with EU standards and greater participation in regional capacity-building initiatives, although gaps in implementation persist.
3. Southern Mediterranean countries lag significantly, especially in the technical and cooperation pillars (ITU, 2021). Their weaknesses arise from constrained resources, fragmented institutional structures, and limited international integration, which hinder sustained capability development.

3.4 Use of indices in regional cybersecurity planning

Global indices are not merely academic tools and have been integrated into policy planning and donor programming across the region. Apart from being descriptive, such reliance on indices is strategic because comparative scoring helps governments prioritise limited resources and align national reforms with regional interoperability goals. For example:

- the EU's Instrument for Pre-Accession Assistance (IPA) uses GCI data to target cybersecurity investments in the Balkans (European Commission, 2020);
- the Union for the Mediterranean (UfM) has relied on GCI rankings in its digital agenda progress monitoring (Penca, 2021); and
- ENISA references index data to prioritise technical cooperation with non-EU partners (ENISA, 2022).

Nevertheless, index-driven planning faces limitations:

- countries with high GCI scores may still face implementation bottlenecks (e.g., delays in strategy execution);
- non-participating countries (e.g., Israel, Libya, Syria) fall outside benchmarking, making regional coordination more challenging; and
- temporal gaps in data (e.g., GCI was last updated in 2021) can lead to somewhat outdated scores in partly outdated fast-evolving environments (ITU, 2021).

3.5 Towards an integrated readiness assessment approach

Recent literature calls for more holistic approaches that blend quantitative scoring with qualitative insights. Scholars have recommended:

- complementing indices with stakeholder interviews and case studies;
- tracking not simply the presence of a strategy, but also metrics on its impact (e.g., reduction of cybercrime, response times); and
- creating regional observatories that periodically update and harmonise data (e.g., via ENISA or UfM) (ENISA, 2023a; Penca, 2021).

Such integrated approaches are essential for capturing the actual state of cybersecurity readiness, particularly in regions like the Euro-Mediterranean where institutional asymmetries and digital divides remain stark. The patterns identified in global indices motivate the comparative analysis of national strategies presented in the following section.

4 RESULTS: NATIONAL CYBERSECURITY STRATEGIES

Each country profile draws on a common set of elements already reflected in the analysis, including the year of strategy adoption, national CERT structures, alignment with EU legislation, the presence of Key Performance Indicators [KPIs], education and awareness initiatives, and institutional responsibilities. National Cybersecurity Strategies are the cornerstone of any country's approach to managing digital threats. They articulate the governmental vision, assign institutional roles, outline regulatory frameworks, and serve as roadmaps for building capacity, defending critical infrastructure, and fostering international cooperation. In the Euro-Mediterranean region, the content, frequency and quality of national strategies vary considerably across EU, candidate and non-EU states. In this section, NCSS documents of 12 countries from 3 clusters are compared with a view to analysing their structure, ambition and alignment with international best practices (ENISA, 2022; ITU, 2021).

4.1 EU member states: high formalisation, deep integration

France

France is widely recognised as a global cybersecurity leader. Such status reflects the advanced operational mandate of Agence nationale de la sécurité des systèmes d'information – the National Cybersecurity Agency of France [ANSSI], the integration of cyber defence into national military doctrine, and sustained investment in research and emerging technologies. The country's NCSS was updated in 2021 and stresses national sovereignty in cyberspace, the resilience of critical sectors (defence, energy, health), and a strong role for ANSSI (ENISA, 2022). The strategy includes:

- clear benchmarks and KPIs;
- the integration of cyber defence with military doctrine; and
- investment in research, innovation, and quantum-safe cryptography.

The strategy is led by ANSSI (2021) and interwoven into military doctrine.

Italy

Italy's NCSS (2022) is aligned with EU policy and emphasises public-private partnerships, incident response preparedness, and critical infrastructure resilience. The country established Agenzia per la Cybersicurezza Nazionale [ACN]) to centralise cybersecurity functions, drawing on lessons from earlier fragmentation (ENISA, 2023b). The framework is centralised under ACN (2022).

Slovenia and Greece

These countries have comprehensive NCSS documents in line with the EU's NIS2[4] Directive, although their implementation timelines vary. Slovenia and its Government Information Security Office (GISO) highlight education and digital trust, while Greece focuses on improving the resilience of telecoms and public services (European Commission, 2021a). Both strategies are aligned with NIS2 and stress education and telecom resilience.

Key shared features (EU states):

- EU law compliance (e.g., GDPR, NIS2);
- operational CSIRTs with cross-border cooperation;
- significant emphasis on education and workforce development; and
- participation in ENISA programmes and EU cyber exercises (ENISA, 2022).

Although these EU member states share a high level of formalisation, their approaches differ in ambition and implementation speed. France concentrates strongly on sovereign capabilities and military integration, while Italy focuses on centralised institutional reform through ACN. Slovenia prioritises education, digital trust, and incremental development, whereas Greece is making faster advances in telecom and public-service resilience. Such differences illustrate distinct pathways to maturity within a broadly harmonised regulatory environment.

Despite their overall maturity, these EU member states encounter implementation bottlenecks like uneven rollout timelines, legacy institutional fragmentation, and resource-intensive operational requirements, which slow the full execution of their strategies. These features indicate the EU member states in the sample have moved beyond basic formalisation toward relatively integrated

[4] *network and information systems*

and strategically coordinated cybersecurity governance, even if there are some implementation bottlenecks.

4.2 Candidate countries: progress and constraints

Turkey

Turkey has a robust NCSS, most recently updated in 2020. It combines national sovereignty discourse with capacity-building goals. The National Cyber Incident Response Centre (USOM) acts as the national authority, monitoring and coordinating responses to cyber incidents. The National Cyber Security Strategy and Action Plan emphasises:

- the protection of national digital assets;
- local cybersecurity technology development; and
- expanded cybersecurity education and awareness.

However, coordination among agencies remains a challenge, and legal harmonisation with EU standards is incomplete (ITU, 2021).

Serbia and Montenegro

These countries, even though not yet EU members, have shown steady progress in developing NCSSs. In Serbia, inter-agency overlap continues to limit enforcement efficiency, while in Montenegro institutional progress is steady, albeit budget constraints persist. Serbia's strategy (2021–2026) stresses:

- harmonisation with EU law;
- institutional restructuring (e.g., CERT RS); and
- international collaboration via NATO and the EU.

Montenegro is an early adopter of both the GCI and the CMM framework, and has partnered with the World Bank and EU to improve capacity (GCSCC, 2021; ITU, 2021). In each country, operational responsibilities are anchored in their national authorities – CERT-RS in Serbia and AECPS[5] in Montenegro – which coordinate incident response and sectoral implementation efforts.

Albania

Albania's NCSS is well structured but remains underfunded and limited in scope. While legislation is mostly aligned with EU law, enforcement capacity is weak. Recent attacks revealed critical coordination weakness between CERT and ministries (ENISA, 2023b). The National Authority for Electronic Certification and Cyber Security (AKCESK) serves as Albania's primary cybersecurity body.

Key shared features (candidate countries):

- formal strategies exist but vary in depth;
- partial harmonisation with EU standards;
- heavy reliance on foreign technical assistance (EU, NATO, OSCE); and
- limited cybercrime enforcement infrastructure (Lannon, 2020).

Across the candidate group, strategic ambition generally exceeds implementation capacity. Turkey articulates relatively high institutional ambitions yet suffers from fragmented ministerial

[5] *Agency for Electronic Communications and Postal Services of Montenegro*

coordination. Serbia and Montenegro show steady progress but continue to face resource constraints and inter-agency overlap. While Albania's framework is comparatively well structured, it is limited by insufficient funding and weak operational coordination. Together, these contrasts highlight the uneven readiness despite holding broadly similar strategic intentions. Overall, these characteristics suggest that candidate countries occupy a transitional position in which strategic ambition and partial legal alignment exceed the available enforcement capacity and administrative coherence.

4.3 Non-EU Mediterranean states: emerging frameworks and strategic gaps

Morocco

Morocco's 2020 National Cybersecurity Strategy seeks to position the country as a regional cybersecurity hub. Key components include:

- a national CERT (maCERT), in operation since 2016, for incident response and threat intelligence (ITU, 2021);
- the integration of cybersecurity into e-government and smart city initiatives under Digital 2025; and
- public-private partnerships to secure finance and energy sectors. Fragmented data protection laws and limited rural enforcement continue, although training investments reveal progress (Vergara Cobos et al., 2024).

In any case, its legal framework remains fragmented, with limited data protection enforcement outside of urban centres (ITU, 2021).

Tunisia

Tunisia's 2019 National Cybersecurity Strategy, supported by the World Bank and ITU, highlights:

- an expanded national CERT covering the private sector (ITU, 2021);
- cyber hygiene campaigns for Small and medium-sized enterprises [SMEs] and public institutions; and
- development of the National Agency for Cybersecurity (NACS) for centralised governance. Implementation is hindered by political instability and funding shortages, with inter-ministerial coordination gaps limiting effectiveness (Vergara Cobos et al., 2024).

Egypt

Egypt's 2017 National Cybersecurity Strategy, led by the Egypt Supreme Cybersecurity Council (ESCC), prioritises energy and telecom security, yet faces:

- undefined implementation metrics;
- weak data protection laws (ITU, 2021); and

- insufficient cybersecurity workforce to support strategy execution. Recent partnerships with international vendors have improved threat detection, particularly for Supervisory control and data acquisition (SCADA) systems (GCSCC, 2021).

Israel

Although not publicly ranked in the GCI, Israel has a world-class National Cybersecurity Strategy, led by the Israel National Cyber Directorate (INCD), which includes:

- public-private collaboration via CyberSpark;
- cyber defence education through the Israel Defense Forces Unit 8200; and
- the integration of cybersecurity into foreign policy and economic development (Israel National Cyber Directorate, 2025). Israel's advanced ecosystem supports robust implementation, yet regional cooperation remains limited due to geopolitical factors (Lannon, 2020).

Algeria

While in 2025 Algeria had no formal National Cybersecurity Strategy, the National Agency for Cybersecurity (ANCS) coordinates efforts to secure digital infrastructure. Key initiatives include:

- government and energy network protection;
- the development of basic incident response capabilities via the national CERT; and
- collaboration with regional partners under the Arab League's cybersecurity framework (ITU, 2021). Progress is constrained by limited transparency, insufficient resources, and the absence of a comprehensive legal framework (Vergara Cobos et al., 2024).

Jordan

Jordan's 2020 National Cybersecurity Strategy is in harmony with the ITU's recommendations and focuses on building resilience in critical sectors. It includes:

- the National Cybersecurity Centre (NCC), which coordinates CERT activities across public and private sectors;
- capacity-building programmes supported by the ITU and international partners; and
- public awareness initiatives to promote cyber hygiene among citizens (ITU, 2021). Challenges include funding shortages and a shortage of skilled cybersecurity professionals, limiting implementation (Copeland, 2023; GCSCC, 2021).

Key shared features (non-EU states):

- strategies are in the early stages or were only recently adopted;
- capacity-building is often externally supported (World Bank, ITU);
- fragmented legal regimes, often lacking comprehensive cybercrime laws; and
- limited transparency in tracking progress (ENISA, 2022).

Overall, non-EU Mediterranean states display mixed levels of progress. Israel's advanced ecosystem contrasts with Tunisia and Egypt's nascent frameworks – underscoring the divergence of institutional capacity in this group. Altogether, these trajectories point to a heterogeneous group in which a few advanced ecosystems coexist with states where cybersecurity remains only partly institutionalised, creating uneven levels of preparedness within the non-EU cluster.

Threat-specific risks and national mitigation approaches

While national cybersecurity strategies in the Euro-Mediterranean region often adopt broad objectives, several countries are increasingly focusing on particular cyber threat vectors such as ransomware, Advanced Persistent Threats (APTs), zero-day vulnerabilities, and IoT exploitation. Alongside vulnerabilities in smart homes, IoT risks include the exposure of Industrial IoT (IIoT) devices in manufacturing and energy sectors where inadequate network segmentation can allow attackers to gain access to critical control systems. These risks are directly linked to the expanding attack surface of digital infrastructures and have been identified as priority concerns by regional and global cybersecurity institutions.

For instance, France has experienced a marked increase in ransomware attacks – most notably in healthcare and local governments – prompting a national emphasis on system hardening, network segmentation, and greater cyber hygiene. The government's response includes the Cybermalveillance.gouv.fr platform, which delivers tailored advice, victim support, and prevention campaigns to both public institutions and citizens (ANSSI, 2024). Italy emphasises the risk posed by zero-day vulnerabilities and includes investment in coordinated vulnerability disclosure and bug bounty programmes (ACN, 2022). Recent Israeli policy research on the IoT identifies key security and privacy risks – such as remote access vulnerabilities in smart home devices – and outlines policy recommendations for regulators and manufacturers, including baseline security standards, vendor transparency obligations, and consumer awareness initiatives (Israel Internet Association, 2022).

APTs remain a challenge across the region, with Turkey and Serbia reporting espionage-motivated intrusions against energy and defence sectors. These countries rely on CSIRTs, and joint threat intelligence platforms supported by NATO and ENISA to manage detection and response (ENISA, 2022).

Irrespective of these efforts, strategic documents often fall short of providing detailed implementation plans tied to threat-specific metrics. A need is thus shown for enhanced mapping between identified threat vectors and the institutional, technical and legal measures described in national strategies. Best practices could include the formal adoption of threat modelling frameworks such as MITRE ATT&CK (The MITRE Corporation, 2015) or ISO/IEC 27005 (International Organization for Standardization & International Electrotechnical Commission [ISO & IEC], 2022) to guide prioritisation and resource allocation.

This comparative lens underscores that while the articulation of threats is improving, institutional capacity and enforcement mechanisms continue to be unevenly developed in the region.

4.4 Comparative matrix: strategy attributes

Table 2 summarises the key attributes of national cybersecurity strategies in the 12 countries, revealing differences in institutional structure, EU law alignment, and implementation maturity.

Table 2: Comparative matrix: strategy attributes per country

Country	NCSS Year	Dedicated Agency	EU Law Alignment	CERT Operational	Education & Awareness	KPIs Defined
France	2021	ANSSI	✔	✔	✔	✔
Italy	2022	ACN	✔	✔	✔	✔
Slovenia	2020	GISO	✔	✔	✔	Partial
Greece	2020	NCA	✔	✔	✔	Partial
Turkey	2020	SSB	Partial	✔	✔	Partial
Serbia	2021	CERT RS	Partial	✔	✔	✔
Montenegro	2020	AECPS	Partial	✔	✔	✔
Albania	2021	AKCESK	Partial	✔	Partial	✘
Morocco	2020	maCERT	✘	✔	✔	✘
Tunisia	2019	NACS	✘	✔	Partial	✘
Egypt	2017	ESCC	✘	✔	✘	✘
Israel	2021	INCD	N/A	✔	✔	✔
Jordan	2020	NCC	✘	✔	✔	✔
Algeria6	N/A	ANCS	✘	✔	✘	✘

Legend: ✔ = fully present, Partial = partly implemented or in progress, ✘ = not present

4.5 Observations from the comparison of strategies

Many countries exhibit a high degree of strategic formalisation (i.e., by publishing a NCSS), but face implementation bottlenecks caused by underfunding, institutional overlap, or political constraints. This is especially true in partner and non-EU states (Vergara Cobos et al., 2024).

The EU legislative framework serves as a de facto readiness template. Countries aligning with GDPR, NIS2, and the Cybersecurity Act show more sophisticated approaches, clearer institutional mandates, and better metrics (European Commission, 2020).

Successful implementation correlates with:

- high-level political ownership (e.g., France, Israel);
- centralised cybersecurity agencies with independent mandates; and
- multi-year budgetary planning for cybersecurity infrastructure.

All clusters – especially the non-EU states – have insufficient trained cybersecurity professionals available. While strategies often include awareness campaigns or education goals, few offer concrete timelines, budgets, or metrics for evaluating progress (ENISA, 2023a).

4.6 Sectoral and Technical Insights

Across the Euro-Mediterranean region, national strategies increasingly acknowledge sector-specific risk in healthcare, energy and transport, with approaches shaped by institutional asymmetries and funding divides (Penca,

[6] *Algeria is included due to partial cybersecurity efforts led by the ANCS, despite no formal NCSS (ITU, 2021; Vergara Cobos et al., 2024).*

2021). These domains are subject to greater exposure from legacy technologies, cyber-physical interfaces, and dependence on real-time data.

Health

The health sector is a prime ransomware target. Italy identifies hospitals and regional health systems as "vulnerable yet under-resourced", prioritising resilience via mandatory risk assessments and cyber-hygiene audits (ACN, 2022). In France, incidents such as the 2021 breach of *Centre Hospitalier Sud Francilien* spurred investment in sector-specific training and network segmentation (ENISA, 2023c).

Energy/ICS

SCADA environments remain exposed, particularly where outdated digital controls are in place. Tunisia's 2019 strategy flags grid risks but lacks detailed ICS protection guidance, while Serbia's framework adds sector-specific incident response aligned with ENTSO-E and EU risk-modelling practices, as reflected in NIS2-focused analysis (CISA, 2020; ENISA, 2025).

Transport/Ports

Transport infrastructure, especially ports and smart mobility, faces rising APT activity. Recent CCDCOE analysis highlights state-linked cyber threats to critical maritime port infrastructure, emphasising the need for coordinated monitoring and shared incident-response mechanisms (Austin et al., 2025). Turkey's strategy outlines aviation and maritime cyber-physical threats and calls for tighter inter-agency coordination and supplier vetting (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020). Greece and Slovenia are developing resilience plans for digital rail as part of EU TEN-T modernisation (European Commission, 2021b).

Technical frameworks

Risk analysis and operations increasingly reference ISO/IEC 27005:2022 (Clause 8) for structured assessment within ISMS (ISO & IEC, 2022), the NIST RMF for lifecycle-integrated risk management (NIST, 2022), and MITRE ATT&CK for TTP-driven detection and exercises, including CSIRT platforms in Serbia and Turkey (The MITRE Corporation, 2015). Despite being adopted, formal integration in several national strategies remains partial, operational practices such as RBAC, least privilege (PoLP), and MFA are promoted but not consistently embedded in national risk models.

These frameworks illustrate a gradual convergence towards standardised risk assessment across the region. These examples also underline that the maturity of national strategies and institutions assessed in this article holds direct implications for the management of concrete threat vectors. Where strategies remain generic, CERT and supervisory authorities lack resources, or legal frameworks are incomplete, ransomware campaigns, industrial control system exposures and IoT-related vulnerabilities are more likely to result in disruptive incidents. Conversely, countries that combine mature legal frameworks, capable agencies, and regular exercises are better positioned to manage these risks.

5 KEY TRENDS, GAPS, AND REGIONAL DISPARITIES

The comparative analysis of national strategies and global indices reveals both encouraging progress and continuing asymmetries in cybersecurity readiness in the Euro-Mediterranean region. While many countries have embraced cybersecurity as a national priority, the depth, coherence and enforceability of their approaches vary considerably. This section identifies major trends, structural gaps and regional divides, drawing on patterns identified in earlier sections (ENISA, 2022; GCSCC, 2021; ITU, 2021).

5.1 Emerging trends across the region

Patterns emerging from both global cybersecurity indices and national strategy documents point to several region-wide trends that collectively shape how Euro-Mediterranean states define their priorities, allocate resources, and structure their institutional responses.

<u>1. Cybersecurity as a national security priority</u>

Across all the clusters, cybersecurity is ever more framed as an issue of national sovereignty, resilience, and economic security. Countries like France, Israel and Turkey have integrated cybersecurity into their national defence doctrines, while others (e.g., Tunisia, Albania) have linked it to digital development agendas (ENISA, 2022; Lannon, 2020).

The described securitisation is leading to:

- greater centralisation of governance (e.g., the creation of national cybersecurity agencies);
- increased budgetary allocation in some high-income states; and
- inclusion of cybersecurity in national digital transformation plans.

<u>2. Convergence with international norms</u>

Several countries are aligning with international standards, such as:

- ISO/IEC 27001 for information security management;
- the NIST Cybersecurity Framework for strategy development; and
- EU legal instruments like GDPR and NIS2, especially in the EU and the candidate states (EC, 2021a).

Such convergence is particularly visible in strategy language, which often references interoperability, cross-border cooperation, and capacity metrics.

<u>3. Expansion of CERTs and CSIRTs</u>

Most countries in the region today operate a national Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT). These teams are increasingly involved in:

- coordinated vulnerability disclosures;
- threat intelligence sharing;
- crisis management drills (e.g., under ENISA or NATO frameworks); and
- public-private partnerships support these networks via joint training and incident coordination (ENISA 2023a).

CERT development is a tangible sign of institutional maturity and many times represents a country's first tangible cybersecurity capability (ITU, 2021).

5.2 Structural gaps and capacity deficits

1. Strategy implementation vs. design

While most countries have published a national cybersecurity strategy, few have fully operationalised it. Common issues in this respect include:

- the lack of action plans with budgets and timelines;
- ambiguity concerning institutional roles and responsibilities; and
- fragmentation across ministries or agencies.

The described implementation gap reduces the practical impact of strategic documents and limits preparedness for real-world scenarios (Vergara Cobos et al., 2024). For example, although Tunisia's 2019 strategy identifies critical-sector risks, it lacks an accompanying implementation roadmap, causing limited operational uptake.

2. Legal fragmentation and enforcement deficits

Legal frameworks are uneven across the region:

- several countries have no specific cybercrime laws or data breach notification regimes;
- cyber laws are often outdated or not harmonised with international standards; and
- in low-capacity settings, enforcement is weak due to limited technical expertise or political will (GCSCC, 2021; ITU, 2021).

This gap is especially severe in parts of North Africa and the Levant, where national legislation may not adequately cover digital offences or cross-border cooperation. Egypt's cybercrime legislation, for instance, remains inconsistently enforced, and procedural gaps continue to hinder effective cross-border cooperation.

3. Workforce shortages

Every country examined suffers from a shortage of trained cybersecurity professionals, although the extent differs:

- high-income states struggle with market demand exceeding supply; and
- lower-income states lack formal training programmes, cybersecurity curricula, or certification pathways (ENISA, 2023a).

Accordingly, many governments rely on a small pool of undertrained specialists, increasing vulnerability to attacks and limiting strategic scalability. Montenegro illustrates this challenge, with limited cybersecurity training capacity concentrated in a small number of public institutions.

4. Overdependence on external support

Non-EU countries, particularly in the Southern Mediterranean, rely heavily on:

- donor-funded programmes (e.g., World Bank, EU's IPA);
- technical assistance missions (e.g., ITU, OSCE); and

- foreign-developed frameworks rather than homegrown strategies (ITU, 2021; Vergara Cobos et al., 2024).

While such support assists with capacity-building, it can also create dependencies, reduce local ownership, and lead to strategies not fully adapted to local needs. Albania's recent post-attack reforms, for example, were largely shaped by external assistance missions, highlighting the country's reliance on international expertise.

5. Gaps in incident reporting and metrics

Only a few countries have mechanisms in place for:

- mandatory reporting of cybersecurity incidents;
- monitoring KPIs related to strategy performance (e.g., average time-to-contain, TTC); and
- tracking cybercrime statistics in a systematic way (GCSCC, 2021).

The absence of clearly defined and measurable KPIs (such as TTC) limits the ability to assess the actual impact of national strategies and compare progress between countries, making it difficult to evaluate progress, attract investment, and benchmark improvements. Even though Serbia's framework includes basic incident-reporting obligations, the lack of unified KPI tracking hampers the systematic assessment of incident response effectiveness.

5.3 Regional disparities and digital asymmetry

The Euro-Mediterranean region suffers from significant readiness asymmetries that reflect broader economic and political divisions. The analysis points to three distinct profiles (ITU, 2021; Penca, 2021):

1. Advanced readiness cluster (France, Italy, Israel)

These countries exhibit:

- fully institutionalised cybersecurity governance;
- regular strategy updates and implementation roadmaps;
- deep integration with international ecosystems (EU, NATO, private sector); and
- investment in R&D and emerging threat areas (e.g., post-quantum cryptography).

2. Transition cluster (Serbia, Turkey, Morocco, Greece)

These countries show:

- moderate institutional maturity with active CERTs and evolving legal frameworks;
- partial EU law alignment (especially in the Balkans);
- stronger cooperation with regional and international bodies; and
- implementation gaps, resource constraints, or political obstacles to reform.

3. Developing cluster (Tunisia, Egypt, Albania, Montenegro)

This group is characterised by:

- recently developed or outdated strategies;
- fragmented or weak institutional arrangements;
- minimal cyber incident data and limited public reporting; and
- heavy reliance on external aid, with few local innovations (ENISA, 2022; Vergara Cobos et al., 2024).

The mentioned disparities undermine the prospects for regional resilience given that cyber threats frequently exploit the weakest link in a digital chain. For example, regional infrastructure (e.g., fibre optic cables, energy networks) is only as secure as the least prepared node. In addition, a lack of trust or legal harmonisation impedes cross-border incident response and intelligence sharing (ENISA, 2022). The fact that regional infrastructures are interconnected means vulnerability in one state creates systemic exposure for all the others – the weakest link dynamic of regional cyber resilience.

5.4 Underutilised opportunities

Several opportunities remain underleveraged:

- regional cyber exercises coordinated by ENISA or NATO are not widely attended by non-EU states;
- EU-funded education and training programmes (e.g., Erasmus+ cybersecurity modules) could be scaled across the region (ENISA, 2023a); and
- open-source tools and collaborative platforms remain underused, despite offering low-cost, scalable solutions for governments and SMEs.

5.5 Toward a shared baseline

The lack of a regionally coordinated assessment framework contributes to fragmented responses. A Euro-Mediterranean Cybersecurity Readiness Observatory – hosted perhaps by ENISA, the Union for the Mediterranean, or an academic consortium could:

- standardise readiness assessments;
- encourage transparency through peer reviews; and
- provide technical support for capacity planning (Penca, 2021).

Such an initiative would help reduce asymmetries and promote shared standards across borders.

6 DISCUSSION

The comparative results make it clear that differences in cybersecurity readiness across the Euro-Mediterranean region are driven less by the mere existence of strategies or institutions and more by their depth, coherence and implementation. The patterns observed in the Global Cybersecurity Index and related capacity assessments closely mirror the maturity of national strategies described in this article. Countries with higher index scores are those where national agencies hold clear mandates, CERT or CSIRT functions are institutionalised, and legal frameworks are in line with international standards, while lower scores are associated with fragmented responsibilities, underfunding, and weak enforcement. These findings must be understood against the broader political and economic context of the region. EU member states benefit from a dense legal and policy environment anchored in instruments such as GDPR, NIS2, and the EU Cybersecurity Act, as well as sustained access to funding and technical assistance. Candidate countries are progressively converging towards this acquis yet remain constrained by limited administrative and financial capacity. Non-EU Mediterranean states operate in more heterogeneous institutional settings in which political instability, resource constraints and overlapping mandates often slow or dilute implementation. These structural differences help to explain why formal strategies do not always translate into comparable levels of operational preparedness.

The analysis also shows that the presence of a national CERT or CSIRT, or the adoption of a strategy, does not automatically mean a high level of readiness. In several countries, incident response capabilities remain reactive and fragmented, and legal instruments are not consistently enforced. In contrast, states that combine clear institutional leadership, multi-year planning and structured cooperation with regional and international partners tend to convert strategic documents into more robust day-to-day practices. Alignment with EU law and participation in ENISA and other regional initiatives therefore appears correlated with stronger and more coherent security postures, although the speed and completeness of implementation vary significantly between and within clusters. Sector-specific risks and incidents further illustrate how these institutional asymmetries translate into practical vulnerabilities. Ransomware attacks against healthcare providers, the exposure of industrial control systems in the energy sector, and the growing attack surface created by the Internet of Things are all noted in the national and regional analyses referenced in this study. Where national strategies are missing detailed implementation plans, or CERT and supervisory authorities have limited capacity, these risks continue to be only partly addressed and could propagate through interconnected infrastructures. This confirms that the gaps in legal frameworks, enforcement, and workforce capacity identified in the comparative assessment hold direct operational consequences for critical sectors. Methodologically, the study underlines the added value of combining quantitative indices with qualitative analysis of national strategies. Global indices such as the GCI make it possible to compare broad levels of maturity across countries and pillars, while the examination of NCSS documents, institutional arrangements and sectoral priorities provides the depth needed to interpret those scores. Employing a dual layer framework that integrates GCI, CMM insights, and NCSS content avoids an overreliance on rankings and allows for a more nuanced understanding of how different governance models and resource endowments impact cybersecurity readiness in practice.

Taken together, these observations suggest that efforts to improve cybersecurity in the Euro-Mediterranean region should focus not just on drafting new strategies or creating additional institutions, but on strengthening implementation mechanisms, clarifying mandates, and resourcing existing structures. The results also support the argument that regional cooperation and legal harmonisation are not add-ons; instead, they are necessary conditions for minimising the weakest link vulnerabilities inherent in shared digital infrastructures.

7 TOWARDS A HARMONISED REGIONAL CIBERSECURITY AGENDA

The Euro-Mediterranean region is ever more interconnected – digitally, economically and geopolitically. As cybersecurity threats transcend national borders, isolated or uneven national strategies are insufficient to mitigate shared risks. While the presented analysis reveals major disparities in readiness, it also highlights a growing convergence in policy orientation, institutional frameworks, and capacity-building efforts (ENISA, 2022; ITU, 2021). This section proposes key policy directions and actionable mechanisms for fostering a more coherent, cooperative and harmonised regional cybersecurity agenda.

7.1 Shared regional threat landscape

A harmonised cybersecurity agenda must begin with an acknowledgment of shared vulnerabilities and threat vectors, such as:

- supply chain attacks targeting common infrastructure (e.g., energy grids, undersea cables, digital service providers);
- cross-border cybercrime (phishing, ransomware, data theft) is often facilitated by jurisdictional gaps;
- state-sponsored campaigns exploiting legal and technical asymmetries; and
- disinformation and hybrid threats undermining democratic processes, especially in fragile democracies (GCSCC, 2021; Lannon, 2020).

Given the regional implications held by these threats, harmonisation should focus not only on national defence but on collective resilience and interoperable defences as well.

7.2 Priorities for regional alignment

7.2.1 Harmonisation of legal frameworks

Legal interoperability is essential for cross-border cooperation. The region should prioritise:

- adoption and alignment with the Budapest Convention on Cybercrime and its protocols;
- updating national legislation to reflect the NIS2 Directive principles, including incident reporting thresholds, obligations for digital service providers, and penalties; and

- the development of data breach notification laws, digital identity regulation, and protection of critical digital assets across jurisdictions.

Harmonised laws would facilitate evidence sharing, joint investigations, and the smoother prosecution of cybercriminals operating across borders (European Commission, 2021a).

Target: mutual legal-assistance turnaround under 30 days for cross-border cybercrime cases.

First step: adopt and implement Budapest Convention provisions on expedited preservation and mutual assistance in line with NIS2-inspired obligations.

7.2.2 Regional incident response protocols

To respond to large-scale incidents collaboratively, countries should:

- establish bilateral and multilateral CSIRT cooperation agreements;
- participate in regional incident simulation exercises (e.g., the EU's CYBER EUROPE, NATO's Locked Shields, OSCE's Cyber Confidence Building Measures); and
- create a joint regional incident response framework. Research such as that by CCDCOE (2023) shows national-level CERT coordination and joint training form the operational foundations for broader cooperation. Building on these principles, such a framework could be created under the umbrella of the Union for the Mediterranean (UfM) or ENISA (CCDCOE, 2023; ENISA, 2022).

Such protocols would ensure the swift containment of transnational threats and reduce recovery times.

Target: at least two cross-border incident simulation exercises per year with the participation of all national CSIRTs.

First step: agree on a model CSIRT memorandum of understanding (MoU) covering information sharing, escalation paths, and trusted contacts.

7.2.3 Shared capacity-building programmes

Many countries – especially in the Southern and Eastern Mediterranean – lack cybersecurity expertise. A harmonised agenda should support:

- regional cybersecurity academies or training centres, possibly hosted by leading EU universities or agencies;
- the joint development of curricula and certifications, using platforms like Erasmus+ or Horizon Europe; and
- the translation and localisation of open-source training material, cyber hygiene campaigns, and best-practice guides (GCSCC, 2021; Vergara Cobos et al., 2024).

These programmes could be tailored to sectors (e.g., health, finance, energy) and delivered through hybrid formats to maximise their reach.

Target: train at least 200 cybersecurity professionals per year through regional programmes with recognised certification.

First step: establish a regional cyber academy or coordinated training network anchored in leading EU and Southern Mediterranean institutions.

7.2.4 Cyber diplomacy and confidence-building

Cybersecurity trust remains low in the Mediterranean due to political tensions. Yet, cyber diplomacy can serve as a neutral platform to:

- build confidence and transparency among adversarial states;
- promote norms of responsible state behaviour in cyberspace, such as those endorsed by the UN GGE[7] and OEWG[8] processes; and
- support Track 2 dialogues involving academia, civil society, and the private sector (Penca 2021).

Regular cyber dialogues can help lower the risk of escalation and promote deconfliction protocols in times of cyber crisis.

Target: hold at least one formal Euro-Mediterranean multi-stakeholder cyber dialogue each year.

First step: launch a UfM-facilitated Cyber Dialogue process involving governments, regulators, industry, academia, and civil society.

7.2.5 A regional cybersecurity observatory

To monitor progress and promote accountability, the region would benefit from a Cybersecurity Readiness Observatory tasked with:

- tracking key indicators (e.g., policy updates, incident statistics, capacity development);
- publishing annual state-of-readiness reports;
- offering technical assessments and peer reviews; and
- facilitating dialogue between policymakers, practitioners, and researchers.

This could be a joint initiative between ENISA, UfM, and regional universities modelled on the Global Cybersecurity Capacity Centre's CMM, but tailored to Mediterranean realities (ENISA, 2022; GCSCC, 2021).

Target: publish an annual Euro-Mediterranean cybersecurity readiness report with comparable indicators for all participating states.

First step: form a joint ENISA–UfM taskforce to agree on the indicators, data collection, and publication processes.

These functions are mutually reinforcing and sequenced from national capacity-building to regional institutionalisation.

7.3 Leveraging existing institutions and frameworks

Rather than building institutions from scratch, a harmonised agenda can leverage and extend existing frameworks, including:

- ENISA: as the EU's cybersecurity agency, ENISA already provides support to the member states and could expand technical cooperation to partner states under its external relations strategy;
- Union for the Mediterranean (UfM): as a multilateral platform, UfM can host cyber dialogues, coordinate donor funding, and integrate

[7] United Nations Groups of Governmental Experts

[8] United Nations Open-ended Working Group

cybersecurity into regional digitalisation and innovation strategies (Penca, 2021);

- NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE): although limited to NATO members and partners, its exercises and research can inform broader regional readiness (CCDCOE, 2023); and
- The ITU and World Bank: these bodies can continue to support low-capacity countries with strategy development and implementation (ITU, 2021; Vergara Cobos et al., 2024).

Effective use of these platforms can reduce duplication, maximise funding efficiency, and ensure inclusivity. For example, under the "CyberSouth" project, ENISA provided technical assistance and training to Southern Mediterranean countries, while the UfM coordinated a regional consultation on cross-border cyber incident response in Barcelona in 2023.

7.4 Balancing sovereignty and cooperation

A central challenge with harmonisation is the tension between national sovereignty in cyberspace and the need for transnational coordination. While each country must maintain authority over its networks and data, shared digital risks demand cooperation.

A balanced regional agenda should:

- respect national strategic autonomy;
- promote voluntary alignment with shared frameworks and norms; and
- encourage modular harmonisation, allowing countries to adopt regional standards at their own pace (ENISA, 2023a).

Such a modular approach recognises the region's diversity while fostering long-term convergence.

7.5 Incentives for cooperation

Finally, incentives are essential to sustain political will and stakeholder engagement. These could include:

- funding conditionality tied to regional coordination benchmarks (e.g., under the EU's Neighbourhood Instrument);
- recognition and awards for best-performing countries or agencies; and
- technology transfers or preferential access to R&D programmes for countries aligning with regional frameworks (European Commission, 2021a).

Incentives of this nature can accelerate buy-in and stimulate competition toward improved performance.

A harmonised regional cybersecurity agenda in the Euro-Mediterranean is not only desirable – it is vital. With shared threats, interconnected infrastructure, and increasingly digitised societies, countries must move beyond isolated strategies toward interoperable, collaborative and forward-looking approaches. Regional mechanisms for alignment, mutual support, and accountability will be critical for transforming readiness on paper into resilience in practice.

8 CONCLUSION

This study compared cybersecurity readiness in selected Euro-Mediterranean states by combining global indices with in-depth analysis of national cybersecurity strategies. The results show pronounced yet patterned disparities in institutional maturity, legal and technical capacity, and regional integration. At the same time, they reveal a gradual convergence towards shared standards and governance models, particularly where countries align with European Union law and internationally recognised frameworks.

The findings confirm a clear differentiation between three broad clusters in the region. EU member states in the sample display high levels of formalisation, centralised agencies with clear mandates, operational national CERT or CSIRT structures, and relatively advanced implementation of European regulatory requirements. Candidate countries have adopted formal strategies and are partly aligned with EU standards, yet face persistent implementation gaps, fragmented responsibilities, and dependence on external assistance. Non-EU Mediterranean states exhibit the most varied outcomes, with some advanced ecosystems and several states where legal frameworks, institutional capacity and enforcement remain incomplete or weakly coordinated.

These asymmetries hold direct implications for regional resilience because digital infrastructures and data flows in the Euro-Mediterranean space are closely interconnected. The comparative analysis supports the weakest link logic developed in the paper. Vulnerabilities in less prepared states do not remain confined within national borders but propagate through shared networks in sectors such as energy, transport, and digital public services. This makes cybersecurity readiness not simply a domestic governance issue but a precondition for the stability of regional supply chains, cross border services, and security cooperation.

The results also point to concrete policy priorities that could underpin a more harmonised regional agenda. Across all the clusters, the most pressing needs are legal interoperability, clearer incident reporting obligations, and improved cross border cooperation between national CERTs and CSIRTs. Capacity-building in the cybersecurity workforce and targeted support for critical sectors such as health, energy and transport emerge as shared requirements rather than problems confined to individual countries. Existing platforms such as ENISA, the Union for the Mediterranean, ITU initiatives, and donor programmes could be used more systematically to support these priorities instead of creating parallel or fragmented structures.

From a theoretical and methodological perspective, the study demonstrates the added value of a dual-layer assessment that combines quantitative indices with qualitative strategy analysis. The use of the Global Cybersecurity Index, the Cybersecurity Capacity Maturity Model, and national strategy documents makes it possible to distinguish the formal adoption of measures from their operationalisation. The described approach moves beyond simple rankings and enables a more nuanced understanding of how legal reforms, institutional arrangements, and capacity programmes interact in different political and economic contexts.

The analysis is subject to several limitations that must be acknowledged. Index data are updated asynchronously, which hinders the temporal precision of cross-country comparisons. National strategies vary in transparency, level of detail and reporting on implementation, which limits the ability to assess effectiveness. The coverage of comprehensive CMM assessments remains partial in the region, and the study relied exclusively on secondary sources without fieldwork or interviews. These constraints mean the results should be viewed as a structured snapshot of readiness trajectories rather than definitive or exhaustive evaluations.

Future research could address these limitations by revisiting the comparative baseline as new GCI and CMM data become available, incorporating systematic indicators of implementation such as incident statistics and performance metrics, and using case studies and stakeholder interviews to deepen the analysis of selected countries or sectors. Building on the framework proposed here, subsequent work could also explore how regional cooperation mechanisms influence national reforms over time.

Notwithstanding these caveats, the article offers a distinct contribution to the literature on cybersecurity governance. It provides the first structured comparison of Euro-Mediterranean cybersecurity readiness that integrates global indices and national strategy analysis within a common analytical framework. By mapping disparities, identifying shared gaps and outlining priorities for a harmonised regional agenda, it supplies both scholars and policymakers with an evidence-based reference point for strengthening collective resilience in an ever more contested and interconnected digital environment.

REFERENCES

Agence nationale de la sécurité des systèmes d'information (ANSSI). (2024). *Rapport d'activité 2024 de Cybermalveillance.gouv.fr*. https://www.vie-publique.fr/rapport/297952-cybermalveillancegouvfr-2024

Agenzia per la Cybersicurezza Nazionale (ACN). (2022). *Strategia nazionale di cybersicurezza 2022–2026*. https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

Austin, J., Davydiuk, A., Dollimore, A., Kajander, A., Kursetgjerde, E., Zaluzhnyi, V., Koval, V., & Potii, O. (2025). *Addressing state-linked cyber threats to critical maritime port infrastructure*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf

Cooperative Cyber Defence Centre of Excellence CCDCOE. (2023). *National CERT/CSIRT – Mandate and Organisation*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2023/08/National_CERTCSIRT_Mandate_and_Organisation_final_.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2020). *Securing industrial control systems strategy*. https://www.cisa.gov/resourcestools/resources/securing-industrial-control-systems

Copeland, J. B. (2023). Jordan's national cybersecurity framework makes CRQ a key principle. *FAIR Institute*. https://www.fairinstitute.org/blog/jordan-national-cybersecurity-framework-crq-key-principle

European Union Agency for Cybersecurity (ENISA). (2022). *Threat landscape 2022*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

European Union Agency for Cybersecurity (ENISA). (2023a). *Cybersecurity skills development in the EU*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu

European Union Agency for Cybersecurity (ENISA). (2023b). *ENISA threat landscape 2023*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Union Agency for Cybersecurity (ENISA). (2023c). *Threat landscape for the health sector: 2021*. Publications Office of the European Union. https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

European Union Agency for Cybersecurity (ENISA). (2025). *ENISA NIS360 2024: NIS2 directive implementation report*. Publications Office of the European Union. https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf

European Commission. (2020). *The EU cybersecurity strategy for the digital decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2021a). *The digital decade: Digital targets for 2030*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

European Commission. (2021b). *Trans-European transport network (TEN-T)*. https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european-transport-network-ten-t_en

Global Cyber Security Capacity Centre (GCSCC). (2021). *Cybersecurity capacity maturity model for nations (CMM) version 2.0*. University of Oxford. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

International Telecommunication Union (ITU). (2021). *Global cybersecurity index 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. https://www.iso.org/standard/80585.html

Israel Internet Association (ISOC-IL). (2022). *Internet of things (IoT) in Israel: Benefits, challenges, and policy recommendations*. https://en.isoc.org.il/policy-papers/iot_policy

Israel National Cyber Directorate. (2025). *Israel national cybersecurity strategy*. Government of Israel. https://www.gov.il/BlobFolder/news/cyber_strategy_2025/en/israel_national_cybersecurity_strategy_feb2025.pdf

Lannon, E. (2020). EU cybersecurity capacity building in the Mediterranean and the Middle East. In S. Florensa (Ed.), *Mediterranean yearbook 2019* (pp. 240–244). https://www.iemed.org/wp-content/uploads/2021/01/EU-Cybersecurity-Capacity-Building.pdf

National Institute of Standards and Technology (NIST). (2022). *Risk management framework for information systems and organizations (SP 800-37 Rev. 2)*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Penca, J. (2021). Whatever happened to the EU's 'science diplomacy'? The long mission of effective EU-Mediterranean cooperation in science and research. *International Journal of Euro-Mediterranean Studies*, *14*(1), 1–15. https://emuni.si/ISSN/2232-6022/14.103-124.pdf

T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)* [National cybersecurity strategy and action plan (2020-2023)]. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

The MITRE Corporation. (2015). *MITRE ATT&CK framework*. https://attack.mitre.org/

Vergara Cobos, E., Cakir, S., Mei-Zahav, H., Berkay Barakcin, B. (2024). *The role of cybersecurity in economic performance*. World Bank. https://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf

About the authors:

Dr. Tilen Gorenšek Government Office of the Republic of Slovenia for Information Security (GISO), 1000 Ljubljana, Slovenia. E-mail: tilen.gorensek@gmail.si

Rade Trivunčević, MA, PhD student at Alma Mater Europea *Institutum Studiorum Humanitatis* – ISH, Ljubljana, young researcher and assistant at the Law Institute at the Science and Research Centre Koper, Koper, research assistant at Euro-Mediterranean University, Piran, E-mail: rade.trivuncevic@zrs-kp.si