GLOBAL JOURNAL
OF COMPUTER SCIENCE AND TECHNOLOGY - G: INTERDISCIPLINARY
Volume 26 | 2026 Article ID: GJCST-258858 Language: English

Structural Readiness for Cyber Diplomacy in the Algorithmic Age: Cybersecurity Capacity and Digital Governance in Selected EU Countries

Online First

Ioana-Cristina VASILOIU[§§*]

PhD Candidate, Research Assistant

ORCID 0009-0006-6787-4433

***Corresponding Author**

§ National Institute for Research and Development in Informatics - ICI Bucharest, Bucharest University of Economic Studies, Bucharest, Romania (**OA**)

RECEIVED	ACCEPTED	ONLINE PUBLISHED	PEER REVIEW
2026-06-24	2026-07-04	2026-07-14	Double Blind

Abstract

This article analyses the structural preparedness for cyber diplomacy in the algorithmic age by examining whether the selected European Union member states possess relevant cybersecurity capacity and digital governance conditions to support data-driven cyber governance. It provides a Cyber-Digital Readiness Index (CDRI), an exploratory proxy for structural preparedness, based on four variables: the Global Cybersecurity Index, the National Cybersecurity Index, the E-Government Development Index, and the Network Readiness Index. An analysis of the CDRI applied to 12 EU member states from Central, Eastern, Baltic, South-Eastern Europe demonstrates that, even though cybersecurity capabilities are critical, they are insufficient in isolation. In addition to cybersecurity capability, structural preparedness is strengthened by digital public-sector maturity, network preparedness, data governance, and inter-institutional interoperability; accountability for the utilisation of algorithmic systems also remains a critical governance issue. The study further indicates that Estonia represents the most robust example in the sample. In contrast, Romania records high cybersecurity scores and low digital development measures, resulting in a large cyber-digital deficit. The study ultimately concluded that structural preparedness for cyber diplomacy in the algorithmic age depends on the combined development of cybersecurity maturity and digital governance capacity.

cyber diplomacy | cybersecurity capacity | digital governance | readiness assessment | European Union

AI USE STATEMENT
No generative AI was used for analysis or results.

FUNDING
No external funding was declared for this work.

CONFLICT OF INTEREST
The authors declare no conflict of interest.

DATA AVAILABILITY
Not applicable for this article.

ETHICS
No ethics committee approval was required for this article type.

CONSENT
Not applicable for this article.

TRIAL REG.
Not applicable.

Crossref DOI: 10.34257/GJCSTG258858

How to Cite: VASILOIU (2026). Structural Readiness for Cyber Diplomacy in the Algorithmic Age: Cybersecurity Capacity and Digital Governance in Selected EU Countries. Global Journal of Computer Science and Technology, Ahead of Print, 1-15. DOI: 10.34257/GJCSTG258858

AR Experience Web Page DOI

Print ISSN 0975-4350

Online ISSN 0975-4172

Under the strict compliance and defined process of

METADATA CONTINUATION

AUTHOR CONTACT QR LEDGER

Ioana-Cristina VASILOIU§θ*

ARCHIVAL RECORD

GJCST · Vol 26 · 2026

Article ID GJCST-258858 · DOI 10.34257/GJCSTG258858

Print ISSN 0975-4350 · Online ISSN 0975-4172

Global Journal of Computer Science and Technology - Section G
GJCST

Structural Readiness for Cyber Diplomacy in the Algorithmic Age: Cybersecurity Capacity and Digital Governance in Selected EU Countries

Ioana-Cristina VASILOIU[§ϑ*] iD

Affiliations
§ National Institute for Research and Development in Informatics - ICI Bucharest, Bucharest University of Economic Studies, Bucharest, Romania (OA)

Qualifications / Designations
ϑ PhD Candidate, Research Assistant

Abstract

This article analyses the structural preparedness for cyber diplomacy in the algorithmic age by examining whether the selected European Union member states possess relevant cybersecurity capacity and digital governance conditions to support data-driven cyber governance. It provides a Cyber-Digital Readiness Index (CDRI), an exploratory proxy for structural preparedness, based on four variables: the Global Cybersecurity Index, the National Cybersecurity Index, the E-Government Development Index, and the Network Readiness Index. An analysis of the CDRI applied to 12 EU member states from Central, Eastern, Baltic, South-Eastern Europe demonstrates that, even though cybersecurity capabilities are critical, they are insufficient in isolation. In addition to cybersecurity capability, structural preparedness is strengthened by digital public-sector maturity, network preparedness, data governance, and inter-institutional interoperability; accountability for the utilisation of algorithmic systems also remains a critical governance issue. The study further indicates that Estonia represents the most robust example in the sample. In contrast, Romania records high cybersecurity scores and low digital development measures, resulting in a large cyber-digital deficit. The study ultimately concluded that structural preparedness for cyber diplomacy in the algorithmic age depends on the combined development of cybersecurity maturity and digital governance capacity.

Keywords: *cyber diplomacy, cybersecurity capacity, digital governance, readiness assessment, European Union*

*** Corresponding Author**
Ioana-Cristina VASILOIU

DOI
10.34257/GJCSTG258858

1. Introduction

Cyber diplomacy has evolved into an essential tool to manage conflict, cooperation, and governance in cyberspace. Due to the increasing number of cyber incidents affecting critical infrastructure, the public and private sectors, and civilians, cybersecurity cannot be seen merely as a technological or internal problem. Cyber diplomacy is the application of diplomatic mechanisms to resolve cyberspace-related problems, such as cybercrime, cyber-attack response, international cooperation, internet governance, and the protection of critical infrastructure [1].

Accordingly, the necessity for cyber diplomacy stems from both the technical and strategic complexities of cyber threats. Asymmetric, dynamic, unpredictable, and unattributed hostile actions in cyberspace characterise many cyber threats. Additionally, cyberattacks can have significant economic, institutional, and political effects that go beyond the initial technical breach. Studies involving ransomware, cyber espionage, and data exfiltration show how quickly cyber events can escalate into strategic pressure, requiring a unified institutional response [8].

At the same time, cyber diplomacy is growing in an environment shaped by digitalisation, artificial intelligence (AI), automated detection systems, open-source intelligence (OSINT), and algorithmic decision-support systems. AI-based cybersecurity tools are already used for anomaly detection, malware classification, phishing detection, user behaviour analysis, and threat intelligence extraction [12]. Tools designed for OSINT can provide automated data collection capabilities, social media monitoring, natural language processing, and multimedia analysis [7]. These advancements indicate that, rather than automation itself being a defining feature of diplomacy, they represent a growing dependence of cyber-diplomacy on governments' capacity to collect, analyse, interpret, and responsibly govern digital information.

Therefore, this article explores the readiness of cyber diplomacy in the algorithmic age. By ”algorithmic age” it is referred to a cyber-governance landscape characterised by greater reliance upon digital data, automated detection mechanisms, platform architectures, and algorithmic decision-support systems. The article does not examine the degree to which selected countries employ artificial intelligence, OSINT or other automated systems in their diplomatic practices. Rather, the article seeks to determine whether these countries have the relevant structural foundations to engage in cyber-diplomacy in a data-intensive, algorithmically mediated environment.

Based on the assumption that structural readiness for cyber diplomacy in the algorithmic age consists of two complementary components – namely cybersecurity capacity (including legal; technical; organizational; and cooperative frameworks for prevention; detection; and response to cyber incidents) and digital governance

capacity (including digital public services; network-readiness; data infrastructure; institutional interoperability; and responsible use of digital technology in public administration) – previous studies assessing cybersecurity and digital development indicators have demonstrated that cybersecurity capability and digital development are highly correlated and should therefore be analyzed jointly [16].

Given its efforts to establish a common framework for cybersecurity policy across member states, the European Union serves as a useful reference point for assessing readiness. EU cyber diplomacy includes preventive, cooperative, stabilising, and restrictive approaches [2]. In addition, recent EU cybersecurity policy instruments (such as NIS2, the Cyber Resilience Act, and the Cyber Solidarity Act) further illustrate that cybersecurity is increasingly tied to concepts such as resilience, preparedness, and institutional coordination [14]. Moreover, the Cyber Solidarity Act demonstrates that the EU is seeking to build detection, preparedness, and response capacities at the supranational level [17].

While some countries have developed strong cybersecurity policies, uncertainty remains regarding whether their public-sector digitalisation, network readiness, data governance and institutional interoperability are sufficient to support participation in this emerging environment. Conversely, digital transformation without sufficient cybersecurity capacity will likely increase vulnerability to cyber risks. Therefore, this paper aims to evaluate this challenge by conducting an exploratory readiness assessment of the following indicators: GCI (global cybersecurity index), NCSI (national cybersecurity index), e-government development index (EGDI), and NRI (network readiness index).

The main research question is: how far do selected European Union member states have the cybersecurity capacity and digital governance conditions to support cyber diplomacy in the algorithmic age? Answering this question involves analysing twelve EU member-states located in Central, Eastern, Baltic, and South-Eastern Europe: Romania; Bulgaria; Hungary; Poland; the Czech Republic; Slovakia; Croatia; Slovenia; Estonia; Latvia; Lithuania; Greece.

The article addresses two areas, starting with clarifying the relationship between cyber diplomacy, cyber-security capacity, and digital governance readiness in light of an algorithmic transformation. Secondly, it introduces the CDRI (Cyber-Digital Readiness Index), that employs existing indicators measuring cybersecurity capacity and digital development as an exploratory proxy for structural readiness. While CDRI does not assess direct cyber diplomacy performance, it assesses whether selected countries possess the cyber and digital conditions that may support cyber diplomacy in an increasingly data-intensive and algorithmically-mediated environment.

The article is structured as follows. In Section 2, there is a discussion of Cyber Diplomacy in the algorithmic age. Section 3 defines and explains what Cyber Security Capacity (CSC) and Digital Governance (DG) are as Readiness Conditions. Section 4 covers how the data were collected and how the index was developed. The findings are compared in Section 5. Then, Section 6 outlines the major implications of the findings, and the last section (7) concludes the article and provides further direction for potential research.

2. Cyber Diplomacy in the Algorithmic Age

Cyber diplomacy involves using tools associated with traditional diplomatic practice and forms of institutional cooperation to address issues related to the use of cyberspace. Issues include cybercrime, cyberattacks, internet governance, the protection of critical infrastructure, the establishment of cyber norms, and international cooperation [1]. Unlike digital diplomacy, which primarily concerns how digital technologies can be used for communication in diplomacy, cyber diplomacy focuses on managing the potential risks and conflicts associated with the use of cyberspace [1].

As the number of cyber incidents worldwide increases, there is a growing need for cyber diplomacy. Cyber incidents can result in more than just technical disruptions. An attack on power grids, banks, government offices, transportation systems, hospitals, or communications services could disrupt the economy, erode citizens' trust in their government, and compromise national security. Because cyberattacks are dynamic, asymmetric, and often unattributed [15], they pose significant challenges for control. This makes cyber diplomacy reliant on both political negotiations and technical evidence, as well as capabilities to respond to incidents and coordinate among institutions.

However, these types of dependencies are even greater due to society's ”algorithmic” nature today. A growing number of cybersecurity organisations now operate in data-rich environments where detecting threats, assessing risk, and automation and/or algorithms can facilitate the analysis of information related to those threats. AI-based cybersecurity tools can help identify anomalies, classify malware, detect phishing attempts, analyse user behaviour, and extract threat intelligence [12]. Tools based on Open Source Intelligence (OSINT) can assist in collecting and interpreting publicly available digital information, such as online content, social media activity, and multimedia materials [7]. While these tools cannot replace cyber diplomacy efforts themselves, they are changing the information environment in which cyber diplomats make decisions regarding cyber diplomacy actions.

These changes also bring new governance risks into play. Automated systems often lack clarity about how decisions were made (opacity); they can reflect biases inherent in the data; they often lack explanation; and they can be very difficult to audit. In particular, the problem of algorithmic opacity is significant because automated systems often play a role in decisions that affect the public interest, national security, and institutional trust [10]. Therefore, for cybersecurity capacity to provide value-added contributions to cyber diplomacy efforts, accountability, transparency, and human oversight must accompany technological capability. Cyber-diplomatic actions cannot rely solely on the outputs of automated processes; rather, they must be informed by expert interpretation, reviewed by institutions, and governed responsibly.

The EU context illustrates this larger-scale transition. Cyber diplomacy in the EU has been implemented through four different categories of responses: preventive, cooperative/stabilising, and restrictive measures [2]. The EU's approach to governing cybersecurity has also expanded to encompass a variety of instruments that connect technical security to institutional preparedness, resilience, and regulatory coordination [14]. The Cyber Solidarity Act provides additional mechanisms at the EU level for identifying large-scale cyber events, preparing responses to such events and developing responses to major cyber events [17].

Therefore, understanding cyber diplomacy in an algorithmic age requires recognising that it represents a governance challenge that connects cybersecurity capacity development with digital infrastructure development, institutional collaboration and accountability for the use of algorithmic systems. The core issue is not whether diplomacy can be automated; instead, the key question is what

structural conditions exist within states that would enable effective cyber-diplomacy operations in an increasingly algorithms-based environment.

3. Cybersecurity Capacity and Digital Governance as Readiness Conditions

In addition to coordinating diplomatically, cyber diplomacy in the algorithmic age relies on technical and institutional capabilities to prevent, detect, evaluate, and respond to cyber incidents. Hence, cybersecurity capability represents the first condition for readiness. To develop effective management of cyber risks, countries need legal frameworks; institutions that provide technical assistance; mechanisms to respond to incidents; organisational structures; ways to build their capacities; and pathways for international collaboration.

Cybersecurity capability is especially important given that cyber threats are generally complex and often difficult to assign. Cyber-attacks may be carried out by a range of actors, from individual attackers to organised groups and even state-affiliated actors [15]. They may consist of multiple stages, such as reconnaissance, exploitation, installation, command-and-control, data exfiltration, and operational impacts [8]. Absent adequate cyber capacity, institutions will be unable to generate the technical evidence and situational awareness required to undertake credible cyber-diplomacy.

However, while cybersecurity capacity is essential to conducting cyber-diplomacy in the algorithmic age, it is insufficient. Cyber-diplomacy in the algorithmic age also needs digital governance capacity. Examples of digital governance include government sector digitalisation, digital infrastructure that provides security, networks ready for digital applications, data governance, interoperability, and the ability of institutions to incorporate digital technology into decision-making. The importance of digital governance stems from the fact that cyber-diplomacy increasingly relies on institutions' ability to collect, process, share, and interpret digital information across a variety of administrative and technical systems.

The relationship between cybersecurity and digital development has already been recognised in studies that employ composite indicators to analyse both. These studies show that cybersecurity capacity and digital development should be examined collectively, as both determine a country's overall cyber resilience and readiness for digital transformation [16]. This paper expands upon that logic by applying it to readiness for cyber-diplomacy in the algorithmic age.

Public sector digitalisation is particularly relevant. Government agencies can enhance efficiency, transparency, data exchange and relationships among institutions, citizens, and private enterprise when utilising electronic government systems [3]. Conversely, public institutions' inability to utilise digital tools effectively may stem from weaknesses in their digital public services, a lack of skilled personnel, fragmented data systems, or poor interoperability. Consequently, for cyber-diplomacy purposes, a country might have cybersecurity strategies and organisations but still experience problems with data-driven or algorithmically supported processes due to weaknesses in its digital governance environment.

A second reason why digital governance capacity is significant is that algorithmic systems create accountability challenges. Government agency algorithms and AI systems can support decision-making processes; however, they can also raise concerns related to transparency, explainability, bias, privacy, and public oversight [9]. As a result of algorithmic opacity, the ability of institutions and citizens to understand how algorithmic outputs were created or utilised could be severely diminished [10]. Accordingly, a country's preparedness for cyber-diplomacy in the algorithmic age would require not just cyber and digital capacity but also responsible governance of algorithmic tools.

Therefore, this study views cyber-diplomacy readiness as a combination of two readiness conditions. The cyber dimension encompasses a country's cybersecurity commitments, preparedness for potential incidents, and level of cooperation. The digital dimension pertains to the maturity of a country's e-government system(s), its network readiness, and other elements of its overall digital development. Individually and collectively, these dimensions represent the structural foundation for examining whether countries are adequately positioned to pursue cyber-diplomacy in environments characterised by increasing amounts of data, platform-based applications, and algorithmic systems.

Consequently, the subsequent empirical analysis does not intend to analyse the actual application of artificial intelligence, open source intelligence, or algorithmic tools by diplomats. Rather, it analyses enablers. A country with high levels of cyber capacity and strong digital governance readiness is much more likely to possess the necessary institutional/technical capabilities to pursue cyber diplomacy in the algorithmic age. A country with strong cyber capacity but less developed digitally may have established important cybersecurity institutions, yet still face limitations in integrating digital data, developing public-sector digital capabilities, and ensuring accountable algorithmic governance.

4. Methodology

This article employs a comparative structural readiness assessment to evaluate whether selected European Union countries possess the necessary cybersecurity capacity and digital governance conditions to support cyber diplomacy in the algorithmic age. The assessment does not assess the direct application of Artificial Intelligence, Open-Source Intelligence (OSINT), or Algorithmic systems in diplomatic practices. Rather, it evaluates structural readiness via cybersecurity and digital development indicators.

Twelve EU Member States from Central and Eastern Europe, the Baltic Region and South-Eastern Europe are analysed: Romania, Bulgaria, Hungary, Poland, the Czech Republic, the Slovak Republic, Croatia, Slovenia, Estonia, Latvia, Lithuania and Greece. The countries were chosen for comparative sampling. Even if they all adhere to the same broad EU cyber and digital governance framework, each has varying degrees of cybersecurity maturity and digital development. This facilitates comparisons across a relatively consistent institutional and regional context.

There were selected four indicators: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Electronic Government Development Index (EGDI), and Network Readiness Index (NRI). The GCI and NCSI are used to approximate national cybersecurity capacity and preparedness. EGDI and NRI are representative of a nation's digital governance capabilities and level of digital development. These indicators collectively enable the assessment of readiness for cyber diplomacy in a data-driven, algorithmically mediated environment. Data for the empirical study include GCI 2024, EGDI 2024, and NRI 2024. NCSI represents the most current country-specific data available at the time of data collection.

Before aggregating the data into a single metric, it was normalised to a 0–100 scale. All GCI, NCSI and NRI indicator values were utilised as 0 – 100 metrics. EGDI is presented on a 0 – 1 scale, so it was adjusted by multiplying it by 100. The article develops a proposed Cyber-Digital Readiness Index (CDRI) based upon the previously described method:

$$\text{CDRI} = 0.30 \times \text{GCI} + 0.30 \times \text{NCSI} + 0.20 \times \text{EGDI} + 0.20 \times \text{NRI} \quad (1)$$

In this formula, higher weightings are assigned to cybersecurity indicators because cyber diplomacy depends on preventing cyber threats, responding to incidents, and cooperating with other nations.

Some aspect of digital governance must be represented to ensure a mature digital public sector capable of responding effectively to algorithmic challenges, with adequate data infrastructure, institutional interoperability, and network readiness. The employed weighting scheme is exploratory and theoretically derived. As such, results from future studies can utilise alternative weighting schemes to validate findings herein.

Additionally, two additional sub-metrics are developed to facilitate the interpretation of CDRI results. The Cyber Capacity Index is defined as the average of the GCI and the NCSI. A Digital Development Index is defined as the average of EGDI and NRI.

$$\text{Cyber Capacity Index} = \frac{\text{GCI} + \text{NCSI}}{2} \quad (2)$$

$$\text{Digital Development Index} = \frac{\text{EGDI} + \text{NRI}}{2} \quad (3)$$

The cyber-digital gap is calculated as the difference between the Cyber Capacity Index and the Digital Development Index. The gap size indicates the degree of imbalance between cybersecurity capacity and digital development capacity.

Finally, the index has several limitations. It does not assess whether a nation currently utilises algorithmically supported cyber diplomacy. Additionally, it does not measure how a country adopts AI technology, whether it has an established OSINT capability, whether it has a sufficient number of diplomats with the requisite skills, or what type of organisational culture exists within those organisations. The index is best viewed as an exploratory proxy for measuring structural readiness rather than as a definitive measure of a nation's overall performance.

5. Results

The relative results demonstrate structural differences in preparedness to engage with digital and cyberspace across all selected countries. Table 1 presents the scores for each country across the four variables, as well as their aggregate value, the Cyber-Digital Readiness Index (CDRI).

For example, Estonia achieved the best overall result, based on its very high level of cybersecurity capacity and digital development, i.e., with an index value of 90.54. In fact, Lithuania, Poland, Slovenia and Czechia all have levels of cyber-digital readiness exceeding 85 points. Romania ranked 9th and scored 81.06; it has relatively strong cybersecurity indexes, specifically GCI and NCSI, whereas its other two indexes (EGDI and NRI) were below those of many nations ranking ahead of it. Therefore, Romania's main structural limitation in this assessment is not cybersecurity capacity, but broader digital governance and network readiness.

Source: Author's calculation based on GCI 2024, NCSI latest available scores, EGDI 2024 and NRI 2024.

Table 1. CDRI scores and ranking of selected countries

Rank	Country	GCI	NCSI	EGDI	NRI	CDRI
1	Estonia	95.04	96.67	97.27	67.85	90.54
2	Lithuania	92.73	95.00	91.10	59.95	86.53
3	Poland	93.54	92.50	86.48	59.94	85.10
4	Slovenia	96.47	89.17	87.59	59.38	85.09
5	Czechia	87.93	98.33	82.39	63.47	85.05
6	Slovakia	94.45	92.50	80.21	54.88	83.10
7	Greece	97.19	85.00	86.74	52.90	82.58
8	Hungary	88.65	93.33	80.43	55.33	81.75
9	Romania	91.62	92.50	76.36	52.77	81.06
10	Latvia	82.63	85.83	88.52	57.68	79.78
11	Croatia	88.28	82.50	88.18	51.96	79.26
12	Bulgaria	74.56	80.83	81.45	53.15	73.54

Source: Author's calculation based on GCI 2024, NCSI latest available scores, EGDI 2024 and NRI 2024.

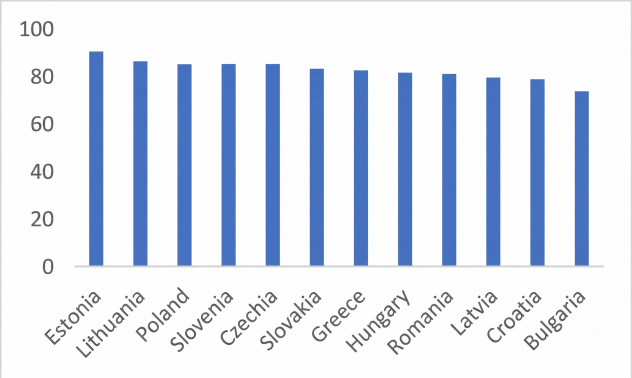

Figure 1. Cyber-Digital Readiness Index by country

Table 2 illustrates the previously described relationships in greater detail by presenting the Cyber Capacity Index, the Digital Development Index, and the cyber-digital gap.

Table 2. Cyber Capacity Index, Digital Development Index and cyber-digital gap

Country	Cyber Capacity Index	Digital Development Index	Cyber-Digital Gap
Estonia	95.86	82.56	13.30
Lithuania	93.87	75.53	18.34
Poland	93.02	73.21	19.81
Slovenia	92.82	73.49	19.34
Czechia	93.13	72.93	20.20
Slovakia	93.48	67.55	25.93
Greece	91.10	69.82	21.28
Hungary	90.99	67.88	23.11
Romania	92.06	64.57	27.50
Latvia	84.23	73.10	11.13
Croatia	85.39	70.07	15.32
Bulgaria	77.70	67.30	10.40

Source: Author's calculation based on Table 1.

Most of the sampled countries outperform their peers in cybersecurity, reflecting the level of sophistication (in terms of institutionalisation) of their commitment to cybersecurity and their ability to respond to incidents, compared with the digital governance requirements necessary for effective cyber-diplomacy in an algorithmic age.

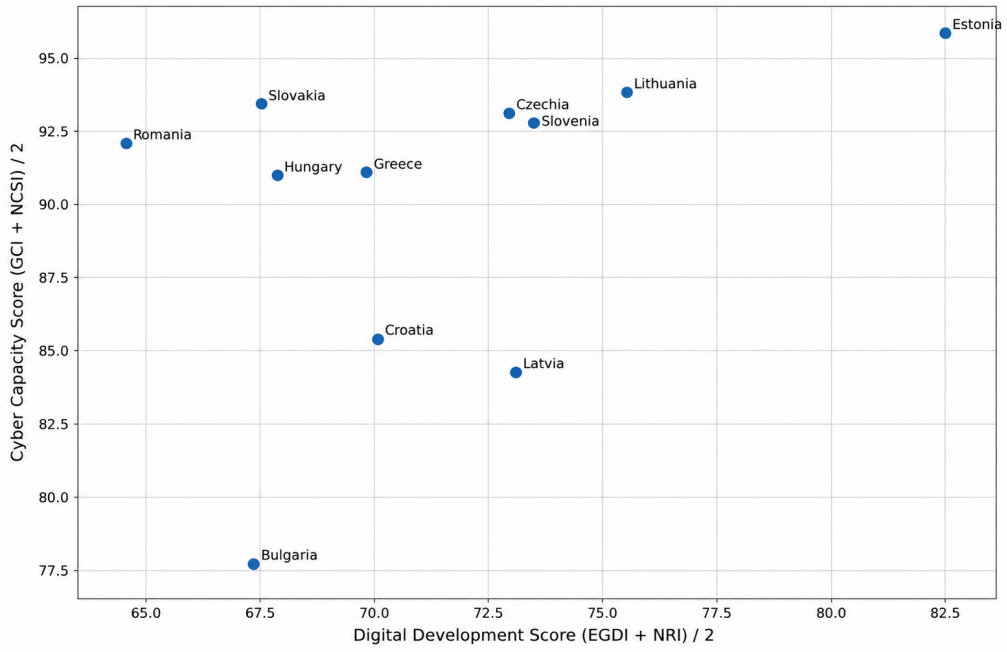

Figure 2. Cyber Capacity Index and Digital Development Index

Source: Author's calculation based on Table 1

Romania has the largest cyber-digital gap among the sampled nations, with a difference of 27.5 points. While its Cyber Capacity Index is 92.06, its Digital Development Index is 64.57 (the lowest value among the countries examined). Thus, while Romania has a solid foundational structure for cybersecurity, it is hindered by less mature digital public-sector structures, networking, and digital development.

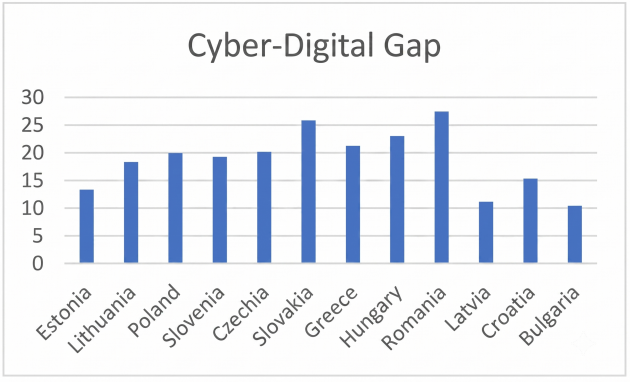

Figure 3. Cyber-Digital Gap by country

Source: Author's calculation based on Table 2.

Four general readiness profiles can be derived from the index results. Estonia exemplifies a balanced high-readiness type. Lithuania, Poland, Slovenia, the Czech Republic, Slovakia, Greece, Hungary and Romania are examples of countries with very high levels of cyber-readiness; however, these countries also demonstrate significantly lower levels of balance between cyber-readiness and digital-readiness. Latvia and Croatia are countries with relatively low overall readiness but a greater balance. Bulgaria recorded the lowest CDRI score of all the selected countries.

In conclusion, while cybersecurity readiness is important, having only this does not guarantee cyber readiness to engage in diplomatic activities regarding cyberspace issues in an "algorithmic world". There needs to be evidence of both cybersecurity maturity and digital governance capacity. For example, countries need to establish and maintain cyber institutions, incident response mechanisms, and cooperative frameworks for international coordination. However, countries also need established digital public services, network readiness, data governance capability, interoperability, and accountability through transparent digital systems.

6. Discussion

The findings confirm the article's argument: In order to be structurally ready for cyber diplomacy in an algorithmic era, a nation depends on both cybersecurity and digital governance capabilities. The CDRI rating shows that a country's cybersecurity indicators by no means correspond predictably to its digital development indicators. Cyber diplomacy increasingly requires technical evidence, digital infrastructure, data exchange, institutional interoperability, and accountable use of algorithmic systems.

Estonia is clearly the best example in this sample due to its relatively high levels of cybersecurity capability and digital development. A balanced structure would enable better structural conditions for cyber diplomacy in a data-driven world.

Romania has high levels of cybersecurity indicators and low levels of digital development indicators. Romania's significant cyber–digital gap indicates that cyber capacity alone is insufficient to ensure full readiness for the algorithmic age.

These findings relate particularly well to those nations that are strong in cybersecurity yet less developed in terms of balance. Cybersecurity strategies, incident response mechanisms, and cooperation frameworks represent the basis upon which cyber-capable states can build their readiness. However, this is insufficient.

Institutional maturity in digital public services, interoperable data systems, network readiness, and responsible management of digital information will be required to ensure that algorithmic or data-driven tools are not isolated from one another and/or difficult to utilise within governance processes.

The Romanian case is particularly relevant here. Although Romania's Cyber Capacity Index ranked as high as many countries above it, Romania's Digital Development Index was the lowest in this sample. As such, any future progress by Romania will likely need to focus on strengthening its digital public administration, data governance, interoperability, network readiness, and human capital. This interpretation is supported by research indicating that Romania has some critical digitalisation goals; however, it continues to struggle with challenges in its digital public services and digital literacy [3].

There are also implications for EU cyber governance. EU cyber diplomacy encompasses a variety of measures - preventative measures, cooperative measures, stabilising measures, and restrictive measures [2] and recent EU instruments indicate a transition towards increased emphasis on resilience, preparedness, and coordinated responses [14]. Nations whose cyber-digital readiness is not even may experience difficulties in making full use of EU-level instruments aimed at increasing cyber-resilience, information-sharing, and coordinating responses.

The second implication relates to accountability. Cyber diplomacy in the algorithmic era cannot solely rely on technical capacity. For example, while an algorithmic system may be technically capable of producing outputs or predictions about a particular phenomenon, it may be opaque regarding how it arrived at those conclusions. Furthermore, demonstrating how an algorithm works through documentation, explaining why it produced a certain outcome (auditability), and providing users with explanations of how it produces its outputs (explainability) are all highly desirable features for promoting transparent and responsible digital governance [5]. These requirements are particularly relevant because cyber-diplomatic actions must remain credible, understandable to others, and subject to human review.

Therefore, based on the findings presented herein, readiness for cyber diplomacy in the algorithmic age must be viewed as a two-part condition. First, there exists a condition of cybersecurity maturity. The latter may comprise strategic planning, institutions, technical capacity, and incident response mechanisms. Second, there exists a condition of digital governance maturity. The latter may comprise government service development via e-government programs and networks, development of data-based infrastructures, and institutionally acceptable interoperability. If either dimension is developed in isolation from the other, that country may be ill-prepared for cyber diplomacy in the algorithmic age.

Use of the CDRI should be cautious. The CDRI does not measure the performance of actual cyber diplomatic activities. The CDRI does not measure AI usage, OSINT usage or the use of algorithms within governmental institutions. Rather, the CDRI uses existing available cybersecurity and digital development indicators to estimate structural readiness for cyber diplomacy in the current time period.

Even though the CDRI has limitations as a tool for measuring structural readiness for cyber diplomacy in the algorithmic age, despite the fact that the CDRI is limited by what is actually measurable, the CDRI remains useful because it illustrates that cyber and digital capacities must be assessed jointly when evaluating structural readiness for modern-day cyber diplomacy.

Overall analysis demonstrates that the algorithmic age does not eliminate the need for traditional forms of diplomacy. Rather than eliminating the need for diplomacy, the algorithmic age merely alters the parameters under which cyber diplomacy occurs. States require technical cyber-capacity. Moreover, states require digital governance capacity and responsible use of data, along with human oversight over algorithmic systems.

7. Conclusion

This study investigated structural readiness for cyber diplomacy in the algorithmic age by evaluating cybersecurity capabilities and conditions for digital governance in select European Union (EU) countries. The authors did not assess the actual employment of Artificial Intelligence, Open-Source Information Collection (OSINT) or Algorithmic Systems in diplomacy practice; instead, they developed a framework for exploring readiness assessments using four measures: The Global Cybersecurity Index, The National Cyber Security Index, The E-Government Development Index, and The Network Readiness Index.

Estonia had the highest readiness among the sampled countries due to its combination of high cybersecurity capacity and advanced digital development. On the other hand, Romania recorded some of the highest levels of cybersecurity capacity; however, Romania was significantly lower than Estonia in terms of digital development, thus creating one of the greatest gaps in cyber/digital readiness among the countries studied.

The primary contribution of this paper is the Cyber-Digital Readiness Index (CDRI). The CDRI offers a possible approach to evaluate structural readiness among countries. Importantly, the index emphasises the need to evaluate cyber capacity and digital governance simultaneously. This is particularly important today as cyber-diplomacy becomes ever more dependent on evidence generated by technology, data exchanged, digital infrastructure, inter-institutional collaboration, and responsible and accountable use of algorithmic systems.

Furthermore, this study demonstrated that the "algorithmic" age will not eliminate diplomacy. Rather, it will transform the environment in which cyber-diplomacy occurs. Therefore, like traditional forms of diplomacy, cyber-diplomacy requires both human judgment and institutional responsibility. Moreover, while these requirements continue to exist in cyberspace, they will become increasingly dependent on digital capabilities and the accountable operation of information systems. As such, cyber-readiness for diplomacy can no longer be evaluated solely on cyber or digital capabilities. Rather, it needs to be assessed in relation to the degree to which cyber-capability and digital capability coexist.

As such, there are several limitations associated with the CDRI. The most significant limit is that it does not measure actual diplomatic performance in cyberspace, nor does it measure AI adoption, OSINT capacity or diplomatic expertise. While the CDRI serves as a proxy for assessing structural readiness, it cannot provide a complete or definitive evaluation of each country's relative cyber-diplomatic capability. Future research may seek to enhance the CDRI by incorporating additional variables, such as those representing AI readiness, digital literacy, public-sector data governance, cyber workforce capacity, and/or algorithmic transparency. Furthermore, studies that apply the model to all EU Member States or compare EU and non-EU countries would also help enhance our understanding of how best to prepare for cyber-diplomacy.

In summary, the results of this study demonstrate that countries seeking to prepare themselves for cyber diplomacy in the algorithmic age must focus their efforts beyond merely developing strong cybersecurity institutions. In addition to establishing robust cybersecurity institutions, nations must also establish a mature digital governance structure (i.e., data infrastructure, interoperability); develop human capital (i.e., knowledge/skills); and create accountability mechanisms. Ultimately, effective cyber diplomacy will increasingly depend on a nation's ability to foster strong cybersecurity maturity and responsible digital governance.

REFERENCES

[1] Cîrnu, C. E. (2019). Cyber Diplomacy, a Strategic Instrument in Foreign Affairs Policy. *Romanian Cyber Security Journal*.

[2] Cîrnu, C. E., Rotună, C. I., & Vasiloiu, I. C. (2023). Comparative Analysis on Cyber Diplomacy in the EU and the US. *Romanian Cyber Security Journal*.

[3] Dumitrache, M., Stănescu, C., & Paraschiv, E. (2023). Digitalisation and artificial intelligence in e-Government applications. *Romanian Journal of Information Technology and Automatic Control*.

[4] e-Governance Academy. (2026). *National Cyber Security Index: Ranking*. e-Governance Academy.

[5] Global Partnership on Artificial Intelligence. (2024). *Algorithmic Transparency in the Public Sector*. OECD/GPAI.

[6] International Telecommunication Union. (2024). *Global Cybersecurity Index 2024*. ITU.

[7] Kovaci, M., & Iacob, R. (2024). Artificial Intelligence and OSINT. Considerations and Challenges. *Romanian Cyber Security Journal*.

[8] Leu, A., et al. (2023). Analysis of some case studies on cyberattacks and proposed methods for preventing them. *Romanian Journal of Information Technology and Automatic Control*.

[9] Levy, K., Chasalow, K., & Riley, S. (2021). Algorithms and Decision-Making in the Public Sector. *Annual Review of Law and Social Science*.

[10] Lu, S. (2021). Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence. *Vanderbilt Journal of Entertainment & Technology Law, 23*(1), 99–159.

[11] Network Readiness Index. (2024). *Network Readiness Index 2024*. Portulans Institute.

[12] Ovreiu, S., Savu, D., Mitan, E., & Neacșu, D. (2026). Intelligence Defense - the Role of Artificial Intelligence in Combating Cyber Threats. *Romanian Cyber Security Journal, 8*(1).

[13] United Nations Department of Economic and Social Affairs. (2024). *UN E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development*. United Nations.

[14] Vasiloiu, I. C., & Vevera, A. V. (2026). Cyberdiplomacy in EU: The context of the technical security framework and the perspective of a normative projection.

[15] Vevera, A. V. (2018). From cyber threat to hostile action in cyberspace. *Romanian Journal of Information Technology and Automatic Control*.

[16] Vevera, A. V., Cîrnu, C. E., & Rădulescu, M. (2022). A multi-criteria approach for the calculation of a complex indicator of Cyber Security and Digital Development. *Romanian Journal of Information Technology and Automatic Control*.

[17] Villani, S. (2025). Cyber Solidarity Act: Framework and perspectives for the new EU-wide cybersecurity solidarity mechanism under the EU legal system. *European Journal of Risk Regulation*.