SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2025), pp. 418-431

PROTECTING THE DIGITAL REALM: A CASE STUDY OF ROMANIA'S CYBER SOVEREIGNTY *

P. TAL

Received 10.12.2024; accepted 20.02.2025
First online publication: 07.03.2025
DOI: https://doi.org/10.55516/ijlso.v5i1.252

"States occasionally do conduct cyber activities that transit through, and target, networks and computers located in other States" (*Schöndorf, 2020*)

Pavel TAL[1],
"Dunarea de Jos" University of Galati, Romania
E-mail: Tal@Cybureau.org
ORCID ID: *https://orcid.org/0000-0002-4046-0867*

Abstract

Cyber sovereignty, a nation's right to govern its cyberspace, has emerged as a critical issue in the 21st century. Indeed, cyber threats increasingly challenge national security worldwide, so cyber sovereignty has become a critical priority for nations seeking to safeguard civilian and military digital domains.

Romania, a significant player in European cyber defence, has developed robust policies to safeguard its digital infrastructure and maintain sovereignty in cyberspace. This paper presents a case study of Romania's approach to cyber sovereignty, examining the strategic and legal frameworks that underpin its efforts to secure digital boundaries across civilian and military spheres. Through a detailed examination of Romania's military and national strategy and cyber-related legislative framework published in the last two decades, the research aims to illustrate how Romania addresses the demands of an evolving cybersecurity landscape and defines its cyber boundaries and sovereignty.

The findings reveal a lack of well-defined cyber sovereignty in Romania. None of the 22 official strategies and policy, civilian and military, publications published between the years 2002-2021 explicitly defines the term "Cyber Sovereignty" or illustrates Romania's cyber borders; (1) Some refer to the borderless nature of cyberspace (2) others refer to Romanian cyberspace, (3) and few indicate the need to ensure cyber security and defence abroad the country and at the international level.

PROTECTING THE DIGITAL REALM: A CASE STUDY OF ROMANIA'S CYBER SOVEREIGNTY*

This paper contributes to a deeper understanding of cyber sovereignty and its implementation within Romania's national strategy and legal context. It emphasises the importance of a well-defined cyber sovereignty in Romania and worldwide.

Key words: *effective remedy, criminal case, legal order, legal security, access to justice.*

INTRODUCTION

The various literature defines the term"Cyber Sovereignty" and addresses its complex and indeterminate nature, while most researchers align cyber sovereignty with fixed physical boundaries:

Nadeem Mirza et al. define that "states have authority within a fixed boundary to devise rules, laws, and norms about behaviour of individuals, institutions, applications, and other actors and factors in the cyberspace" (*Nadeem Mirza et al., 2021*). Pandey designates "Cyber Sovereignty" as "the control of cyberspace and the dissemination of information within a country's sovereign territory" (*Pandey, 2024*).

Fiveable definitions limit cyber sovereignty to local cyberspace, arguing that "Cyber sovereignty refers to the concept that nations have the right to govern their own cyberspace without external interference, reflecting their unique political, cultural, and legal frameworks" while emphasising the applying cyber sovereignty out of state's borders, "This idea emphasizes that states can create and enforce laws and regulations that apply to digital spaces within their borders, influencing how data is controlled and shared across international boundaries" (*Fiveable, n.d.).*

Others fail to align cyber sovereignty with fixed physical boundaries but assert that the concept refers to the nations' cyberspace:

Jensen describes "Cyber Sovereignty" as "The extent to which nations exercise sovereignty over cyberspace and cyber infrastructure" (*Jensen, 2014*). Similarly, Leiter characterises it as "the ability to create and implement rules in cyberspace through state governance" *(Leiter, 2020*). The Tallinn Manual addresses the internal ("A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations") and external ("A State is free to conduct cyber activities in its international relations subject to any contrary rule of international law binding on it") components of "Cyber Sovereignty" (*M. N. Schmitt, 2017*).

Others refer to the complexity of sovereignty in cyberspace and, therefore, to the ability to define the term "Cyber Sovereignty" properly:

Baezner and Robin address the nature and complexity of cyber sovereignty and its definition: "While cyber sovereignty is a vague concept in general that is often used in relation to state power and independence in cyberspace, sovereignty

itself is a clearly defined concept in International Law. Therefore, the concept of cyber sovereignty needs to be defined more precisely" (*Baezner & Robin, 2018*).

Prof Michael Schmitt describes two attitudes towards "whether sovereignty is simply a principle of international law from which binding international law rules emerge, or a primary rule of international law, the violation of which by cyber means constitutes an 'internationally wrongful act'" mentioning two positions and the fact that the United States and Israel remain on the fence "either by failing to express a view or by discussing the matter without taking a firm position thereon"(*M. Schmitt, 2020*). The same as Dr Schöndorf's claim that "the State of Israel has largely refrained thus far from making specific statements on whether and how particular rules apply" (*Schöndorf, 2020*).

Support for this hypothesis on strategic cyber sovereignty ambiguity may be found in international strategic ambiguity relating to cyber norms and specifically to cyber sovereignty (*Barker, 2020; Brake, 2015; Broeders & Cristiano, 2020; Palladino & Amoretti, n.d.; Ruohonen, 2021*).

The research literature analyses cyber sovereignty of various states, including The U.S. (*Kelton et al., 2022*), China (*Creemers, 2020*), Ukraine (*Dimich & Yeromina, 2022*), Russia (*Gaiser, 2021*), Israel (*Pavel, 2024*), Thailand (*Chachavalpongpun, 2023*), Indonesia (*Ro'is, 2022*), Morocco (*Maleh & Maleh, 2022*), Turkey (*Eldem, 2021*), Bhutan (*Tshering Tshering, 2021*), and The EU (*Barrinha & Christou, 2022*).

In addition, the research literature analyses various aspects of Romania's cyberspace, including the cyber security policy (Petcu & Barbu, 2022), The CYRESRANGE project (*Dinu & Cîrnu, 2024*), education (*Vasiloiu, 2022*), approaches and efforts (*Brânda, 2021*), including its passive cyber defence (*Ceuca, 2023*), law (*Dragomir & Florescu, 2022*), cybercrime (*Zlati, 2021*), disinformation (*Bârgăoanu & Pană, 2024*), feminism (*Voina et al., 2021*), and regional cyber aspects (*Nagy, 2021*).

Nevertheless, the research literature lacks an analysis of Romania's national cyber sovereignty. To minimise this research gap, the study analyses the following research questions: (RQ1) What is Romania's official definition of its sovereignty in cyberspace? (RQ2) What are the official boundaries of Romania's cyberspace? (RQ3) Do the definitions differ between official Romanian agencies?

I. METHODOLOGY

The analysis is qualitative research based on the following steps:

Phase A – the sources –

1. Map all of Romania's official cyber policies and strategies published by the Government of Romania at the Legislative Portal (*Government of Romania, n.d.*).

2. Map all of Romania's official cyber policies and strategies as published by the United Nations Institute for Disarmament Research in the Cyber Policy Portal (*United Nations Institute for Disarmament Research, n.d.*).
3. A general search for Romania's cyber-related strategy policy using a search engine.
4. Collect all the publications to Table 1 – "Romania's Cyber Sovereignty and Boundaries in its Civilian and Military National Strategy and Legal Frameworks".

Phase B – the content –

5. Search for the terms "Sovereignty" and "Boundary" or "Border" in the context of cyberspace in every publication that appears in Table 1 – "Romania's Cyber Sovereignty and Boundaries in its Civilian and Military National Strategy and Legal Frameworks".
6. Perform a broader indication of cyber sovereignty or boundaries definitions if a document does not explicitly include such a term.

II. FINDINGS

The total number of published Romanian national documents regarding cybersecurity policy, structure, and legal framework is 22, covering two decades of civilian and military national policy. The findings are gathered in Table 1 – "Romania's Cyber Sovereignty and Boundaries in its Civilian and Military National Strategy and Legal Frameworks."

Subject	Name	Publisher	"Sovereignty"	"Boundary" / "Border"	General Reference
Cybersecurity Policy	Military Strategy of Romania	(*Ministry of National Defence of Romania, 2005a*)	-	-	-
	The Military Strategy of Romania	(*Ministry of National Defense, 2016*)	-	-	"The Communications, Information and Cyber Defense Forces provide, through their standing and deployable capabilities, combat support for the management, operating, and maintenance of the infrastructure, communications systems and services of, information technology, information security, and cyber defense, in the country and

					abroad".
	Military Strategy of Romania	(*Ministry of National Defence, 2021*)	-	-	-
	Romania's National Security Strategy	(*Ministry of National Defence of Romania, 2005b*)	-	-	-
	The National Security Strategy of Romania	(*The President, 2007*)	-	-	-
	National Defence Strategy Romania 2015-2019	(*Presidential Administration, 2015*)	-	-	-
	National Defence Strategy 2020-2024	(*Presidential Administration, 2020*)	-	-	-
	Romania's Cybersecurity Strategy and Action Plan for 2022-2027	(*Government of Romania, 2021*)	-	-	"Cyber attacks target networks and computer systems on the territory of Romania, including those with an impact on national security". "Cyberspace is not limited by borders, so cyber security must be thought of and ensured at an international level".
	White Paper on Defense - 2015	(*Ministry of National Defence, 2015*)	-	-	-
	White Paper on Defense - 2021	(*WHITE PAPER of 11 May 2021, 2021*)	-	-	-
	National Strategy on Digital Agenda for Romania	(*Ministry of Communication and Information Technology, 2014*)	-	"This document acknowledges that there may exist some gaps in legislation pertaining to the use, operation or maintenance of information systems. It is of utmost importance to create the correct climate for change in ITC and these needs to start from the	-

				legislative framework which should clearly define the boundaries and the cascading effects of this charter to all the underlying functions".	
	Cyber Security Strategy of Romania	(*Government of Romania, 2013*)	-	"Cyberspace is characterised by the absence of borders, dynamism and anonymity, generating equal both opportunities to develop knowledge-based information society and risks to its functionality (at the individual, state and even transborder)".	-
Structures	Law no. 415 of June 27, 2002 regarding the organisation and functioning of the Supreme National Defense Council	(*Law No. 415 of June 27, 2002 Regarding the Organization and Functioning of the Supreme National Defense Council, 2002*)	-	-	-
	The functioning regulation of the Supreme Council of Defense of the Country	(*The Functioning Regulation of the Supreme Council of Defense of the Country, 2002*)	-	-	-
	LAW no. 346 of July 21, 2006 (*republished*)	(*LAW No. 346 of July 21, 2006 (*republished*), 2006*)	-	-	-
	DECISION no. 494 of May 11, 2011 regarding the establishment of the National Cyber Security Incident Response Center - CERT-RO	(*DECISION No. 494 of May 11, 2011 Regarding the Establishment of the National Cyber Security Incident Response Center - CERT-RO, 2011*)	-	-	-
	DECISION no. 584	(*DECISION No. 584*	-	-	-

	of August 8, 2019	*of August 8, 2019, 2019*)			
	RFC 2350 description for CERT-RO	(*DECISION No. 584 of August 8, 2019, 2019*)	-	-	"The CERT-RO constituency is composed of all users, systems and networks from Romanian cyber-space". "CERT-RO is authorised to address all types of computer security incidents which occur, or threaten to occur, in Romanian cyber-space".
	DECISION no. 1,005 from November 23, 2020	(*DECISION No. 1,005 from November 23, 2020, 2020*)	-	-	-
	EMERGENCY ORDINANCE 104/2021 on establishing the National Cyber Security Directorate	(*The National Cyber Security Directorate, 2021*)	-	"cyber threats do not have a clear national address of a sender, are not blocked at state borders".	-
Legal Framework	LAW no. 362 of December 28, 2018, on ensuring a common high level of security of networks and IT systems	(*The Functioning Regulation of the Supreme Council of Defense of the Country, 2002*)	-	"Determines, based on the notifications received, the national and cross-border impact of the incidents and informs the relevant authorities at the national level, as well as similar authorities in other potentially affected state".	-
	Decision No. 271	(*DECISION No. 271 of May 15, 2013, 2013*)	-	"The cyberspace is characterised by the lack of borders, dynamism and anonymity, generating both opportunities for the development of the	

				knowledge-based information society, but also risks to its operation (at the individual, state and even cross-border level)".	

Table 1 – "Romania's Cyber Sovereignty and Boundaries in its Civilian and Military National Strategy and Legal Frameworks"

The findings indicate that none of the 22 covered official strategies and policies, and civilian and military publications published between 2002 and 2021 directly refer to Romania's cyber borders, boundaries, or sovereignty.

Some national policy publications refer to the nature of cyberspace as "not limited by borders" (*Government of Romania, 2021*) and that it "is characterized by the absence of borders" (*Government of Romania, 2013*). Therefore, "cyber threats do not have a clear national address of a sender, are not blocked at state borders" (*The National Cyber Security Directorate, 2021*), and the cyber defence of Romania's Army is "in the country and abroad" (*Ministry of National Defense, 2016*).

Some publications refer to Romanian cyberspace, but there are no definitions of the boundaries of cyberspace: "The CERT-RO constituency is composed of all users, systems and networks from Romanian cyber-space". "CERT-RO is authorized to address all types of computer security incidents which occur, or threaten to occur, in Romanian cyber-space" (*DECISION No. 584 of August 8, 2019*).

III. DISCUSSION

The study aims to outline Romania's cyber sovereignty and boundaries based on its national strategy and legal frameworks. The findings indicate a lack of comprehensive definition and discussion of these issues.

The lack of an official definition of cyber sovereignty in Romania's national publications addresses Baezner & Robin's findings, which analysed 93 national cyber strategies of 69 states. The analysis revealed that 18 out of 93 documents contained the term "Sovereignty," and only one (Canada) contained the term "Cyber sovereignty."

In addition, the researchers assert that "The contexts in which the word "sovereignty" was used in strategies were various, but the word was never clearly defined in any of the documents". Therefore, the researchers emphasise "a lack of shared understanding and definition of the word "sovereignty" in the context of cybersecurity", a misunderstanding that needs to be rectified (*Baezner & Robin, 2018*).

Therefore, the paper can address the research questions and argue that (RQ1) Romania did not define its cyber sovereignty and boundaries in the civilian and military national strategy and legal frameworks. (RQ2) Even though the various Romanian national strategies and legal frameworks avoid defining Romania's cyber sovereignty and boundaries, some refer to the borderless nature of cyberspace and the fact that cyber threats are not blocked at state borders and therefore, the need to ensure cyber security and defence at abroad the country and at the international level. In addition, several national official strategies and policy publications refer to the "Romanian cyberspace". (RQ3) No distinction was found between military and national strategies defining Romania's cyber sovereignty.

Even though the few indications of Romanian cyber sovereignty refer to cyberspace's borderless nature, Romania's Army's cyber defence is defined explicitly as "in the country and abroad".

CONCLUSION

The conclusion emphasises the various research outcomes for reducing confusion surrounding "Cyber Sovereignty".

Several reasons may lie behind the lack of a coherent definition of Romania's cyber sovereignty: (1) Misunderstanding and insufficient awareness of the need to define the civilian and military cyber boundaries as part of national strategy. (2) There is a lack of international consensus on how sovereignty applies in cyberspace, which is in its early stages and remains a particular case compared to the other domains, and debates over sovereignty are still ongoing (Baezner & Robin, 2018). (3) The inherently borderless nature of cyberspace makes traditional territorial concepts challenging to apply. Unlike physical domains, cyberspace is a complex, interconnected, constantly evolving environment that defies traditional notions of territorial boundaries. This makes applying traditional concepts of sovereignty, rooted in the physical territory, to cyberspace challenging. (4) Governments often prefer to maintain strategic ambiguity in their cyber strategies to allow operational flexibility. Therefore, nations have been reluctant to agree on norms that might restrict their freedom in cyberspace, which limits the development of cohesive definitions in national strategies. Therefore, we may consciously try to avoid a public discussion on cyber sovereignty and boundaries, as in the case of Israel (Pavel, 2024). (5) Cyberspace evolves faster than traditional legal or regulatory frameworks. New technologies continually alter the cyber landscape, complicating efforts to establish stable definitions of boundaries and sovereignty that can adapt to such rapid advancements. (6) The constantly evolving threat landscape, including state-sponsored cyberattacks, cybercrime, and cyberterrorism, further complicates the issue of cyber sovereignty. In addition, attributing cyber activities to specific actors or nations remains technically challenging. Therefore, countries

must adapt their strategies to address these evolving threats, which may require rethinking traditional approaches to sovereignty.

Future research may analyse two approaches: (1) National cyber sovereignty in the EU member states and especially the Balkans, to explore whether Romania's approach toward cyber sovereignty definitions is unique or familiar among other region's states. (2) Romania's approach to other cyber-related definitions, to identify whether the lack of Romania's cyber sovereignty appears in national publications relating to various cyber-related terms, such as cyber terrorism, cyber warfare, cyber deterrence, and cyber resilience.

BIBLIOGRAFIE

1. Baezner, M. ;, & Robin, P. (2018). *ETH Library Cyber Sovereignty and Data Sovereignty*. https://doi.org/10.3929/ethz-b-000314613

2. Bârgăoanu, A., & Pană, M. (2024). Cyber influence defense: Applying the DISARM framework to a cognitive hacking case from the Romanian digital space. *Applied Cybersecurity & Internet Governance*. https://doi.org/10.60097/ACIG/190196

3. Barker, T. (2020, January 16). *Europe Can't Win Its War for Technology Sovereignty*. Foreign Policy. https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/

4. Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security*, *31*(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895

5. Brake, B. (2015). Strategic Risks of Ambiguity in Cyberspace. In *Contingency Planning Memorandum* (Issue 24). https://www.cfr.org/report/strategic-risks-ambiguity-cyberspace

6. Brânda, O.-E. (2021). Romanian Cybersecurity Efforts. In *Routledge Companion to Global Cyber-Security Strategy*. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-11/romanian-cybersecurity-efforts-oana-elena-br%C3%A2nda

7. Broeders, D., & Cristiano, F. (2020, March 18). *Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road*. Italian Institute for International Political Studies. https://www.ispionline.it/en/publication/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417

8. CEUCA, R.-O. (2023). Passive Cyber Defense as a Norm Preservation Tool: Romania's Behaviour as a Norm Antipreneur in Cybersecurity. *Romanian Cyber Security Journal*, *5*(2), 1–16. https://doi.org/https://doi.org/10.54851/v5i2y202302

9. Chachavalpongpun, P. (2023). Nationhood in the Cloud: Cyber Sovereignty in Thailand. *Asian Studies Review*, *47*(2), 392–411. https://doi.org/10.1080/10357823.2022.2109591

10. Creemers, R. (2020). China's conception of cyber sovereignty. In *Governing Cyberspace: Behavior, Power and Diplomacy* (pp. 107–142). https://books.google.co.il/books?hl=en&lr=&id=F2vsDwAAQBAJ
11. DECISION No. 1,005 from November 23, 2020 (2020). https://legislatie.just.ro/Public/DetaliiDocument/234190
12. DECISION No. 271 of May 15, 2013 (2013). https://legislatie.just.ro/Public/DetaliiDocument/148324
13. DECISION No. 494 of May 11, 2011 Regarding the Establishment of the National Cyber Security Incident Response Center - CERT-RO (2011). https://legislatie.just.ro/Public/DetaliiDocument/129052
14. DECISION No. 584 of August 8, 2019 (2019). https://legislatie.just.ro/Public/DetaliiDocument/217149
15. Dimich, A., & Yeromina, L. (2022). Contemporary Scientific Approaches to the Definition of the Concept «Information Sovereignty of Ukraine». *Information Security of the Person, Society and State*, *34–36*, 13–19. https://doi.org/10.51369/2707-7276-2022-(1-3)-2
16. DINU, A., & CÎRNU, C.-E. (2024). Empowering National Cybersecurity: The CYRESRANGE Project. *Romanian Cyber Security Journal*, *6*(1), 1–10. https://doi.org/https://doi.org/10.54851/v6i1y202408
17. DRAGOMIR, A., & FLORESCU, I. (2022). Romania's Implementation of International and European Cyber Law to Strengthen National Cybersecurity. *International Journal of Information Security and Cybercrime*, *11*(2), 19–28. https://doi.org/10.19107/IJISC.2022.02.01
18. Eldem, T. (2021). Between Multi-stakeholderism and Cyber Sovereignty: Understanding Turkey's Cybersecurity Strategy. In *Routledge Companion to Global Cyber-Security Strategy*. Routledge. https://www.researchgate.net/publication/349723868_Between_Multi-stakeholderism_and_Cyber_Sovereignty_Understanding_Turkey's_Cybersecurity_Strategy
19. Fiveable. (n.d.). *Cyber sovereignty*. Retrieved 9 November 2024, from https://fiveable.me/key-terms/technology-policy/cyber-sovereignty
20. Gaiser, L. (2021). Seeking a New Order for Global Cybersecurity : The Russian approach to cyber-sovereignty. *Routledge Companion to Global Cyber-Security Strategy*, 153–164. https://doi.org/10.4324/9780429399718-15
21. Government of Romania. (n.d.). *Legislative Portal*. Retrieved 5 November 2024, from https://legislatie.just.ro/Public/Acasa
22. Government of Romania. (2013). *Cyber Security Strategy of Romania*. https://www.cyberwiser.eu/sites/default/files/RO_NCSS_2013_en.pdf
23. Government of Romania. (2021, December 30). *Strategy from December 30, 2021 of cyber security of Romania, for the period 2022-2027*. https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235

24. Jensen, E. (2014). Cyber Sovereignty: The Way Ahead. *Texas International Law Journal*, *50*. https://digitalcommons.law.byu.edu/faculty_scholarship/239
25. Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/IA/IIAC226
26. LAW No. 346 of July 21, 2006 (*republished*) (2006). https://legislatie.just.ro/Public/DetaliiDocument/73882
27. Law No. 415 of June 27, 2002 Regarding the Organization and Functioning of the Supreme National Defense Council (2002). https://csat.presidency.ro/ro/prima-pagina/legea-de-organizare
28. Leiter, A. (2020). Cyber Sovereignty: A Snapshot From a Field in Motion. *Harvard International Law Journal Frontiers*, *60*, 1–6. https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/Leiter-PDF-format.pdf
29. Maleh, Y., & Maleh, Y. (2022). *Cyber Sovereignty in Morocco*. 77–89. https://doi.org/10.1007/978-3-031-18475-8_7
30. Ministry of Communication and Information Technology. (2014). *National Strategy on Digital Agenda for Romania*. https://www.trusted.ro/wp-content/uploads/2014/09/Digital-Agenda-Strategy-for-Romania-8-september-2014.pdf
31. Ministry of National Defence. (2015). *White Paper on Defense*. https://eda.europa.eu/docs/default-source/Defence-Procurement-Gateway/ro_white-paper-on-defence.pdf
32. Ministry of National Defence. (2021). *Military Strategy of Romania*. https://www.mapn.ro/legislatie/documente/STRATEGIA-MILITARA-A-ROMANIEI-ENG.pdf
33. Ministry of National Defence of Romania. (2005a). *Military Strategy of Romania*. https://www.files.ethz.ch/isn/156801/RomaniaMilitaryStrategy.pdf
34. Ministry of National Defence of Romania. (2005b). *Romania's National Security Strategy*. https://www.files.ethz.ch/isn/156799/Romania%20nationalsecurity.pdf
35. Ministry of National Defense. (2016). *The Military Strategy of Romania*. https://eda.europa.eu/docs/default-source/Defence-Procurement-Gateway/ro_milstrategy.pdf
36. Nadeem Mirza, M., Abid Ali, L., & Hasnain Qaisrani, I. (2021). Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order. *Webology*, *18*(5), 598–610. https://www.webology.org/data-cms/articles/20220301123539amwebology%2018%20(5)%20-%2099%20pdf.pdf

37. Nagy, M. (2021). Cyber Security Strategies of the Visegrád Group States and Romania. *Acta Universitatis Sapientiae, European and Regional Studies*, *19*, 72–87.
38. Palladino, N., & Amoretti, F. (n.d.). The Ambiguity of Digital Sovereignty between Cybersecurity and Digital Rights. *International Political Science Association*. Retrieved 16 November 2023, from https://www.ipsa.org/wc/paper/ambiguity-digital-sovereignty-between-cybersecurity-and-digital-rights
39. Pandey, K. (2024, August 20). *Chinese notion of cyber sovereignty: Building an alternate digital order*. Observer Research Foundation. https://www.orfonline.org/expert-speak/chinese-notion-of-cyber-sovereignty-building-an-alternate-digital-order
40. Pavel, T. (2024). Defining Digital Boundaries: A Study on Israel's Cyber Sovereignty Policy. *International Journal of Applied Technology & Leadership*, *3*(1), 1–15. https://www.researchgate.net/publication/377219706_Defining_Digital_Boundaries_A_Study_on_Israel's_Cyber_Sovereignty_Policy?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InNlYXJjaCIsInBvc2l0aW9uIjoicGFnZUhlYWRlciJ9fQ
41. PETCU, I., & BARBU, D.-C. (2022). The New Challenges of Romania's Cyber Security Policy. *Romanian Cyber Security Journal*, *4*(1), 57–67. https://doi.org/10.54851/V4I1Y202207
42. Presidential Administration. (2015). *National Defence Strategy Romania 2015-2019*. https://eda.europa.eu/docs/default-source/Defence-Procurement-Gateway/national-defense-strategy-2015---2019.pdf
43. Presidential Administration. (2020). *National Defence Strategy 2020-2024*. https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf
44. Ro'is, N. (2022). Cyber Sovereignty Gotong Royong, Indonesia'a Way of Dealing with the Challenges of Global Cyber Sovereignty. *Pancasila and Law Review*, *3*(1), 15–30. https://doi.org/10.25041/PLR.V3I1.2573
45. Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, *31*(3), 439–456. https://doi.org/10.1007/S11023-021-09566-7/METRICS
46. Schmitt, M. (2020, December 17). *Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)*. EJIL: Talk! https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/
47. Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9
48. Schöndorf, R. (2020, December 9). *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*. EJIL: Talk! https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/
49. The Functioning Regulation of the Supreme Council of Defense of the Country (2002). https://csat.presidency.ro/ro/prima-pagina/regulament-de-functionare
50. The National Cyber Security Directorate. (2021). *EMERGENCY ORDINANCE 104/2021 on establishing the National Cyber Security Directorate*. https://dnsc.ro/vezi/document/emergency-ordinance-104-2021-on-establishing-the-national-cyber-security-directorate
51. The President. (2007). *The National Security Strategy of Romania*. https://www.bbn.gov.pl/ftp/dok/07/ROU_National_Security_Strategy_Romania_2007.pdf
52. Tshering Tshering, J. (2021). *Digital Data Sovereignty: A Case Study on Bhutan*. https://www.researchgate.net/publication/353443155_Digital_Data_Sovereignty_A_Case_Study_on_Bhutan
53. United Nations Institute for Disarmament Research. (n.d.). *Romania - Cyber Policy Portal*. Retrieved 5 November 2024, from https://cyberpolicyportal.org/states/romania
54. Vasiloiu, I. C. (2022). Cybersecurity education in Romania - competitive advantage in the EU market. *Proceedings of the International Conference on Virtual Learning*, *17*, 297–307. https://doi.org/10.58503/ICVL-V17Y202225
55. VOINA, A., PAVELEA, A., & CULIC, L. (2021). Hashtag Feminism in Romania: #MeToo and Its Effects on Cyberspace Behavior. *Transilvania*, *11–12*, 62–70. https://doi.org/10.51391/trva.2020.12.07
56. WHITE PAPER of 11 May 2021 (2021). https://legislatie.just.ro/Public/DetaliiDocumentAfis/242221
Zlati, G. (2021). Cybercrime in Romania. *Jurnalul Baroului Cluj*, *2021*. https://heinonline.org/HOL/Page?handle=hein.journals/jbcluj2021&id=6&div=&collection=.