جامعة عبد الحميد بن باديس مستغانم
كلية الحقوق والعلوم السياسية
مخبر القانون العقاري والبيئة

مشروع البحث التكويني الجامعي PRFU

"أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها-دراسة استشرافية قانونية"-

الرقم: 105/ م ق ع ب/ 2025 مستغانم في: 09 جوان 2025

شهادة نشر فصل في كتاب

تشهد السيدة رئيسة مشروع الكتاب الموسوم ب " استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني أن الدكتور(ة) حجاب عبد الغني من جامعة المسيلة قد ساهم(ت) في تأليف فصل تحت عنوان:

The Role of Artificial Intelligence in Enhancing Digital Sovereignty and Cybersecurity: A Case Study of Algeria

من الكتاب الحامل للترقيم الدولي ISBN 978-9969-544-36-7

سلمت هذه الشهادة لاستعمالها في حدود ما يسمح به القانون.

رئيسة مشروع الكتاب

د. والي حاجة
أستاذة محاضرة
كلية الحقوق و العلوم السياسية
جامعة مستغانم

جامعة عبد الحميد بن باديس-مستغانم
كلية الحقوق والعلوم السياسية
مخبر القانون العقاري والبيئة

بالتعاون مع مشروع البحث التكويني الجامعي PRFU:
" أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها-دراسة استشرافية قانونية-"

استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني

رئيسة الكتاب الجماعي:
الدكتورة وافي حاجة

جمع وتنسيق:
الدكتورة لطروش أمينة

توطئة:

إن ثورة تكنولوجيا المعلومات والاتصال التي مست مختلف دول العالم دون استثناء جعل هذه الأخيرة تعرف تطور في المفهوم التقليدي للسيادة الذي كان مرتبط بقدرة الدولة على تسيير شؤونها الداخلية والخارجية بطريقة منفردة ومستقلة دون المساس بها من قبل أيا كان، غير أن التطور الذي عرفه المجتمع الدولي بداية بالاعتراف بالعديد من الأشخاص كأشخاص فاعلين في المجتمع الدولي وصولا إلى العولمة وتسارع التحول الرقمي كل هذا ساهم في ظهور مفاهيم جديدة على غرار ما بات يعرف بالسيادة الرقمية، هذا من جهة.

من جهة أخرى أسهمت ثورة تكنولوجيا المعلومات والاتصال في حدوث طفرة في التهديدات الأمنية لتنتقل من البعد العسكري الى التهديدات السيبرانية حيث أن الدول في الوقت الراهن تواجه تحديات جديدة تهدد سيادتها الرقمية، والتي ترتكز على الحروب السيبرانية والهجمات الإلكترونية التي تستهدف أنظمتها الحيوية. وعليه لم تعد أساليب الدفاع التقليدية كافية لمجابهة هذه التهديدات المستجدة، لذا أصبحت أنظمة الذكاء الاصطناعي أداة أساسية لتعزيز القدرات الدفاعية الرقمية، قصد الكشف المبكر عن التهديدات والتعامل الفعّال معها في الوقت المناسب وبنجاعة كبيرة.

كل هذا جعل الذكاء الاصطناعي يحدث ثورة في مجال الأمن السيبراني من خلال تقديم حلول فعالة لمكافحة التهديدات السيبرانية بدءًا من الكشف عن التهديدات وحتى الاستجابة للحوادث، بحيث تعمل الأدوات والتقنيات المعتمدة على الذكاء الاصطناعي على تعزيز كفاءة وفعالية التدابير الأمنية ويتجلى ذلك من خلال التعامل مع كميات هائلة من البيانات، وتحديد التهديدات غير المعروفة، والتعلم المستمر والتكيف مع أساليب الهجوم الجديدة، كل هذا يجعل من أنظمة الذكاء الاصطناعي أداة لا تقدر بثمن في سبيل الكشف عن التهديدات السيبرانية والاستجابة لها بكفاءة وفعالية أكبر.

بذلك نجد أن مسألة تعزيز السيادة الرقمية في ظل تحديات الأمن السيبراني وفي عصر الذكاء الاصطناعي، تواجهها تحديات ورهانات عديدة، الأمر الذي يستدعي وضع سياسات واستراتيجيات دولية ووطنية عبر تحديد التطبيقات الحديثة للذكاء الاصطناعي في المجالات الأمنية، واقتراح حلول مبتكرة للتصدي للحروب السيبرانية مع الاخذ بعين الاعتبار بين الاستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية البيانات والمعطيات، والسهر على ترقية ونشر ثقافة رقمية أساسها التحسيس المستمر واليقظة الإعلامية لكل مؤسسات الدولة على اختلافها، وبطبيعة الحال كل هذا يستلزم تكاثف الجهود المؤسساتية والتشريعية لتعزيز السيادة الرقمية وتحقيق الأمن السيبراني في عصر الذكاء الاصطناعي.

أهداف الكتاب:

- التعرف على الذكاء الاصطناعي واستخداماته.
- التعرف على السيادة الرقمية.
- التعرف على الامن السيبراني وابعاده.
- تأثير استخدامات الذكاء الاصطناعي على السيادة الرقمية والأمن السيبراني.
- استكشاف دور الذكاء الاصطناعي في تعزيز الأمن السيبراني.
- السياسات والاستراتيجيات الدولية والوطنية المتبعة لتحقيق السيادة الرقمية وتعزيز الأمن السيبراني في ظل تنامي أنظمة الذكاء الاصطناعي.

الإشكالية:

ما هو دور أنظمة الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني؟ وكيف استطاعت الدول وبالأخص الجزائر في حماية سيادتها الرقمية في ظل بزوغ تهديدات أمنية ذات طابع رقمي؟

محاور الكتاب الجماعي:

المحور الأول: مفاهيم حول: الذكاء الاصطناعي-السيادة الرقمية-الأمن السيبراني.

المحور الثاني: تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني وحماية السيادة الرقمية.

المحور الثالث: رهانات وتحديات استخدام الذكاء الاصطناعي في مجال الامن السيبراني.

المحور الرابع: السياسات الدولية والوطنية المتبعة لتحقيق السيادة الرقمية وتعزيز الأمن السيبراني .

استخدامات الذكاء الاصطناعي

في

تعزيز السيادة الرقمية وتحقيق الأمن السيبراني

فصول في كتاب من تأليف مجموعة من المؤلفين

الإشراف العام على الكتاب: الدكتورة وافي حاجة

دار الأيمة للنشر والتوزيع
Editions LAIMMA

عنوان الكتاب: استخدامات الذكاء الاصطناعي
تعزيز السيادة الرقمية وتحقيق الأمن السيبراني في
اسم المؤلف: إشراف الدكتورة وافي حاجة
الحجم: 15,5 × 23,5
عدد الصفحات: 487
ISBN : 978-9969-544-36-7
منشورات دار لايمة، 2025
الإيداع القانوني: ماي-2025

للتواصل معنا

القليعة-تيبازة-الجزائر

الهاتف النقال: 550.085.725 (0) 213 +

WWW NLLIBRAIRIE.COM

المقدمة

إن الحمد لله، نحمده ونستعينه ونستغفره، ونعوذ بالله من شرور أنفسنا وسيئات أعمالنا، من يهده الله فلا مضل له، ومن يضلل فلا هادي له. وأشهد أن لا إله إلا الله وحده لا شريك له، وأشهد أن محمداً عبده ورسوله.

وبعد...

فإن ما يُكتب ويُسطر، إنما هو أثر من آثار الإنسان، وقد جرت سنة الله ألا يرتفع شيء إلا بفضل، ولا يثبت إلا بأصل، ولا يُبارك في عمل إلا بإخلاص، فما هذا الجهد إلا نفحة من فضل الله.

نسأله سبحانه أن يجعل هذا العمل خالصاً لوجهه الكريم، وأن ينفع به من قرأه، ويجعله شاهداً لا علينا، بل لنا يوم نلقاه، وهو أرحم الراحمين.

نحمد الله على إخراج هذا الكتاب العلمي حول استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني بمشاركة مجموعة من المؤلفين من داخل الجزائر وخارجها بالتعاون مع مشروع البحث التكويني الجامعي-PRFU- الموسوم ب «أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها-دراسة استشرافية قانونية-" الموطن بمخبر القانون العقاري والبيئة.

إن ثورة تكنولوجيا المعلومات والاتصال التي مست مختلف دول العالم دون استثناء جعل هذه الأخيرة تعرف تطور في المفهوم التقليدي للسيادة الذي كان مرتبط بقدرة الدولة على تسيير شؤونها الداخلية والخارجية بطريقة منفردة ومستقلة دون المساس بها من قبل أيا كان، غير أن التطور الذي عرفه المجتمع الدولي بداية بالاعتراف بالعديد من الأشخاص كأشخاص فاعلين في المجتمع الدولي وصولا إلى العولمة وتسارع التحول الرقمي كل هذا ساهم في ظهور مفاهيم جديدة على غرار ما بات يعرف بالسيادة الرقمية، هذا من جهة.

من جهة أخرى أسهمت ثورة تكنولوجيا المعلومات والاتصال في حدوث طفرة في التهديدات الأمنية لتنتقل من البعد العسكري الى التهديدات السيبرانية حيث أن الدول في

الوقت الراهن تواجه تحديات جديدة تهدد سيادتها الرقمية، والتي ترتكز على الحروب السيبرانية والهجمات الإلكترونية التي تستهدف أنظمتها الحيوية. وعليه لم تعد أساليب الدفاع التقليدية كافية لمجابهة هذه التهديدات المستجدة، لذا أصبحت أنظمة الذكاء الاصطناعي أداة أساسية لتعزيز القدرات الدفاعية الرقمية، قصد الكشف المبكر عن التهديدات والتعامل الفعّال معها في الوقت المناسب وبنجاعة كبيرة.

كل هذا جعل الذكاء الاصطناعي يحدث ثورة في مجال الأمن السيبراني من خلال تقديم حلول فعالة لمكافحة التهديدات السيبرانية بدءًا من الكشف عن التهديدات وحتى الاستجابة للحوادث، بحيث تعمل الأدوات والتقنيات المعتمدة على الذكاء الاصطناعي على تعزيز كفاءة وفعالية التدابير الأمنية ويتجلى ذلك من خلال التعامل مع كميات هائلة من البيانات، وتحديد التهديدات غير المعروفة، والتعلم المستمر والتكيف مع أساليب الهجوم الجديدة، كل هذا يجعل من أنظمة الذكاء الاصطناعي أداة لا تقدر بثمن في سبيل الكشف عن التهديدات السيبرانية والاستجابة لها بكفاءة وفعالية أكبر.

بذلك نجد أن مسألة تعزيز السيادة الرقمية في ظل تحديات الأمن السيبراني وفي عصر الذكاء الاصطناعي، تواجهها تحديات ورهانات عديدة، الأمر الذي يستدعي وضع سياسات واستراتيجيات دولية ووطنية عبر تحديد التطبيقات الحديثة للذكاء الاصطناعي في المجالات الأمنية، واقتراح حلول مبتكرة للتصدي للحروب السيبرانية مع الاخذ بعين الاعتبار بين الاستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية البيانات والمعطيات، والسهر على ترقية ونشر ثقافة رقمية أساسها التحسيس المستمر واليقظة الإعلامية لكل مؤسسات الدولة على اختلافها، وبطبيعة الحال كل هذا يستلزم تكاثف الجهود المؤسساتية والتشريعية لتعزيز السيادة الرقمية وتحقيق الأمن السيبراني في عصر الذكاء الاصطناعي.

وعليه تتمحور الإشكالية الرئيسية لهذا الكتاب حول: ما هو دور أنظمة الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني؟ وكيف استطاعت الدول وبالأخص الجزائر في حماية سيادتها الرقمية في ظل بزوغ تهديدات أمنية ذات طابع رقمي؟

للإجابة على هذه الإشكالية تم تقسيم الكتاب إلى بابين كل باب يتناول ثمانية فصول، بحيث تطرقنا في الباب الأول إلى الإطار المفاهيمي والتشريعي للذكاء الاصطناعي والسيادة

الرقمية والأمن السيبيراني، في حين يتناول الباب الثاني آليات وتحديات الذكاء الاصطناعي في إطار تعزيز السيادة الرقمية وتحقيق الأمن السيبراني.

في ختام نشكر كل من ساهم وشارك في هذا الإنتاج العلمي الذي نتمنى أن يشكل إضافة في حقل البحث العلمي لاسيما القانوني منه.

الدكتورة وافي حاجة

رئيسة مشروع البحث التكويني الجامعي-PRFU- الموسوم ب "أنظمة الذكاء الاصطناعي بين تعزيز حماية حقوق الإنسان والتهديد بانتهاكها"

-دراسة استشرافية قانونية-

المشرفة العامة على الكتاب

Chapter 06

The Role of Artificial Intelligence in Enhancing Digital Sovereignty and Cybersecurity:

A Case Study of Algeria

دور الذكاء الاصطناعي في تعزيز السيادة الرقمية والأمن السيبراني: دراسة حالة الجزائر،

Dr. Abdelghani Hadjab (MCA) Mohamed Boudiaf University-M'sila (Algeria)

د. عبد الغني حجاب (أستاذ محاضر أ) جامعة محمد بوضياف بالمسيلة (الجزائر)

abdelghani.hadjab@univ-msila.dz

الملخص

أصبح الذكاء الاصطناعي (AI) أداة حاسمة في تعزيز السيادة الرقمية والأمن السيبراني، خاصة للدول التي تسعى لحماية بنيتها التحتية الرقمية من التهديدات المتطورة. تبحث هذه الدراسة دور الذكاء الاصطناعي في تعزيز الأمن السيبراني والاستقلالية الرقمية في الجزائر، مع التركيز على تطبيقاته في كشف التهديدات وحماية البيانات وتأمين البنى التحتية الحرجة. من خلال منهج دراسة الحالة، تقيّم الورقة الوضع الحالي للأمن السيبراني في الجزائر، وتحدد التحديات الرئيسية، وتستكشف كيف يمكن للحلول المدعومة بالذكاء الاصطناعي أن تقلل المخاطر مع تعزيز السيادة الرقمية الوطنية. تُظهر النتائج إمكانات الذكاء الاصطناعي في تحسين آليات الدفاع الاستباقي، وأتمتة الاستجابة للحوادث، وتقليل الاعتماد على التقنيات

الأجنبية في مجال الأمن السيبراني. وتختتم الدراسة بتوصيات سياساتية لدمج الذكاء الاصطناعي في الاستراتيجية الوطنية للأمن السيبراني في الجزائر لضمان المرونة والاكتفاء التكنولوجي.

الكلمات المفتاحية: الذكاء الاصطناعي (AI)، السيادة الرقمية، الأمن السيبراني، الجزائر، كشف التهديدات.

Abstract

Artificial Intelligence (AI) is increasingly becoming a pivotal tool in strengthening digital sovereignty and cybersecurity, particularly for nations seeking to safeguard their digital infrastructure against evolving threats. This study examines the role of AI in enhancing Algeria's cybersecurity framework and digital autonomy, focusing on its applications in threat detection, data protection, and critical infrastructure security. Through a case study approach, the paper evaluates Algeria's current cybersecurity landscape, identifies key challenges, and explores how AI-driven solutions can mitigate risks while reinforcing national digital sovereignty. The findings highlight the potential of AI in improving proactive defense mechanisms, automating incident response, and reducing dependency on foreign cybersecurity technologies. The study concludes with policy recommendations for integrating AI into Algeria's national cybersecurity strategy to ensure resilience and technological self-sufficiency.

Keywords: Artificial Intelligence (AI), Digital Sovereignty, Cybersecurity, Algeria, Threat Detection.

1. Introduction

The digital realm increasingly defines the contemporary global landscape, which has become indispensable for national security, economic prosperity, and the overall well-being of societies. Within this context, the concepts of digital sovereignty and cybersecurity have emerged as critical pillars for nations seeking to navigate the complexities and challenges of the digital age. Digital sovereignty, at its core, concerns the ability of a nation to exercise control over its digital infrastructure, data, and technological development, safeguarding its interests and the rights of its citizens. Cybersecurity, on the other hand, focuses on protecting digital assets and systems from a wide array of threats in cyberspace. The intersection of these two domains is becoming ever more crucial as nations strive to maintain autonomy and security in an increasingly interconnected world.

The advent of artificial intelligence (AI) represents a transformative force with the potential to significantly impact both digital sovereignty and cybersecurity. AI, with its advanced capabilities in data analysis, automation, and pattern recognition, offers new avenues for enhancing a nation's control over its digital resources and for bolstering its defenses against sophisticated cyber threats. However, the rise of AI also presents potential challenges, including concerns about data privacy, algorithmic bias, and the concentration of AI power in the hands of a few global entities. Consequently, the pursuit of what is increasingly termed "AI

sovereignty" has gained momentum, reflecting the desire of nations to maintain control over their AI development and deployment.

Nations today face a complex landscape of digital threats, ranging from sophisticated state-sponsored attacks aimed at critical infrastructure and sensitive data to the pervasive challenges of cybercrime, including ransomware, phishing, and identity theft. These threats can have significant consequences for national security, economic stability, and public trust. In this environment, the strategic application of AI in both enhancing digital sovereignty and strengthening cybersecurity capabilities is of paramount importance.

The central research question addressed in this article is: **What is the role of artificial intelligence in enhancing digital sovereignty and achieving cybersecurity, and how has Algeria specifically addressed these challenges?**

To answer this question, the **article aims** to: define digital sovereignty and cybersecurity from recent academic perspectives; analyze the potential of AI in strengthening the various components of digital sovereignty; examine the crucial role of AI in enhancing cybersecurity capabilities across detection, prevention, and response; present a detailed case study of Algeria's efforts in pursuing digital sovereignty and cybersecurity, with a particular focus on its adoption and development of AI; and finally, identify the key challenges and opportunities that Algeria faces in this evolving landscape.

The structure of this article will proceed as follows:

Section 2 will establish the conceptual framework by defining digital sovereignty and cybersecurity.

Sections 3 and **4** will analyze the synergistic role of AI in enhancing digital sovereignty. Section IV will explore AI as a cornerstone of modern cybersecurity.

Section 5 will present a detailed case study of Algeria's pursuit of digital sovereignty and cybersecurity.

Section 6 will discuss the challenges and opportunities for Algeria in this context.

Finally, **Section 7** will **conclude** with a summary of key findings and broader implications.

2. Conceptual Framework: Digital Sovereignty and Cybersecurity

The concept of digital sovereignty has garnered increasing attention in academic and policy circles as the digital realm becomes more central to state power and societal functioning. Recent academic definitions highlight various facets of this evolving idea. Digital sovereignty is broadly understood as the capacity of a country or region to exercise control over its digital infrastructure, data usage, and technological advancements without being unduly influenced by external forces. This encompasses the authority to make strategic decisions, create laws, and enforce them within the digital sphere. Some scholars define it as the ability to have control over one's digital destiny, encompassing the data, hardware, and software that a nation relies on and creates. This perspective emphasizes the importance of fostering homegrown tech industries, particularly where national security consequences are significant[1].

From a political economy standpoint, digital sovereignty can be seen as the manifestation of a political claim by a community to act as an autonomous agent in the digital realm. This understanding

[1] Sean Fleming, what is digital sovereignty, and how are countries approaching it? | World Economic Forum, Accessed May 9, 2025 https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

underscores that sovereignty is not merely about technological control but also about a conscious assertion of autonomy in the digital space[1]

Furthermore, digital sovereignty is increasingly viewed as encompassing the need to maintain and shape modes of freedom for individuals and groups within digitized societies. This perspective suggests that digital sovereignty should be normatively oriented towards vulnerability and freedom, remaining open to tensions and ambivalences in the digital environment[2].

The demand for digital sovereignty often involves an idea of greater autonomy, freedom of choice, co-determination, and control over "the digital". However, it is important to recognize that achieving complete self-sufficiency in all areas of the digital realm is neither possible nor sensible. Rather, the goal is often to create sufficient decision-making scope and reduce dependencies on potential hegemonic actors in the digital space. Ultimately, digital sovereignty can be understood as the power of a governing body to rule over itself in the digital realm, free from any interference by outside sources or bodies[3].

[1] Marília Maciel, Digital sovereignty: The end of the open internet as we know it? (Part 1) – Diplo Foundation, Accessed May 9, 2025 https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/

[2] Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? Information, Communication & Society, 1–14. https://doi.org/10.1080/1369118X.2024.2332624

[3] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

Key components of digital sovereignty include data sovereignty, technological sovereignty, cybersecurity sovereignty, and legal sovereignty. Data sovereignty refers to the ability of a country or region to exercise full control over the data collected and processed within its territory, including establishing legal and regulatory frameworks for data protection and management. Technological sovereignty denotes the capacity to independently develop and manage a nation's technological infrastructure and resources, which is crucial for national security and innovation. Cybersecurity sovereignty ensures the protection of a nation's digital infrastructure and systems from cyber threats through the implementation of standards and incident management mechanisms. Finally, legal sovereignty refers to the ability to create and enforce a nation's own legal rules in the digital space, regulating online services and digital platforms[1]. These components highlight the multifaceted nature of digital sovereignty and the various dimensions that nations must address to assert their autonomy in the digital age.

Cybersecurity, as a crucial element of digital sovereignty, is defined in academic literature as the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyberattacks. Its primary aim is to reduce the risk of cyberattacks and to safeguard against the unauthorized exploitation of digital assets. Fundamentally, cybersecurity involves ensuring the confidentiality, integrity, and availability of information

[1] Hulkó G, Kálmán J and Lapsánszky A (2025) the politics of digital sovereignty and the European Union's legislation: navigating crises. Front. Polit. Sci. 7:1548562. doi: 10.3389/fpos.2025.1548562

in the digital realm[1]. Confidentiality entails keeping sensitive information private and accessible only to authorized individuals, often through methods like encryption and access controls. Integrity ensures that data has not been tampered with and remains accurate and complete throughout its lifecycle. Availability means keeping systems and data accessible to authorized users when needed, while protecting against disruptions such as cyberattacks.

A more comprehensive academic definition views cybersecurity as the collection and coordination of resources, including personnel, infrastructure, structures, and processes, to protect networks and cyber-enabled computer systems from events that compromise integrity and interfere with property rights[2]. This definition emphasizes the proactive and resource-intensive nature of cybersecurity in addressing present and emerging challenges in the digital environment. It is also understood as a multidisciplinary process that involves prevention, detection, and response to attacks[3]. This includes identifying potential vulnerabilities and instituting effective strategies to minimize the impact of possible threats[4].

[1] What is Cybersecurity? - CISA, Accessed May 9, 2025 https://www.cisa.gov/news-events/news/what-cybersecurity

[2] Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity, arxiv.org, https://doi.org/10.48550/arXiv.2302.02274

[3] Cybersecurity - Glossary | CSRC - NIST Computer Security Resource Center, Accessed May 9, 2025 https://csrc.nist.gov/glossary/term/cybersecurity

[4] Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity - ResearchGate, Accessed May 9, 2025 DOI:10.48550/arXiv.2302.02274DOI:10.48550/arXiv.2302.02274

Key principles and practices of cybersecurity include authentication, which verifies the identity of users trying to access systems; authorization, which determines what verified users can access; and the implementation of strong password practices, regular software updates, data backup strategies, and robust access control mechanisms. User education and awareness training are also critical components, as human error remains a leading cause of data breaches[1].

The relationship between digital sovereignty and cybersecurity is deeply intertwined. Cybersecurity is not merely a technical issue but a fundamental condition for achieving and maintaining digital sovereignty. A state's inability to effectively protect its digital infrastructure and data from cyber threats directly undermines its capacity to exercise control over its digital space and safeguard its national interests in the digital age. Conversely, a strong commitment to digital sovereignty provides the legal and policy framework for implementing and enforcing robust cybersecurity measures nationally[2]. Cyber incidents can strike at the very core of a nation's sovereignty by disrupting critical infrastructure, enabling the theft of intellectual property and state secrets, facilitating disinformation campaigns, and creating dominance by foreign ICT suppliers. Therefore, the pursuit of digital sovereignty inherently necessitates a

[1] What is Cyber Security? Definition & Best Practices - IT Governance, Accessed May 9, 2025 https://www.itgovernance.co.uk/what-is-cybersecurity

[2] Benjamin de Carvalho, Digital Sovereignty, Policy Brief, 2(2022), Accessed May 9, 2025. http://dx.doi.org/10.13140/RG.2.2.13315.27680

strong focus on establishing and maintaining a high level of cybersecurity[1].

Table 1: Academic Definitions of Digital Sovereignty

Definition
Ability to manage and regulate digital infrastructure, data, and technological development
Control over digital destiny, including data, hardware, and software
Capacity to control digital infrastructure, data use, and technological advancements without undue influence
A political community consciously understands itself as an autonomous agent in the digital realm
Maintaining and shaping modes of freedom for individuals and groups within digitized societies
More autonomy, freedom of choice, co-determination, and control over "the digital"
Power of a governing body to rule over itself in the digital realm, free from external interference

[1] Paul Timmers, Matthijs Punter, Claire Stolwijk, Cybersecurity and Digital sovereignty - Bridging the gaps, securitydelta.nl, Accessed May 9, 2025 https://securitydelta.nl/media/com_hsd/report/702/document/Whitepaper-digital-sovereignty.pdf

3. The Synergistic Role of Artificial Intelligence

Artificial intelligence offers a powerful suite of tools and capabilities that can significantly enhance various aspects of digital sovereignty, particularly in the realms of data, technology, and cybersecurity. By leveraging AI, nations can strengthen their control over their digital assets and reduce their reliance on external entities.

In the context of data sovereignty, AI provides advanced capabilities for enhanced data analysis and localization. AI-driven algorithms can be employed for robust data encryption and protection, ensuring that sensitive information remains secure within national borders. The concept of sovereign AI further underscores this, advocating for the development of AI models based on a country's own unique data, research, and intelligence. This approach allows nations to maintain greater control over the data used to train AI systems and the data generated by them, reducing the risk of foreign access or interference. The ability of AI to efficiently analyze large datasets can also help in identifying and managing sensitive national data, providing a deeper understanding of national resources and trends[1].

Technological sovereignty can also be significantly bolstered by the strategic application of AI. AI can facilitate the development of tailored technological solutions to address specific industrial and

[1] Niall McCarthy, Navigating Digital Sovereignty in the Age of AI - Planet Crust, Accessed May 9, 2025 https://www.planetcrust.com/decoding-digital-sovereignty-meaning-navigating-ai-era/?utm_campaign=blog

national needs, thereby reducing reliance on imported technologies[1]. By investing in national AI capabilities and infrastructure, countries can direct their technological future in alignment with their unique strategic priorities and cultural values[2]. The development of domestic AI capabilities aims to reduce dependence on foreign AI technologies, protecting nations from potential supply chain disruptions and reinforcing national sovereignty in critical technological domains[3]. This focus on homegrown innovation can stimulate domestic AI innovation, enhance national economic competitiveness, and create high-value jobs within the country[4].

While the role of AI in cybersecurity sovereignty will be explored in greater detail in the subsequent section, it is important to note here that AI is also playing an increasing role in legal sovereignty within the digital realm. AI-powered tools can assist in developing and enforcing legal rules in the digital space by monitoring compliance with data protection and AI governance

[1] Sanjay Misra, Petter Kvalvik, Bjørn Axel Gran, Kai Morgan Kjølerbakken, Aida Omerovic, Nadia Saad Noori, Book on Digital Sovereignty - IFE, Routledge, (Taylor & Francis Group), 2025, Accessed May 9, 2025 https://ife.no/en/research-fields/digital-sovereignty-artificial-intelligence-human-centric-ai-cybersecurity-digital-trust-icds-2024/

[2] Brian Letort, what is sovereign AI and why is it growing in importance? - Digital Realty, 2025, Accessed May 9, 2025 https://www.digitalrealty.com/resources/articles/what-is-sovereign-ai

[3] Muath Alduhishy, Sovereign AI: What it is, and 6 ways states are building it | World Economic Forum, 2024, Accessed May 9, 2025 https://www.weforum.org/stories/2024/04/sovereign-ai-what-is-ways-states-building/

[4] The Rise of Sovereign AI: National Strategies, Global Implications, Alphanome.AI, Accessed May 9, 2025 https://www.alphanome.ai/post/the-rise-of-sovereign-ai-national-strategies-global-implications

regulations. The ability of AI to analyze vast amounts of digital data can help in identifying potential violations of national laws, ensuring that online services and digital platforms operate within the established legal framework.

The concept of AI sovereignty has emerged as a critical subset of digital sovereignty, reflecting the growing understanding that control over AI development and deployment is essential for overall national autonomy in the digital age. Concerns about the increasing dominance of a small number of companies in the AI landscape have driven the need for nations to assert control over their use of AI through the development of national infrastructure and skills[1]. Pursuing AI sovereignty is seen as the latest and perhaps most crucial step in the ongoing quest for digital sovereignty, as AI continues its rapid spread into virtually every aspect of society, culture, and economy[2].

[1] Michael Webb, What is AI Sovereignty, and why does it matter for education? - Artificial intelligence, Accessed May 9, 2025 https://nationalcentreforai.jiscinvolve.org/wp/2024/08/02/what-is-ai-sovereignty-and-why-does-it-matter-for-education/

[2] Akash Kapur, From Digital Sovereignty to Digital Agency - New America, Accessed May 9, 2025 https://www.newamerica.org/planetary-politics/briefs/from-digital-sovereignty-to-digital-agency/

Table 2: Key Components of Digital Sovereignty and AI Enhancement

Component	Description	AI Enhancement
Data Sovereignty	Control over data collected and processed within a nation's borders	Enhanced data analysis and localization, AI-driven encryption and protection, Building AI on national data
Technological Sovereignty	Independent development and control of technological infrastructure	Developing tailored solutions, investing in national AI capabilities, reducing reliance on foreign AI
Cybersecurity Sovereignty	Protection of digital infrastructure from cyber threats	(Covered in Section IV)
Legal Sovereignty	Ability to create and enforce laws in the digital space	Developing and enforcing legal rules, Monitoring and enforcing data protection and AI governance

4. AI as a Cornerstone of Modern Cybersecurity

Artificial intelligence has become an indispensable component of modern cybersecurity strategies, offering significant enhancements across threat detection, prevention, and response. Its ability to process and analyze vast quantities of data at high speeds, identify complex patterns, and adapt to evolving threats makes it a crucial asset in defending against increasingly sophisticated cyberattacks.

In the domain of threat detection, AI excels at analyzing massive datasets from various sources, including network traffic, user behavior, and system logs, to identify patterns and anomalies that may indicate malicious activity. Machine learning algorithms, a key subset of AI, are particularly effective in performing behavioral analysis and anomaly detection, establishing baselines of normal activity and flagging any deviations that could signify a potential threat. AI systems can also monitor networks, endpoints, and applications in real-time, providing continuous vigilance against emerging threats. Furthermore, AI enables predictive analytics, allowing security teams to anticipate future threats based on the analysis of historical attack data and emerging trends[1]. This capability is vital for identifying new and complex threats, such as

[1] AI In Cybersecurity: Enhancing Threat Detection And Prevention, Boston Institute of Analytics, Accessed May 9, 2025 https://bostoninstituteofanalytics.org/blog/ai-in-cybersecurity-enhancing-threat-detection-and-prevention/

zero-day exploits and advanced persistent threats (APTs), which often evade traditional signature-based detection methods[1].

AI also plays a critical role in threat prevention. AI-powered threat hunting tools can proactively search for hidden threats within an organization's systems, identifying and neutralizing them before they can cause harm. Predictive analytics capabilities allow AI to identify vulnerabilities in systems and recommend necessary patches or security measures to prevent potential exploitation by attackers. AI enhances endpoint security by continuously monitoring activity on user devices and detecting and neutralizing threats directly at the endpoint, thus preventing breaches before they occur. Some organizations even use AI to simulate social engineering attacks, helping to identify potential vulnerabilities in human behavior and allowing for targeted training to improve overall security awareness[2].

The application of AI in threat response has revolutionized how organizations manage and mitigate cyber incidents. AI-driven systems can automate responses to certain types of attacks, enabling faster mitigation and reducing the potential for significant damage. AI-powered incident response systems can analyze security alerts in real-time, prioritize threats based on their severity, and automate workflows for investigating, containing, and eradicating attacks. This includes capabilities such as isolating affected systems and blocking

[1] What is AI in cybersecurity? EC-Council University, Accessed May 9, 2025 https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/

[2] AI and Cybersecurity: A New Era | Morgan Stanley, 2024, Accessed May 9, 2025 https://www.morganstanley.com/articles/ai-cybersecurity-new-era

malicious IP addresses automatically[1]. Moreover, AI-driven threat intelligence provides security teams with a deeper understanding of attack trends, allowing them to proactively adapt their security measures and stay ahead of emerging threats[2].

Machine learning (ML) is a fundamental component of many AI applications in cybersecurity. Supervised learning involves training ML models on labeled datasets of known benign and malicious samples, enabling them to predict whether new, unseen samples are malicious. Unsupervised learning, on the other hand, allows ML algorithms to analyze unlabeled data and discover hidden structures, relationships, and patterns, which can be invaluable for uncovering new attack patterns and anomalies. Reinforcement learning, a third type of ML, involves training models through trial and error, rewarding correct actions and penalizing incorrect ones, which can be particularly useful for identifying innovative ways to solve complex cybersecurity problems. Machine learning also enables the rapid processing and synthesis of large volumes of security data, allowing security teams to operationalize intelligence from various sources in near real-time[3]. Through continuous learning from

[1] AI-Powered Incident Response: Revolutionizing Threat Detection and Mitigation - Cyble, Accessed May 9, 2025 https://cyble.com/knowledge-hub/ai-powered-incident-response/

[2] Courtney Goodman, AI in Cybersecurity: Transforming Threat Detection and Prevention - Balbix, 2025, Accessed May 9, 2025 https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

[3] Lucia Stanham, Machine Learning (ML) in Cybersecurity: Use Cases - CrowdStrike, 2023, Accessed May 9, 2025 https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/machine-learning/

evolving data, ML models can improve their accuracy over time, reduce false positives, and adapt to the ever-changing threat landscape[1].

5. Algeria's Pursuit of Digital Sovereignty and Cybersecurity

Algeria has recognized the increasing importance of the digital realm for its national development and has embarked on a comprehensive digital transformation strategy. The government has placed a significant focus on improving the nation's digital infrastructure, regulatory frameworks, and the provision of digital services to its citizens. A key objective of this strategy is to position Algeria as a leading digital hub in the region by the year 2029, fostering an ecosystem where technology drives economic growth, innovation flourishes, and global partnerships thrive. Digital sovereignty has been identified as a central pillar in achieving this vision, with the government expressing a clear commitment to strengthening Algeria's control over its digital destiny[2].

In line with its digital sovereignty goals, Algeria has undertaken several significant cybersecurity initiatives. In 2020, the government established the National Council for Information Systems Security (CNSSI). Operating within the Ministry of

[1] What Is Machine Learning in Cybersecurity? | The University of Tulsa, 2024, Accessed May 9, 2025 https://online.utulsa.edu/blog/what-is-machine-learning-cybersecurity/

[2] Connected Algeria accelerates the nation's transition towards a competitive, digitally-driven economy., Accessed May 9, 2025 https://www.connectedalgeria.dz/about

National Defense, the CNSSI is responsible for developing the national strategy for information systems security. The government also created the Agency for Information Systems Security, tasked with implementing and enforcing the policies and strategies approved by the CNSSI. Furthermore, Algeria has put in place laws related to data protection and cybercrime, including Law No. 07-18 on the protection of natural persons in the processing of personal data[1]. The National Information Security Repository (NISR), published in 2020, provides a set of recommendations, best practices, guidelines, and controls to improve the security of information systems for individuals and companies, aligning with various international standards[2]. Efforts to strengthen national cybersecurity agencies and overall strategies are ongoing, as Algeria aims to build a more secure digital landscape[3].

Algeria has also recognized the strategic importance of artificial intelligence for its digital sovereignty and has taken proactive steps to build capabilities in this field. In 2023, the government established an AI Council, jointly under the Ministry of Higher Education and Scientific Research and the Ministry of Knowledge Economy,

[1] Hana Saada, "Algeria Aims to Enhance its Digital Sovereignty," Says Head of National Authority for the Protection of Personal Data - Dzair Tube, 2024, Accessed May 9, 2025 https://www.dzair-tube.dz/en/algeria-aims-to-enhance-its-digital-sovereignty-says-head-of-national-authority-for-the-protection-of-personal-data/

[2] Abdeldjalil Fortas, Cybersecurity and governance | The State of Software Engineering in Algeria, 2025, Accessed May 9, 2025 https://state-of-algeria.dev/docs/insights/cybersecurity/

[3] Algeria's Cybersecurity Journey: A Nation on the Rise! - EKSec, 2024, Accessed May 9, 2025 https://eksec.net/algerias-cybersecurity-journey-a-nation-on-the-rise/

Startups, and Micro-Enterprises. The nation has also adopted a National Artificial Intelligence Strategy, aiming to improve Algerian skills in AI through education, training, and research, and to leverage AI as a development tool across various socio-economic sectors. This strategy focuses on key areas such as scientific research, creating a supportive environment for AI development, building local expertise, and assisting startups in providing AI-powered solutions[1]. To support these efforts, Algérie Télécom, the state-owned telecom company, announced the launch of an investment fund dedicated to startups specializing in AI, cybersecurity, and robotics[2]. The government also emphasizes the importance of aligning AI strategies with national priorities, including cybersecurity, recognizing the potential of AI to enhance the nation's digital defenses.

[1] Benjamin FLAUX, Algeria Unveils AI Strategy to Boost Digital Transformation - Ecofin Agency, 2024, Accessed May 9, 2025 https://www.ecofinagency.com/public-management/1012-46241-algeria-unveils-ai-strategy-to-boost-digital-transformation

[2] Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025 https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

Table 3: Algeria's Digital Sovereignty and Cybersecurity Initiatives

Initiative	Description
National Council for Information Systems Security (CNSSI)	Develops national strategy for information systems security.
Agency for Information Systems Security	Implements and enforces cybersecurity policies and strategies.
Law No. 07-18 on the protection of natural persons in the processing of personal data	Establishes legal framework for data protection.
National Information Security Repository (NISR)	Provides guidelines and best practices for information security.
AI Council	Scientific advisory body for AI strategy and policy.
National Artificial Intelligence Strategy	Aims to improve AI skills and leverage AI for socio-economic development.
Investment fund for AI, cybersecurity, and robotics startups	Supports the growth of the tech ecosystem in these key areas.

6. Challenges and Opportunities for Algeria

Despite the progress made, Algeria faces several challenges in its pursuit of digital sovereignty and robust cybersecurity. The regulatory environment in Algeria has been described as slow to adapt to rapidly evolving international digital trends, which can hinder the growth of the digital economy and the adoption of new technologies. Gaps in digital infrastructure persist, particularly in rural areas where access to high-speed broadband remains limited, creating a digital divide within the country. Enhancing digital skills and awareness among a broader segment of the population is also crucial for maximizing the benefits of digital transformation and improving overall cybersecurity posture[1].

Balancing the need for stringent data protection regulations, which are essential for digital sovereignty, with the need to foster an environment conducive to the development and deployment of AI technologies presents another challenge. Additionally, Algeria's reliance on imported hardware and software for its digital infrastructure could potentially create vulnerabilities and undermine its digital sovereignty in the long term[2].

[1] Hadia Beghoura, Algeria - Digital Economy - International Trade Administration, 2024, Accessed May 9, 2025 https://www.trade.gov/country-commercial-guides/algeria-digital-economy

[2] Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025 https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

However, Algeria also has significant opportunities to further advance its digital sovereignty and cybersecurity goals. The strong commitment and strategic focus on digital transformation at the highest levels of government provide a solid foundation for continued progress. The government's proactive investments in AI and cybersecurity startups and the development of national digital infrastructure are likely to yield positive results in the coming years. The establishment of key institutions such as the AI Council and the CNSSI demonstrates a forward-thinking approach to governance and coordination in these critical areas[1]. With its strategic location and growing digital capabilities, Algeria has the potential to emerge as a regional leader in digital transformation, setting an example for other nations in the Middle East and North Africa. Furthermore, by strategically leveraging AI to enhance its cybersecurity capabilities, Algeria can better protect its critical infrastructure, sensitive data, and national interests in the increasingly complex digital landscape[2].

[1] Maria Buza, Sherif Taha, DPA Digital Digest: Algeria [2025 Edition], Digital Policy Alert, 2025, Accessed May 9, 2025 https://digitalpolicyalert.org/digest/dpa-digital-digest-algeria

[2] Driving Innovation in AI for a Smarter Algeria, aicouncil, Accessed May 9, 2025 https://aicouncil.dz/

7. Conclusion

The analysis presented in this article underscores the critical and increasingly intertwined roles of artificial intelligence, digital sovereignty, and cybersecurity in the contemporary global context. AI offers powerful tools for enhancing a nation's control over its digital assets and for strengthening its defenses against the growing spectrum of cyber threats. Digital sovereignty provides the overarching framework for nations to assert their autonomy in the digital realm, while cybersecurity serves as the essential foundation for ensuring the security and resilience of digital infrastructures and data.

Algeria's journey towards digital transformation highlights the nation's commitment to embracing the opportunities and addressing the challenges of the digital age. The establishment of national strategies and institutions focused on digital sovereignty, cybersecurity, and artificial intelligence demonstrates a proactive approach to building a secure and autonomous digital future. While challenges related to infrastructure, regulation, and skills development remain, Algeria's strategic investments and policy initiatives, particularly in the realm of AI, position it for potential leadership in the region's digital evolution.

The experiences of Algeria offer valuable lessons for other developing nations seeking to strengthen their digital sovereignty and cybersecurity in the age of AI. A holistic and strategic approach that integrates AI into national digital frameworks, addresses specific

national challenges, and leverages unique opportunities is crucial for success. As the digital landscape continues to evolve at a rapid pace, the ongoing commitment to innovation, adaptation, and international collaboration will be essential for all nations striving to secure their digital future.

References :

1. Abdeldjalil Fortas, Cybersecurity and governance | The State of Software Engineering in Algeria, 2025, Accessed May 9, 2025 https://state-of-algeria.dev/docs/insights/cybersecurity/

2. AI and Cybersecurity: A New Era | Morgan Stanley, 2024, Accessed May 9, 2025 https://www.morganstanley.com/articles/ai-cybersecurity-new-era

3. AI In Cybersecurity: Enhancing Threat Detection And Prevention, Boston Institute of Analytics, Accessed May 9, 2025 https://bostoninstituteofanalytics.org/blog/ai-in-cybersecurity-enhancing-threat-detection-and-prevention/

4. AI-Powered Incident Response: Revolutionizing Threat Detection and Mitigation - Cyble, Accessed May 9, 2025 https://cyble.com/knowledge-hub/ai-powered-incident-response/

5. Akash Kapur, From Digital Sovereignty to Digital Agency - New America, Accessed May 9, 2025 https://www.newamerica.org/planetary-politics/briefs/from-digital-sovereignty-to-digital-agency/

6. Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025

https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

7. Algeria earmarks $11 million to support AI, cybersecurity startups - Techpression, Accessed May 9, 2025 https://techpressionmedia.com/algeria-earmarks-11m-to-support-ai/

8. Algeria's Cybersecurity Journey: A Nation on the Rise! - EKSec, 2024, Accessed May 9, 2025 https://eksec.net/algerias-cybersecurity-journey-a-nation-on-the-rise/

9. Benjamin de Carvalho, Digital Sovereignty, Policy Brief, 2(2022), Accessed May 9, 2025. http://dx.doi.org/10.13140/RG.2.2.13315.27680

10. Benjamin FLAUX, Algeria Unveils AI Strategy to Boost Digital Transformation - Ecofin Agency, 2024, Accessed May 9, 2025 https://www.ecofinagency.com/public-management/1012-46241-algeria-unveils-ai-strategy-to-boost-digital-transformation

11. Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? Information, Communication & Society, 1–14. https://doi.org/10.1080/1369118X.2024.2332624

12. Brian Letort, What is sovereign AI and why is it growing in importance? - Digital Realty, 2025, Accessed May 9, 2025

https://www.digitalrealty.com/resources/articles/what-is-sovereign-ai

13. Connected Algeria accelerates the nation's transition towards a competitive, digitally-driven economy., Accessed May 9, 2025 https://www.connectedalgeria.dz/about

14. Courtney Goodman, AI in Cybersecurity: Transforming Threat Detection and Prevention - Balbix, 2025, Accessed May 9, 2025 https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

15. Cybersecurity - Glossary | CSRC - NIST Computer Security Resource Center, Accessed May 9, 2025 https://csrc.nist.gov/glossary/term/cybersecurity

16. Driving Innovation in AI for a Smarter Algeria, aicouncil, Accessed May 9, 2025 https://aicouncil.dz/

17. Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity, arxiv.org, https://doi.org/10.48550/arXiv.2302.02274

18. Francesco Schiliro, Towards a Contemporary Definition of Cybersecurity - ResearchGate, Accessed May 9, 2025 DOI:10.48550/arXiv.2302.02274DOI:10.48550/arXiv.2302.02274

19. Hadia Beghoura, Algeria - Digital Economy - International Trade Administration, 2024, Accessed May 9, 2025

https://www.trade.gov/country-commercial-guides/algeria-digital-economy

20. Hana Saada, "Algeria Aims to Enhance its Digital Sovereignty," Says Head of National Authority for the Protection of Personal Data - Dzair Tube, 2024, Accessed May 9, 2025 https://www.dzair-tube.dz/en/algeria-aims-to-enhance-its-digital-sovereignty-says-head-of-national-authority-for-the-protection-of-personal-data/

21. Hulkó G, Kálmán J and Lapsánszky A (2025) The politics of digital sovereignty and the European Union's legislation: navigating crises. Front. Polit. Sci. 7:1548562. doi: 10.3389/fpos.2025.1548562

22. Lucia Stanham, Machine Learning (ML) in Cybersecurity: Use Cases - CrowdStrike, 2023, Accessed May 9, 2025 https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/machine-learning/

23. Maria Buza, Sherif Taha, DPA Digital Digest: Algeria [2025 Edition], Digital Policy Alert, 2025, Accessed May 9, 2025 https://digitalpolicyalert.org/digest/dpa-digital-digest-algeria

24. Marília Maciel, Digital sovereignty: The end of the open internet as we know it? (Part 1) - DiploFoundation, Accessed May 9, 2025 https://www.diplomacy.edu/blog/digital-sovereignty-the-end-of-the-open-internet-as-we-know-it-part-1/

25. Michael Webb, What is AI Sovereignty, and why does it matter for education? - Artificial intelligence, Accessed May 9, 2025 https://nationalcentreforai.jiscinvolve.org/wp/2024/08/02/what-is-ai-sovereignty-and-why-does-it-matter-for-education/

26. Muath Alduhishy, Sovereign AI: What it is, and 6 ways states are building it | World Economic Forum, 2024, Accessed May 9, 2025 https://www.weforum.org/stories/2024/04/sovereign-ai-what-is-ways-states-building/

27. Niall McCarthy, Navigating Digital Sovereignty in the Age of AI - Planet Crust, Accessed May 9, 2025 https://www.planetcrust.com/decoding-digital-sovereignty-meaning-navigating-ai-era/?utm_campaign=blog

28. Paul Timmers, Matthijs Punter, Claire Stolwijk, Cybersecurity and Digital sovereignty - Bridging the gaps, securitydelta.nl, Accessed May 9, 2025 https://securitydelta.nl/media/com_hsd/report/702/document/Whitepaper-digital-sovereignty.pdf

29. Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

30. Sanjay Misra, Petter Kvalvik, Bjørn Axel Gran, Kai Morgan Kjølerbakken, Aida Omerovic, Nadia Saad Noori,Sanjay Misra, Petter Kvalvik, Bjørn Axel Gran, Kai Morgan Kjølerbakken, Aida Omerovic, Nadia Saad Noori, Book on Digital Sovereignty - IFE, Routledge, (Taylor & Francis

Group), 2025, Accessed May 9, 2025 https://ife.no/en/research-fields/digital-sovereignty-artificial-intelligence-human-centric-ai-cybersecurity-digital-trust-icds-2024/

31. Sean Fleming, What is digital sovereignty, and how are countries approaching it? | World Economic Forum, Accessed May 9, 2025 https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

32. The Rise of Sovereign AI: National Strategies, Global Implications, Alphanome.AI, Accessed May 9, 2025 https://www.alphanome.ai/post/the-rise-of-sovereign-ai-national-strategies-global-implications

33. What is AI in cybersecurity? EC-Council University, Accessed May 9, 2025 https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/

34. What is Cyber Security? Definition & Best Practices - IT Governance, Accessed May 9, 2025 https://www.itgovernance.co.uk/what-is-cybersecurity

35. What is Cybersecurity? - CISA, Accessed May 9, 2025 https://www.cisa.gov/news-events/news/what-cybersecurity

36. What Is Machine Learning in Cybersecurity? | The University of Tulsa, 2024, Accessed May 9, 2025

https://online.utulsa.edu/blog/what-is-machine-learning-cybersecurity/

الفهرس