QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Cyber Power and State Sovereignty: Redefining Security in the Digital Age

Dr. Ahmad Raza Khan
Assistant Professor, Department of Political Science,
GC University Lahore.
ahmadraza@gcu.edu.pk
Mr. Faisal Awais
Assistant Professor, School of Law,
Multan University of Science and Technology, Multan.
faisal.awais@multanust.edu.pk

Abstract
This paper explores the intricate relationship between cyber power and state sovereignty, analyzing how advancements in digital technologies necessitate a re-evaluation of traditional security paradigms. The proliferation of sophisticated cyber threats, coupled with the emergence of immersive digital environments like the Metaverse, introduces unprecedented challenges to national security, data privacy, and the exercise of state control over digital infrastructures. Furthermore, the integration of artificial intelligence within these digital ecosystems profoundly influences both the methods of cyber warfare and the strategies for defense, necessitating a detailed examination of AI's dual role in threat generation and cybersecurity enhancement. This analysis delves into the mechanisms through which AI-driven cyber capabilities, including self-learning autonomous defense agents, reshape global power dynamics and digital sovereignty by enabling real-time threat detection, adaptive response, and autonomous mitigation actions. This dual capacity of AI presents a complex landscape where states strive for sovereign control over AI infrastructures while simultaneously establishing sovereign competence through them. This dynamic tension underscores the need for a comprehensive framework to understand and combat the evolving challenges posed by AI-driven cyber threats, moving beyond reactive measures to proactive and predictive cybersecurity strategies. This paper therefore posits that the effective assertion of digital sovereignty in an AI-empowered landscape hinges on a nation's capacity to not only deploy advanced AI for defensive purposes but also to regulate its pervasive influence across critical infrastructure and emerging digital realms such as the Metaverse.

Keywords: *Artificial Intelligence, Cyber Warfare, Digital Sovereignty, Cybersecurity, Metaverse, National Security, Threat Detection, Autonomous Systems, International Law, Geopolitics.*

1. Introduction

The problem of the transition of power to the digital space and spaces implies the necessity to re-examine conventional concepts of state sovereignty that can now view digital infrastructure and digital resources in an increasingly globalized world (Kaloudis, 2024). The result of this digitalization is an increase in the attack area both of nation-states and cybercriminal and is a challenge to traditional perimeter-based protection strategies and requires new ways of looking at national security (Sontan and Samuel, 2024; Wu, 2025). The actual idea of power during the information age, then, passes through networks, and there is a need to have states control perception, manipulate information, and interfere with the decision-making process of adversaries in these dynamical digital ecosystems (Akoz and Sururi, 2025). This encompasses not only ensuring the national digital boundaries but also exerting cyber power to manipulate the relations with other countries and securing the critical infrastructure against the activities of state-sponsored and advanced non-state actors

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

(Balarabe, 2024; Wu, 2025). The Stuxnet case and the Estonian cyberattacks of 2007 are the crucial historical precedents that intensified a radical reconsideration of the cybersecurity policies worldwide due to the fact that critical infrastructures are deeply vulnerable to the advanced forms of cyber action (Oyewole et al., 2024). In addition, the Colonial Pipeline ransomware incident and the SolarWinds breach provide further examples of why the uncontrolled growth of digital ecosystems and their integration allows exploiting the vulnerability, making cybersecurity a kitchen table topic in the national security agenda (Malatji and Tolah, 2024). Due to this growing threat environment, there has been a need to re-evaluate the traditional security paradigms to deal with the transnational aspect of cyber warfare and how it can lead to the destabilization of countries (Botezatu and VEVERA, 2024). It is because cyber-attacks have become a more significant threat to critical infrastructure than certain physical attacks, and affect national sovereignty by causing digital disruptions and technological interdependence due to the convergence of cyber and physical worlds (Herzog, 2011; Molina et al., 2023; Timmers, 2023). The possibility of cyberattacks through the tools of disruptive and destructive intent on critical infrastructures is driven by cyber capabilities, which allow state and non-state actors to integrate cyberattacks with other types of terror tactics to deliver political signaling and psychological effects (Akoz and Sururi, 2025). This requires a reconsideration of the principles of national security because cyber terrorism obliterates the boundaries between political violence and cyber sabotage, and the importance of cyber resilience as a geopolitical necessity is crucially significant (Akoz and Sururi, 2025). This development highlights the need to take proactive actions to maintain international relations in the face of new cyber threats, and the fact that cybersecurity, global politics, and national stability are inextricably connected with each other (Oyewole et al., 2024). Hence, it is essential to comprehend the complex aspects of cyber power and how these affect state sovereignty in order to formulate effective policies related to cybersecurity in individual countries, and collaborate with other nations to address the emerging risks (Acworth, 2023).

The emergence of the cyberspace as a strategic arena (along with land, sea, air, and space) has made cyberspace a topical area of geopolitical rivalry where states are compelled to build advanced cyber capacity both to defend their interests and attack (Molina et al., 2023). It involves safeguarding national digital assets against a wide range of threats, such as advanced persistent threats, ransomware, and supply chain attacks, and may also, in turn, involve cyber operations to deliver on strategic goals (Adeyeri and Abroshan, 2024; Manoharan and Sarker, 2024). The increasing interconnectedness of critical infrastructures also increases the potential damage of cyberattacks, which is a major challenge to national security and a multi-layered defense approach is required (Housen-Couriel, 2025; Sontan and Samuel, 2024). In this strategic imperative, governments have been developing effective cybersecurity systems, establishing international relations, and investing in new technologies such as artificial intelligence to identify and curtail emerging cyber threats (Malatji and Tolah, 2024; Sontan and Samuel, 2024). Moreover, it is essential to incorporate the human and non-technical aspect into the discourse of cybersecurity and depart from the rather technology-oriented paradigm, focusing on the interdisciplinary approach that includes the impact of the cyber threat on society at large (Malatji and Tolah, 2024). This broadened view recognizes the fact that although AI can provide powerful defensive capabilities, in the form of automation and quick learning, these same capabilities and features have offered unprecedented opportunities for misuse by ill-intentioned individuals, and thus require a dynamic and offensive cybersecurity posture (Malatji, 2025).

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

2. Research problem.

This study will examine the complex nature of the Artificial Intelligence influence on cybersecurity with reports of how AI can be used as both a developmental tool in improving defense-related capabilities and as an avenue of new cyber-attack. Particularly, it aims at exploring the dualistic nature of AI in cybersecurity and how its use may enhance security, as well as add new weaknesses and attack patterns.

3. Research objectives and significance.

This study is a critical research on the emergent cybersecurity threats presented by AI tools used as malicious hacking tools especially in the IoT-based MIS systems. The project will consist of creating a general framework of studying and preventing AI-powered cyber-attacks, given their effects on the digital sovereignty and national security. Moreover, the study will explore the theoretical basis and practical relevance of these issues and the necessity to create adaptive security designs and coordinate international policies.

4. Conceptual Framework: Cyber Power and Sovereignty:

It is a framework that examines the complex connection between the ability of one state to wield power in cyberspace and the possibility of that state to stay controlling its digital infrastructure and data on its borders (Familoni, 2024). It also discusses how AI innovations are helping add to and frustrate this sovereignty both by allowing more advanced defense systems to be implemented and also establishing new paths of attack (Timmers, 2019). This type of analysis is also essential in comprehending the dynamic nature of cyber warfare and in formulating effective policies that will safeguard national interest in the ever-digitised world.

4.1.Defining Cyber Power

In this respect, cyber power is the capability of a country to use digital technologies and infrastructure to benefit itself at a national level, including offensive and defensive capabilities within the cyber domain (Stoltz, 2024). This involves the ability to perform cyber espionage, sabotage, and influence operations and the ability to protect critical national infrastructure and countering cyberattacks (Efe, 2025).

4.2.Classical and Modern Conceptions of State Sovereignty

Sovereignty of states that was long based on the idea of territorial jurisdiction and non-intervention is under severe threat in the digital era, as the cyber space is without borders (Familoni, 2024). This creates the need to re-examine the concept of national sovereignty in the digital age since cyber-attacks are able to bypass physical barriers and affect the critical infrastructure, economic well-being, and democratic activities of a country (Maathuis and Cools, 2025). Furthermore, the employment of highly autonomous AI agents in cybersecurity, despite its efficiency, also creates new risks that involve a sensitive approach to their structural design and functional goals to embed it in the framework of the current organizational risk management norms (Malatji, 2025).

4.3.Cyberspace as a Challenge to Territoriality

The very fact of deterritorialization of cyberspace undermines the conventional Westphalian model of state sovereignty as actors can act in the world without being physically present and without having to rely on the traditional means of national control and legal jurisdiction (Timmers, 2019). Such digital reality requires establishing new legal and regulatory frameworks, including legislation on digital sovereignty using AI infrastructure and fit-for-purpose co-regulatory systems with tech platforms, to regulate transnational cyber activities and preserve state powers (Srivastava and Bullock, 2024). The clash between the territoriality

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

of the traditional sovereignty and the borderless quality of cyberspace indicates the necessity of new strategies of digital governance, such as Indigenous views on data self-determination (Pierucci, 2025). This reconsideration also applies to digital sovereignty being viewed as one of the key determining factors in international relations, as both a defensive measure and a tool of diplomacy within a time when cyber warfare is on the rise (Kaloudis, 2024).

5. Cyber Threats and National Security Paradigms:

5.1.State-Sponsored Cyber Operations:

These activities are an important and expanding issue because nation-states use advanced cyber capabilities in collecting intelligence, industrial espionage, disrupting infrastructure, and manipulating politics (Kaloudis, 2024). The current war in Ukraine clearly demonstrates the paramount importance of cyber activity in the contemporary war and the necessity to have resilient and adaptive control structures to protect national interests and digital sovereignty (Maathuis and Cools, 2025). The next dimension of threat is the incorporation of AI into the state-sponsored operations, which makes more advanced and covert attacks with the potential to avoid conventional defense mechanisms possible, thus, necessitating the constant development of cybersecurity approaches (Malatji and Tolah, 2024). Moreover, the ethical aspects of AI in state-sponsored cyber activities, in terms of transparency and accountability, should be considered with great care to avoid unintended outcomes and retain credibility in the digital infrastructure of the world (Adewusi et al., 2024). This two-sided quality of AI as a tool of cyber defense and offense requires strong governance solutions that can guarantee strategic legitimacy as a concern of national interests and law (Alanezi and AL-Azzawi, 2024; Maathuis and Cools, 2025). These frameworks should include not just the technical capacity of AI but also more generally the societal and ethical effects of using AI in the setting of national security (as illustrated by the European Union AI Act debates, Kulothungan, 2024). To ensure that these multifaceted issues are handled, it is thus necessary to develop all-encompassing structures of global AI regulations in cybersecurity (Kulothungan, 2025).

5.2.Non-State Actors and Asymmetric Cyber Power:

In addition to threats sponsored by the state, the emergence of non-state actors, such as terrorist groups and cybercriminal gangs, has brought a specific asymmetrical aspect to the cyber warfare battleground, where the traditional ideas of military supremacy do not hold (Manoharan and Sarker, 2024). Such groups are progressively using cyberspace to achieve both strategic and tactical goals, such as financial benefits, propaganda broadcasting, and critical service interruption, in most cases, taking advantage of weaknesses in global supply chains and capitalizing on sophisticated persistent threats (Adeyeri and Abroshan, 2024). These non-state threats possess the additional advantage of being relatively anonymous and able to function internationally, making it unbelievably difficult to assign them responsibility and respond to them (Butler et al., 2025). In addition, the increasing complexity of AI-based tools available to these non-state actors, including those that automate phases of the attack lifecycle, also ends up making the task of defending against their dynamic strategies more difficult (Malatji and Tolah, 2024). It requires paradigm shift in the approach to cybersecurity by transitioning outside of a traditional perimeter protection to proactive efforts in threat intelligence, real-time behavioral analytics, and anomaly detection via AI to combat these hard-to-detect attackers (Abrahams et al., 2024; Sontan and Samuel, 2024).

5.3.Hybrid Warfare and Information Operations:

An example of a hybrid form of warfare is the combined application of both conventional and unconventional warfare tactics, and most commonly, the use of information as a key tool of

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

war, supplemented by cyberspace to influence public opinion and create discord (Nowicka et al., 2024). This may include advanced disinformation operations, propaganda distribution, and cyber-attacks on media infrastructure, all of which are designed to undermine confidence in institutions and have an effect on geopolitical results. Incorporating AI into the information operations also enhances their effects and allows the automatic production and distribution of high-persuasive and targeted information, making it more complicated to detect and counteract those (Uddin et al., 2025). To give just a few examples, AI can be used to produce highly convincing fake websites and emails, enhancing the success of phishing attacks, and also can be utilized to generate deepfakes which are an effective disinformation weapon (Malatji and Tolah, 2024; Molina et al., 2023). This intersection of AI with information functions demands superior defense strategies, such as applying AI to detect anomalies and forecasting, to prevent the developing threats and to protect the democratic models (Alanezi and AL-Azzawi, 2024). Further, artificial intelligence-generated fake news and fake reviews, as well as AI-aided stalking and forgery, are just some of the examples of malicious application of AI in information warfare (Malatji and Tolah, 2024).

6. International Law and the Regulation of Cyberspace:

6.1.Applicability of Existing International Law:

Although classical international laws (armed conflict, state sovereignty, and others) can provide certain foundations, their direct relevance to new cases of cyber warfare is still debatable and insufficient (Usman et al., 2023). This can be mostly attributed to the inability to define cyberattacks and the impossibility to attribute them, and the absence of universally accepted concepts defining such notions as the use of force in the cyber domain (Rahman et al., 2024). Such a gray zone reveals the pressing necessity to develop new legal tools and interpretations that could be effective to tackle the intricacies that AI-powered cyber activities bring, such as accountability and proportionality (Wong, 2022). Moreover, the lack of standardization of the effectiveness of different Generative AI models and commercially available security tools makes it difficult to come up with specific legal precedents and effective regulatory frameworks (Uddin et al., 2025). Another disadvantage is that the creation of new international norms and regulations is also undermined by the dual-use characteristic of a great number of AI technologies, which can be utilized both within legitimate defensive purposes and as weapons in the offensive uses. Such duality inherently requires a subtle regulation approach in terms of both stimulating innovation and the need to curb possible harms.

6.2.Sovereignty, Due Diligence, and State Responsibility:

The complex network of cyber activities, particularly of the AI genre, brings fundamental concerns on the issue of state sovereignty, and states need to show due diligence in ensuring their state is not used in perpetrating malicious cyber operations (Brown, 2018). Furthermore, the issue of attributing cyberattacks to certain state actors facilitates the issue of implementing the state responsibility, which complicates the responsibility of countries over AI-based cyber intrusions originating in their territories (Bayer et al., 2019). The further complicates the issue of responsibility attribution, especially when there is an element of a non-state actor, as the cyber warfare is being developed too fast, and there is the problem of attributing a cyberattack, and its secretive nature (Mazaraki and Goncharova, 2022).

6.3.Soft Law and Emerging Normative Frameworks:

The international community has long relied on the use of soft law tools and voluntary norms as an increasing complement to traditional hard law in regulating responsible state behavior in cyberspace, which is often inspired by multi-stakeholder discussions (Lahmann, 2023).

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

Although legally non-binding, these frameworks are designed to develop common understanding and expectations of state behavior and bring greater transparency and trust in an ever-expanding digital environment (Cahyanto et al., 2025). However, such soft law practices tend to be outpaced by the fast development of AI technologies, which results in regulatory gaps and difficulties in properly enforcing the laws in a variety of countries (Cristiano et al., 2023; Norhashim, n.d.). In addition, the fact that AI cannot be regulated due to the technical incompetence of the existing regulations and the fact that AI lacks geographical boundaries requires an international-level solution to overcome regulatory inertia (Zaidan and Ibrahim, 2024).

7. Redefining Sovereignty in the Digital Age:

The borderless character of cyberspace, which AI enhances due to the global nature of AI, is fundamentally problematic to the concept of state sovereignty, necessitating a revision of the territorial control and national jurisdiction of cyberspace (Cristiano et al., 2023). Reconsidering will require a new set of laws that would be capable of integrating the extraterritorial outcomes of cyber activities and the distributed character of AI systems (Timmers, 2019). This involves conceptualizing such issues as digital sovereignty, which assumes that a country has the right to regulate data and digital infrastructure inside of state borders and how global collaboration can help create norms that regulate cyberspace (Elmisery et al., 2025). In addition, the creation of effective international norms in cybersecurity requires a framework that involves continuous improvement, effective attribution, accountability measures, and proactive participation of international bodies and multi-stakeholder efforts (Balarabe, 2025) to facilitate its development.

7.1.Digital Sovereignty and Data Governance:

Digital sovereignty is also applied to the capacity of a state to own its digital frontiers, dominate data streams, and implement its laws in its digital space, which requires all-encompassing data management approaches (Familoni, 2024). It involves the adoption of policies that govern data localization, data privacy and the defense of critical digital infrastructure against foreign influence all of which are also being increasingly affected by the capabilities of AI technologies (Familoni, 2024). Digital sovereignty is also complicated by the fact that AI systems are transnational, meaning that the information processed by AI may have crossing jurisdictions, making the issue of the legal authority and ethical regulation a complex problem (Usman et al., 2023). Moreover, because AI governance becomes more entrenched, the states will tend to claim more supreme power on AI, despite AI supporting the preservation of the state power (Srivastava and Bullock, 2024).

7.2.Cyber Deterrence and Strategic Stability:

The spread of AI-enabled cyber capabilities demands reconsidering the old approach to deterrence and the states should take into account the impact of AI on the processes of strategic stability in the conventional and unconventional environments (Usman et al., 2023). It involves creating new strategies to combat cyber incursion that acknowledge the pace and self-directedness of AI-powered attacks, and defining red lines and escalation opportunities to ensure wrong calculation and unintended warfare (Malatji and Tolah, 2024). The evolution of AI into cyber warfare also requires the creation of advanced detection and response tools that can identify AI-generated threats and human-planned attacks and ensure that the strategic balance in a highly dynamic threat environment is preserved.

7.3.Sovereignty versus Global Internet Governance:

The conflict between national digital sovereignty and the need to have a globally connected internet is a major issue of concern to the policymakers requiring new governance paradigms

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

that can strike a balance between national security interests and the gains of an open digital ecosystem (Maathuis and Cools, 2025). This is complicated by the ubiquitous nature of multinationals and the difficulties of data sovereignty, and requires a reconsideration of the traditional models of digital security, data management, and economic competitiveness (Fratini et al., 2024). This dynamic process tends to be a complicated balance between social and personal authority, with technology firms more and more integrating AI frameworks into the worldwide framework of governance, simultaneously collaborating with and competing against state-based actors (Srivastava and Bullock, 2024). This dynamic emphasizes the difficulties of digital sovereignty, in which certain countries seek to create their own sovereign AI systems to oppose the role of any foreign technology company and to make sure they have control over important AI systems (Srivastava and Bullock, 2024). This quest to achieve this so-called sovereign AI usually entails significant government funding of local AI research and development in efforts to lessen the dependency on overseas AI models and platforms, and strengthen national cybersecurity and economic autonomy (Usman et al., 2023).

8. Case Studies

8.1.Estonia Cyber Attacks (2007)

The 2007 Estonian cyberattacks can also be viewed as a case in point as it was a trailblazer in showing the susceptibility of a highly digitalized society to state-sponsored aggression, and started an international reassessment of the doctrine of critical infrastructure protection and cyber defense. These incidents have highlighted the paramount significance of a multidisciplinary approach to the field of cybersecurity, which incorporates both technological progress and human factors of protection tactics (Oyewole et al., 2024). The attacks demonstrated the need of international cooperation and frameworks of mutual assistance to combat complex cyber threats, which resulted in projects such as the NATO Cooperative Cyber Defence Centre of Excellence. In addition, the case in Estonia triggered the discussion of legal principles in the context of cyber warfare, such as whether international humanitarian law applies and whether cyberattacks can be attributed to state actors (Srivastava and Bullock, 2024). The case also revealed the vulnerabilities in the current security procedures, which highlights the necessity of the constant renewal of security procedures to combat advanced attacks in digitally transformed settings (Homaei et al., 2024). The attacks also led to major changes in AI-based predictive-based approaches to preventive cybersecurity and created a shift in the paradigm of the reactive defense toward the anticipatory prevention of the threat (Radanliev, 2024).

8.2.Stuxnet Cyber Operation against Iran (2010)

A technologically advanced worm called the Stuxnet cyber operation, which was found in 2010, was a turning point in the history of cyber warfare because it showed that nation-state actors can cause physical harm to something critical to the state with the help of computers. The attack opened a new chapter in the history of cyber warfare when digital exploits could be transformed into real-life disruptions, and considerable reconsiderations of the approaches to the protection of critical infrastructure occurred around the world (Molina et al., 2023). The case of the Stuxnet incident also reinforced the need to have a solid security system in the industrial control system, and this has led to specialized cybersecurity frameworks and technologies to provide protection to the operational technology environments against such attacks (Rahimi and Jones, 2025). Malware was specifically designed to attack Supervisory Control and Data Acquisition systems and used zero-day vulnerabilities to exploit programmable logic controllers in the Iranian nuclear plants, which eventually malfunctioned

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 03 (2025)

with centrifuges (Aslam et al., 2025). This complex malware proved the actual possibility of cyber-physical damage, revealing the weakness of the industrial control system to serious cyber-attackers (Malatji and Tolah, 2024; Nuruzzaman and Rana, 2025).

8.3.SolarWinds Cyber Espionage Incident (2020)

In the 2020 SolarWinds hack, also known as Sunburst, this complex nature of vulnerabilities in digital supply chains was further demonstrated by the ability of advanced persistent threats to work quietly and silently (Malatji and Tolah, 2024). This incident with the large scale of its impact and the exposure of a significant part of the government agencies and private companies to various threats was a strong reminder of the fact that greater security in their supply chains and more effective threat intelligence sharing between organizations are necessary (Devanny et al., 2022). The attack highlighted the complexity of contemporary cyber espionage which tends to exploit supply chain vulnerabilities to gain extensive access to top-tier networks (Sontan & Samuel, 2024). It also highlighted the increased use of Artificial Intelligence and Machine Learning to enhance detection and response efforts to such sophisticated threats (Roshanaei et al., 2024). The SolarWinds event therefore cemented the need to maintain constant surveillance and proactive security stance to combat extremely well organized and resourceful attackers (Goel, 2020). The given real-life events, as well as other cases such as the one of the Colonial Pipeline attack, highlight the necessity to provide a holistic level of security to all levels of IIoT systems to avoid serious financial and operational losses (Zhukabayeva et al., 2025). These incidents, along with ransomware attacks on vital infrastructure, and other high-tech cyberattacks, show that modern systems are getting more interconnected, which offers a more entry point to attack (Malatji & Tolah, 2024). Indicatively, the 2018 cyberattack against industrial control systems in Ukraine caused a massive power outage that affected about 225,000 consumers, which underscores the real-life effects of cyberattacks on the society (Aslam et al., 2025).

9. Policy and Legal Implications:

All these examples highlight the fact that industrial sensors could be affected by even primitive tools, as in the case with Fuxnet, and hacktivist organizations could have a great impact without being highly sophisticated technologically, which illustrates a wide range of threats posed to critical infrastructure (Malikussaid & Sutiyo, 2025). The integration of Operational Technology and Information Technology, increases the attack surface and is more prone to a zero-day vulnerability, ransomware, supply chain attacks, and Advanced Persistent Threats (Paulraj et al., 2025). These events were analyzed in respect to the complexity and variety of cyber-physical attacks of critical infrastructure, demonstrating the immediate necessity to enhance security in interconnected control systems, legacy equipment, IoT/OT devices, and network edges that sometimes happen to be a highly visible point of entry (Ojo et al., 2024). Such events require reconsidering the existing cybersecurity systems and the immediate deployment of advanced detection systems, including AI/ML-based ones, to be proactive in noticing new threats (Ojo et al., 2024). Further, the widespread risk of ransomware, DDoS attacks, and advanced supply chain breaches as manifested in reports of a rise in these cases worldwide requires the development of effective defensive mechanisms that are specific to the vulnerabilities of the industrial IoT and operational technology settings (Kumar and Vardhan, 2025; Zhukabayeva et al., 2025). The increasing rate and complexity of such attacks, especially ransomware cases, is compelling organizations to secure systems that have not been developed with current cybersecurity in mind, which is a major source of technical debt of insecurity (Malikussaid and Sutiyo, 2025). The fact that IT and OT systems are becoming more and more interconnected is another contributor to this technical debt, as it

exposes an additional source of attacks and manages the response to the incidents more challenging (Aslam et al., 2025; Hammad, 2024). The nature of SCADA systems vulnerabilities as seen in the case of Stuxnet, along with the critical necessity of a sophisticated level of security countermeasures, compared to standard IT protocols (Nuruzzaman and Rana, 2025).

10. Conclusion

Consequently, an all-encompassing and proactive approach to cybersecurity is needed, which can be characterized by the combination of the latest technologies such as AI/ML and efficient policy frameworks and international partnership to protect the critical infrastructure in the face of the constantly changing threat environment (Bajwa et al., 2025; Daniel and Victor, 2024; Nuruzzaman and Rana, 2025). This can involve dealing with the legacy systems with its inherent vulnerabilities, improper network segmentation, and ineffective incident response processes that are often present in industrial control systems (Aslam et al., 2025). Therefore, the problem of sustainability and security of these systems needs to be addressed with an integrated strategy that should include resource optimization, energy control, and the implementation of green technologies (Aslam et al., 2025). Furthermore, the integration of the state-of-the-art security protocols, including artificial-intelligence-powered intrusion detection systems, will be the most important component to detect an unusual activity and react proactively to the emerging threats within these interconnected settings (Nuruzzaman and Rana, 2025). Cognitive science and machine learning application to decision-making systems can also enhance the performance of security analysts in dealing with intricate cyber threats, enhancing dissemination of information, and enabling a quicker response to incidents via automation and cognitive functions (Rehan, 2024). This interdisciplinary strategy that involves the integration of technology and strategic policy-making is essential in enhancing a sustainable cybersecurity environment that will be effective in reducing risks in smart cities and industrial setting (Chukwurah et al., 2024). It is an essential holistic approach that combines technological innovation and policy reinforcement to protect the critical infrastructure against the ever-growing complexity of cyber threats and provide the sustainability of smart city projects and industrial activities (Chukwurah et al., 2024; Nuruzzaman and Rana, 2025). Moreover, it is necessary to carry on the research and cooperate with AI researchers to formulate viable, quantifiable resolutions that can enhance long-term sustainability and improve security as well as operational efficiency (Asal et al., 2025).

List of References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION [Review of *A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION*]. *Computer Science & IT Research Journal*, *5*(1), 1. Fair East Publishers. https://doi.org/10.51594/csitrj.v5i1.699

Acworth, F. (2023). *National Security Policy Options For Cyber Ecosystem Resilience*. https://doi.org/10.26686/wgtn.22313419

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). REVIEW OF CYBERSECURITY STRATEGIES IN PROTECTING NATIONAL INFRASTRUCTURE: PERSPECTIVES FROM THE USA. *Computer Science & IT Research Journal*, *4*(3), 200. https://doi.org/10.51594/csitrj.v4i3.658

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E. M., Daraojimba, D. O., & Chimezie, O. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review [Review of *Artificial*

intelligence in cybersecurity: Protecting national infrastructure: A USA review]. *World Journal of Advanced Research and Reviews*, *21*(1), 2263. GSC Online Press. https://doi.org/10.30574/wjarr.2024.21.1.0313

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682. https://doi.org/10.3390/info15110682

Aköz, S., & Süruri, H. (2025). CYBERSECURITY IN CRITICAL INFRASTRUCTURES AND CYBER TERRORISM: A STRATEGIC ANALYSIS ON TÜRKİYE. *DergiPark (Istanbul University)*. https://doi.org/10.61314/traddergi.1618580

Alanezi, M., & AL-Azzawi, R. M. A. (2024). AI-Powered Cyber Threats: A Systematic Review [Review of *AI-Powered Cyber Threats: A Systematic Review*]. *Deleted Journal*, *4*(3), 166. https://doi.org/10.58496/mjcs/2024/021

Aslam, M. M., Tufail, A., Gul, H., Irshad, M. N., & Namoun, A. (2025). Artificial intelligence for secure and sustainable industrial control systems - A Survey of challenges and solutions. *Artificial Intelligence Review*, *58*(11). https://doi.org/10.1007/s10462-025-11320-9

Bajwa, A., Tonoy, A. A. R., Rana, Md. S., & Ahmed, I. (2025). *CYBERSECURITY IN INDUSTRIAL CONTROL SYSTEMS: A SYSTEMATIC LITERATURE REVIEW ON AI-BASED THREAT DETECTION FOR SCADA AND IOT NETWORKS*. *1*(1), 1. https://doi.org/10.63125/1cr1kj17

Balarabe, K. (2024). *Digital Borders and Beyond: Establishing Normative Grounds for Cybersecurity and Sovereignty in International Law*. https://doi.org/10.2139/ssrn.4876617

Balarabe, K. (2025). Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. *Computer Law & Security Review*, *58*, 106180. https://doi.org/10.1016/j.clsr.2025.106180

Bayer, J., Bitiukova, N., Bárd, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3409279

Berg, J. van den. (2024). Present-Day Cybersecurity: Actual Challenges and Solution Directions. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.1007021

Botezatu, U.-E., & VEVERA, A. V. (2024). Cyber Orbits: The Digital Revolution of Space Security. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.1005235

Brown, J. (2018). An Alternative War: The Development, Impact, and Legality of Hybrid Warfare Conducted by the Nation State. *Journal of Global Faultlines*, *5*. https://doi.org/10.13169/jglobfaul.5.1-2.0058

Butler, P. J., Kelley, J. H., Ellis, J., & Olatunbosun, S. (2025). Cybersecurity Threats: An Analysis of the Rise and Impacts of State Sponsored Cyber Attacks. In *Communications in computer and information science* (p. 187). Springer Science+Business Media. https://doi.org/10.1007/978-3-031-86644-9_14

Butt, Mag. J. S. (2024). Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024. *International Journal of Research Publication and Reviews*, *5*(3), 7343. https://doi.org/10.55248/gengpi.5.0324.0914

Cahyanto, T. N., Nurtono, A. Y., Susilo, T., Marpaung, B., & Saroso, B. (2025). Cyber War and Civil Protection in the Perspective of International Humanitarian Law: Legal Challenges and Innovations in the Digital Age. *Jurnal Impresi Indonesia*, *4*(5), 1422. https://doi.org/10.58344/jii.v4i5.6442

Campo, E. A. P. D., Alvis, S. P., Acevedo, M. E. S., & Aguirre, C. M. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi*, *16*(1). https://doi.org/10.15332/19090528.6480

Chesney, R., & Citron, D. K. (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3213954

Chukwurah, E. G., Okeke, C. D., & Ekechi, C. C. (2024). Innovation green technology in the age of cybersecurity: Balancing sustainability goals with security concerns. *Computer Science & IT Research Journal*, *5*(5), 1048. https://doi.org/10.51594/csitrj.v5i5.1115

Cristiano, F., Broeders, D. W. G. A., Delerue, F., Douzet, F., & Géry, A. (2023). Artificial intelligence and international conflict in cyberspace. In *Routledge eBooks* (p. 1). Informa. https://doi.org/10.4324/9781003284093-1

Daniel, S. A., & Victor, S. S. (2024). EMERGING TRENDS IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION: A COMPREHENSIVE REVIEW [Review of *EMERGING TRENDS IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION: A COMPREHENSIVE REVIEW*]. *Computer Science & IT Research Journal*, *5*(3), 576. Fair East Publishers. https://doi.org/10.51594/csitrj.v5i3.872

Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2022). Strategy in an Uncertain Domain: Threat and Response in Cyberspace. *Journal of Strategic Security*, *15*(2), 34. https://doi.org/10.5038/1944-0472.15.2.1954

Efe, A. (2025). BIR RISK PERSPEKTIFINDEN, YAPAY ZEKÂNIN (YZ) BT SISTEMLERINI HACKLEME VE HACKLENME POTANSIYELI. *DergiPark (Istanbul University)*. https://dergipark.org.tr/en/pub/btkdergi/issue/93609/1625825

Elmisery, A. M., Sertovic, M., Zayin, A., & Watson, P. F. (2025). Cyber Threats in Financial Transactions -- Addressing the Dual Challenge of AI and Quantum Computing. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2503.15678

Erigha, E. D., Obuse, E., Ayanbode, N., Cadet, E., & Etim, E. D. (2025). Self-Learning autonomous cyber defense agents in AI-empowered security operations. *Computer Science & IT Research Journal*, *6*(8), 475. https://doi.org/10.51594/csitrj.v6i8.2011

Familoni, B. T. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. *Computer Science & IT Research Journal*, *5*(3), 703. https://doi.org/10.51594/csitrj.v5i3.930

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Deleted Journal*, *3*(3). https://doi.org/10.1007/s44206-024-00146-7

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections The Quarterly Journal*, *19*(1), 73. https://doi.org/10.11610/connections.19.1.07

Gonçalves, C. P. (2019). Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.88648

Groesmeyer, J., Breitenbauch, H. Ø., Kristensen, K. S., & Valášek, T. (2019). Military and Environmental Challenges in the Arctic. *Research Portal Denmark*, 45. https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=ku&id=ku-14e4fb72-0407-4e95-8bf9-71718fe195f9&ti=Military%20and%20Environmental%20Challenges%20in%20the%20Arctic

Hacker, P., Kasirzadeh, A., & Edwards, L. (2025). AI, Digital Platforms, and the New Systemic Risk. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2509.17878

Hammad, E. (2024). *Demystifying Cybersecurity Experiential Learning for Operational Technologies (OT) and Industrial Control Systems (ICS)*. https://doi.org/10.18260/1-2--45370

Hasan, M. (2024). Regulating Artificial Intelligence: A Study in the Comparison between South Asia and Other Countries. *Legal Issues in the Digital Age*, *5*(1), 122. https://doi.org/10.17323/2713-2749.2024.1.122.149

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49. https://doi.org/10.5038/1944-0472.4.2.3

Homaei, M., Mogollón-Gutiérrez, Ó., Núñez, J. C. S., Ávila, M., & Caro, A. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence [Review of *A review of digital twins and their application in cybersecurity based on artificial intelligence*]. *Artificial Intelligence Review*, *57*(8). Springer Science+Business Media. https://doi.org/10.1007/s10462-024-10805-3

Housen-Couriel, D. (2025). Cybersecurity and national security: integrating new challenges. In *Edward Elgar Publishing eBooks* (p. 97). Edward Elgar Publishing. https://doi.org/10.4337/9781803929194.00011

Kaloudis, M. (2024). Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in Democracies. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.1005231

Kolade, T. M. (2024). Artificial Intelligence and Global Security: Strengthening International Cooperation and Diplomatic Relations. *Archives of Current Research International*, *24*(11), 23. https://doi.org/10.9734/acri/2024/v24i11945

Kulothungan, V. (2024). Securing the AI Frontier: Urgent Ethical and Regulatory Imperatives for AI-Driven Cybersecurity. *2021 IEEE International Conference on Big Data (Big Data)*, 5602. https://doi.org/10.1109/bigdata62323.2024.10826010

Kulothungan, V. (2025). Securing the AI Frontier: Urgent Ethical and Regulatory Imperatives for AI-Driven Cybersecurity. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2501.10467

Kumar, S., & Vardhan, H. (2025). Cyber security of OT networks: A tutorial and overview. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2502.14017

Lahmann, H. (2023). State Behaviour in Cyberspace: Normative Development and Points of Contention. *Zeitschrift Für Außen- Und Sicherheitspolitik*, *16*(1), 31. https://doi.org/10.1007/s12399-023-00939-7

Maathuis, C., & Cools, K. (2025a). *Digital Sovereignty Control Framework for Military AI-based Cyber Security*. https://doi.org/10.48550/ARXIV.2509.13072

Maathuis, C., & Cools, K. (2025b). Digital Sovereignty Control Framework for Military AI-based Cyber Security. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2509.13072

Malatji, M. (2025). A cybersecurity AI agent selection and decision support framework. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2510.01751

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00427-4

Malikussaid, & Sutiyo. (2025). Autonomous Cyber Resilience via a Co-Evolutionary Arms Race within a Fortified Digital Twin Sandbox. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2506.20102

Manoharan, A., & Sarker, M. (2024). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/irjmets32644

Mansur, M. C. (2025). National Security and Cyber Defense in the Rise of Artificial Super Intelligence. *European Scientific Journal ESJ*, *21*(10), 116. https://doi.org/10.19044/esj.2025.v21n10p116

Mazaraki, N., & Goncharova, Y. (2022). CYBER DIMENSION OF HYBRID WARS: ESCAPING A 'GREY ZONE' OF INTERNATIONAL LAW TO ADRESS ECONOMIC DAMAGES. *Baltic Journal of Economic Studies*, *8*(2), 115. https://doi.org/10.30525/2256-0742/2022-8-2-115-120

Molina, S. B., Nespoli, P., & Mármol, F. G. (2023). Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision [Review of *Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision*]. *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2312.06229

Nowicka, J., Ciekanowski, Z., Czternastek, M., Król, A., & Kacprzak, M. (2024). Navigating Hybrid Threats: Advanced Security Solutions for Modern Organizations. *EUROPEAN RESEARCH STUDIES JOURNAL*, 488. https://doi.org/10.35808/ersj/3414

Nuruzzaman, M., & Rana, Md. S. (2025). *IOT-ENABLED CONDITION MONITORING IN POWER DISTRIBUTION SYSTEMS: A REVIEW OF SCADA-BASED AUTOMATION, REAL-TIME DATA ANALYTICS, AND CYBER-PHYSICAL SECURITY CHALLENGES* [Review of *IOT-ENABLED CONDITION MONITORING IN POWER DISTRIBUTION SYSTEMS: A REVIEW OF SCADA-BASED AUTOMATION, REAL-TIME DATA ANALYTICS, AND CYBER-PHYSICAL SECURITY CHALLENGES*]. *1*(1), 25. https://doi.org/10.63125/pyd1x841

Ojo, B., Ogborigbo, J. C., & Okafor, M. O. (2024). Innovative solutions for critical infrastructure resilience against cyber-physical attacks. *World Journal of Advanced Research and Reviews*, *22*(3), 1651. https://doi.org/10.30574/wjarr.2024.22.3.1921

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio [Review of *Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio*]. *World Journal of Advanced Research and Reviews*, *21*(3), 625. GSC Online Press. https://doi.org/10.30574/wjarr.2024.21.3.0707

Paulraj, J., Raghuraman, B., Gopalakrishnan, N., & Otoum, Y. (2025). *Autonomous AI-based Cybersecurity Framework for Critical Infrastructure: Real-Time Threat Mitigation*. https://doi.org/10.48550/ARXIV.2507.07416

Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, *4*(1). https://doi.org/10.1007/s44206-025-00189-4

Radanliev, P. (2024). Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. *Frontiers in Blockchain*, *7*. https://doi.org/10.3389/fbloc.2024.1359130

Rahimi, N., & Jones, H. H. (2025). Cyber Warfare: Strategies, Impacts, and Future Directions in the Digital Battlefield. *Journal of Information Security*, *16*(2), 252. https://doi.org/10.4236/jis.2025.162013

Rahman, S. U., Shaikh, A., Tahir, M., Naseem, I., Sriyanto, S., Fatihah, N., Bandar, A., & Zaman, K. (2024). NAVIGATING MODERN WARFARE CHALLENGES: A REVIEW OF THE EVOLUTION OF INTERNATIONAL HUMANITARIAN LAW IN CYBERWARFARE [Review of *NAVIGATING MODERN WARFARE CHALLENGES: A REVIEW OF THE EVOLUTION OF INTERNATIONAL HUMANITARIAN LAW IN CYBERWARFARE*]. *Journal of Southwest Jiaotong University*, *59*(1). Science Press. https://doi.org/10.35741/issn.0258-2724.59.1.21

Rashid, A. (2024). *Untitled*. https://doi.org/10.55277/researchhub.vq5dnd6h

Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Deleted Journal*, *1*(1), 47. https://doi.org/10.60087/jaigs.v1i1.p66

Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions. *Journal of Information Security*, *15*(3), 320. https://doi.org/10.4236/jis.2024.153019

Shahana, A., Hasan, R., Farabi, S. F., Akter, J., Mahmud, Md. A. A., Johora, F. T., & Suzer, G. (2024). AI-Driven Cybersecurity: Balancing Advancements and Safeguards. *Journal of Computer Science and Technology Studies*, *6*(2), 76. https://doi.org/10.32996/jcsts.2024.6.2.9

Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*, *21*(2), 1720. https://doi.org/10.30574/wjarr.2024.21.2.0607

Srivastava, S., & Bullock, J. B. (2024a). AI, Global Governance, and Digital Sovereignty. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4996387

Srivastava, S., & Bullock, J. B. (2024b). AI, Global Governance, and Digital Sovereignty. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2410.17481

Stoltz, M. (2024). Artificial Intelligence in Cybersecurity: Building Resilient Cyber Diplomacy Frameworks. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.13585

Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4), 635. https://doi.org/10.1007/s11023-019-09508-4

Timmers, P. (2023). *Sovereignty in the Digital Age* (p. 571). https://doi.org/10.1007/978-3-031-45304-5_36

Uddin, M., Irshad, M., Kandhro, I. A., Alanazi, F., Ahmed, F., Maaz, M., Hussain, S., & Ullah, S. S. (2025). Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations [Review of *Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations*]. *Artificial Intelligence Review*, *58*(8). Springer Science+Business Media. https://doi.org/10.1007/s10462-025-11219-5

Usman, H., Tariq, I., & Nawaz, B. (2023). IN THE REALM OF THE MACHINES: AI'S INFLUENCE UPON INTERNATIONAL LAW AND POLICY. *Journal of Social Research Development*, *4*(2), 383. https://doi.org/10.53664/jsrd/04-02-2023-13-383-399

Wendt, J. A. (2023). ARTIFICIAL INTELLIGENCE, GENOM, CYBERSPACE AND SPACE – CONTEMPORARY THREATS TO THE SECURITY OF THE STATE AND NATIONS. *Revista Română de Geografie Politică*, *25*(2), 54. https://doi.org/10.30892/rrgp.252101-364

Wong, A. D. (2022). BLADERUNNER: Rapid Countermeasure for Synthetic (AI-Generated) StyleGAN Faces. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2210.06587

Wu, H. (2025). Multi-Domain Moving Target Defense for Resilient Security in Power Cyber-Physical Systems: A Review [Review of *Multi-Domain Moving Target Defense for Resilient Security in Power Cyber-Physical Systems: A Review*]. *Preprints.Org*. https://doi.org/10.20944/preprints202506.0030.v1

Zaidan, E., & Ibrahim, I. A. (2024). AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03560-x

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors*, *25*(1), 213. https://doi.org/10.3390/s25010213