

VOLUME 10 (2025) ISSUE 1

European Cybersecurity Journal

Strategic perspectives on cybersecurity
management and public policies

ANALYSES • POLICY REVIEWS • OPINIONS



THE KOSCIUSZKO INSTITUTE

European Cybersecurity Journal

Strategic perspectives on cybersecurity
management and public policies

The European Cybersecurity Journal (ECJ)
is a specialised publication devoted to cybersecurity.
The main goal of the Journal is to provide concrete
policy recommendations for European decision-makers
and raise awareness on both issues and problem-
-solving instruments.

Editorial Board:

Chief Editors:

Marietta Gieroń – Chairwoman,
the Kościuszko Institute

Paulina Górka – Project Coordinator,
the Kościuszko Institute

Proofreading:

Marietta Gieroń – Chairwoman,
the Kościuszko Institute

Paulina Górka – Project Coordinator,
the Kościuszko Institute

Members Of The Editorial Board:

Ciaran Martin – Professor of Practice, Blavatnik
School of Government, University of Oxford

Christopher Painter – Senior Advisor, Center for
Strategic and International Studies (CSIS)

dr Przemysław Roguski – University Chair for Public
International Law and Principal Investigator at the
Sovereignty 2.0

Rafał Rohozinski – Chief Executive Officer,
SecDev Group

Paul Timmers – Professor, University of Leuven

Design & DTP:

Wiktoria Konieczniak – Creative Manager,
the Kościuszko Institute

ISSN: 2450-2111

Citations: This journal should be cited as follows:
"European Cybersecurity Journal"
Volume 10 (2025) Issue 1, page reference



THE KOSCIUSZKO INSTITUTE

Published by:

The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków

Phone: 00 48 12 632 97 24

E-mail: editor@cybersecforum.eu

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute.
Authors may have consulting or other business relationships with the companies they discuss.

© 2025 The Kosciuszko Institute

All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without
the written permission of the publisher.

Contents

4

Enhancing Cyber Resilience:
Leveraging Advanced Threat
Intelligence Strategy and Tools
Against Cyber Threats

Adam Palmer
Dr. Carsten Willems

10

Rethinking
Cybersecurity: A Blueprint
for Europe's Digital Future

Matthias Muhlert

48

Toward Inclusive and
Equitable Cybersecurity
Governance

Kayle Giroud

53

Strategic autonomy and
the EU. A short history

Prof Dr Paul Timmers

67

DeGen Artificial Intelligence:
Challenges and Opportunities
of AI Applications

Marco Marsili

81

Mass data collection
in cyberspace and new methods
of fighting crime

Dr Paweł Opitek

91

Content Creators, Elections
and Disinformation: A US
Perspective

Alyssa Micalizzi

ARTICLE

DeGen Artificial Intelligence: Challenges and Opportunities of AI Applications

MARCO MARSILI

RESEARCHER AT CA' FOSCARI UNIVERSITY
OF VENICE

ABSTRACT:

Generative artificial intelligence (AI) is revolutionizing various fields, yet it also presents significant ethical, social, and technical challenges. This paper explores the dual nature of generative AI, highlighting its potential for innovation alongside its capacity for misuse, which we term “degenerate AI”. We will examine ethical dilemmas such as bias and misinformation, societal impacts including privacy and employment, and technical challenges related to system integrity and transparency. Additionally, we propose regulatory frameworks to ensure responsible AI development and deployment. This study aims to contribute to the discourse on AI ethics and governance, providing valuable insights for policymakers, technologists, and society.

Keywords: generative AI, ethics, social impact, technical challenges, regulatory frameworks, AI governance

Introduction

Generative artificial intelligence (AI) represents a groundbreaking advancement in the field of technology, with the ability to create content that ranges from text and images to music and complex simulations. This transformative capability has opened new avenues for innovation across various sectors, including healthcare, entertainment, and scientific research (Marsili, & Wróblewska-Jachna, 2024; Sengar, Hasan, Kumar, & Carroll, 2024). However, alongside its potential for positive impact, generative AI also poses significant ethical, social, and technical challenges that must be addressed to ensure its responsible development and deployment (Watson, Brezovec, & Romic, 2025).

The dual nature of generative AI—its capacity to generate both beneficial and harmful outcomes—necessitates a comprehensive examination of its implications. On one hand, generative AI can drive creativity, enhance productivity, and solve complex problems (Brynjolfsson & McAfee, 2014). On the other hand, it can perpetuate biases, spread misinformation, and be misused for malicious purposes such as creating deepfakes or automating cyberattacks (Chesney & Citron, 2019). This duality is encapsulated in the concept of “degenerate AI”, which refers to the unethical or harmful applications of AI that can cause significant societal harm.

This paper aims to explore the multifaceted nature of generative AI by delving into its ethical implications, social impact, and technical challenges. We will also propose regulatory frameworks to guide the responsible use of this technology. By providing a balanced analysis, this study seeks to contribute to the ongoing discourse on AI ethics and governance, offering valuable insights for policymakers, technologists, and society at large.

The following sections will discuss the ethical dilemmas associated with generative AI, including issues of bias and misinformation. We will then examine the societal impacts, focusing on privacy concerns, employment effects, and the digital

divide. The technical challenges related to system integrity, transparency, and accountability will also be addressed.

Finally, we will propose regulatory frameworks to ensure that the development and deployment of generative AI are conducted responsibly, balancing innovation with risk mitigation.

Ethical Implications of Generative AI

Generative artificial intelligence has the potential to revolutionize various industries by creating innovative solutions and enhancing productivity. However, its deployment also raises significant ethical concerns that must be addressed to ensure responsible use.

One of the primary ethical dilemmas associated with generative AI is the issue of bias. AI systems are trained on large datasets that often contain historical biases, which can be inadvertently perpetuated by the AI. This can lead to unfair treatment of certain groups and reinforce existing inequalities (Marsili, & Wróblewska-Jachna, 2024; Sengar et al., 2024). For example, facial recognition systems have been shown to exhibit racial and gender biases, resulting in higher error rates for minority groups (Buolamwini & Gebru, 2018).

Another critical ethical concern is the spread of misinformation.

Generative AI can create highly realistic but false content, such as deepfakes, which can be used to deceive and manipulate public opinion. This poses a significant threat to the integrity of information and can undermine trust in digital media.

The ability of generative AI to produce convincing fake news and misleading information necessitates the development of robust mechanisms to

detect and mitigate such risks (Chesney & Citron, 2019; Watson et al., 2025). For instance, deepfake videos have been used to impersonate public figures, leading to potential political and social unrest (Floridi et al., 2018).

Privacy is another major ethical issue. Generative AI systems often require vast amounts of data to function effectively, raising concerns about data privacy and security. The collection, storage, and use of personal data by AI systems must be carefully managed to protect individuals' privacy rights. Additionally, there is a risk that generative AI could be used to generate synthetic data that mimics real individuals, further complicating privacy concerns (Zuboff, 2019). For example, AI-generated synthetic voices can be used to create fraudulent audio recordings, posing risks to personal and financial security (Al-kfairy et al., 2024).

The potential misuse of generative AI for malicious purposes, such as automating cyberattacks or creating harmful content, also presents significant ethical challenges. Ensuring that AI systems are designed and deployed with safeguards to prevent misuse is crucial. This includes implementing measures to ensure accountability and transparency in AI systems, so that their actions can be understood and traced back to their developers and operators (Brynjolfsson & McAfee, 2014). For instance, AI-generated phishing emails can be highly convincing, increasing the risk of successful cyberattacks (Hagendorff, 2024).

Intellectual property and copyright infringement are additional ethical concerns. Generative AI can create content that closely resembles existing works, raising questions about originality and ownership. This can lead to disputes over intellectual property rights and the potential for AI-generated content to infringe on copyrighted material (Al-kfairy et al., 2024). For example, AI-generated art that mimics the style of famous artists can blur the lines between inspiration and plagiarism (Hagendorff, 2024).



Moreover, generative AI has been misused in several high-profile cases, highlighting the potential for harm. In 2023, a Belgian man took his life after interacting with an AI chatbot that encouraged his suicidal ideation (Hinduja, 2024). In another case, an English man attempted to assassinate the Queen of England after being encouraged by an AI chatbot (Hinduja, 2024). Additionally, AI-generated voices have been used in swatting incidents, where false emergencies are reported to law enforcement, leading to dangerous confrontations (Hinduja, 2024).

Further examples of misuse include financial fraud and identity theft. In a high-profile case from February 2024, an international company lost approximately \$26 million after an employee was tricked into making a financial transfer during an online meeting. In this instance, every other “person” in the meeting, including the company’s chief financial officer, was a convincing, computer-generated imposter (Marchal & Xu, 2024). Additionally, AI-generated content has been used to create fake social media profiles, which can be employed for various malicious purposes, including spreading disinformation and conducting scams (Mohamed, Osman, & Mohamed, 2024; Wei, & Tyson, 2024).

Social Impact of Generative AI

Generative artificial intelligence is reshaping various aspects of society, bringing both opportunities and challenges. One of the most significant social impacts of generative AI is its effect on employment. While AI has the potential to automate repetitive and mundane tasks, thereby increasing efficiency and productivity, it also poses a threat to jobs that are susceptible to automation. This displacement of jobs can lead to economic instability and increased inequality if not managed properly (Sengar, Hasan, Kumar, & Carroll, 2024; Brynjolfsson & McAfee, 2014).

Privacy concerns are another critical social issue associated with generative AI. The vast amounts of data required to train AI systems often include personal and sensitive information. The collection, storage, and use of this data raise significant privacy issues, as individuals may not always be aware of how their data is being used or have control over it. Moreover, the ability of generative AI to create synthetic data that closely mimics real individuals further complicates privacy concerns, potentially leading to identity theft and other forms of misuse (Watson, Brezovec, & Romic, 2025; Zuboff, 2019).

The digital divide is also exacerbated by the proliferation of generative AI. Access to advanced AI technologies is often limited to those with the necessary resources and infrastructure, creating a gap between those who can benefit from AI and those who cannot. This divide can lead to further social and economic disparities, as individuals and communities without access to AI technologies may be left behind in terms of education, employment, and overall quality of life (Marsili, & Wróblewska-Jachna, 2024; Eubanks, 2018).

Generative AI also has the potential to influence public opinion and social dynamics. The creation of realistic but false content, such as deepfakes, can be used to manipulate public perception and spread misinformation. This can undermine trust in digital media and institutions, leading to social unrest and polarization. The ability of generative AI to produce convincing fake news and misleading information necessitates the development of robust mechanisms to detect and mitigate such risks (Sengar et al., 2024; Chesney & Citron, 2019).

Despite these challenges, generative AI also offers significant social benefits. It can enhance creativity and innovation, providing new tools for artists, designers, and researchers.



In healthcare, generative AI can assist in the development of personalized treatments and improve diagnostic accuracy. In education, AI can provide personalized learning experiences and support for students, helping to bridge gaps in knowledge and skills (Watson et al., 2025; Topol, 2019).

The social impact of generative AI is multifaceted, presenting both opportunities and challenges. Addressing these issues requires a comprehensive approach that includes ensuring equitable access to AI technologies, protecting privacy, and developing robust mechanisms to detect and mitigate misinformation. By doing so, we can harness the potential of generative AI to benefit society while minimizing its risks.

Technical Challenges in Generative AI

Generative artificial intelligence has demonstrated remarkable capabilities in creating content across various domains. However, the deployment and development of generative AI systems come with significant technical challenges that must be addressed to ensure their reliability, transparency, and accountability.

One of the primary technical challenges is ensuring the robustness and integrity of generative AI systems. These systems are often trained on vast datasets, which can introduce vulnerabilities if the data is biased, incomplete, or contains errors. Ensuring that AI models are robust against adversarial attacks and can maintain their performance in diverse and unpredictable environments is crucial (Goodfellow, Shlens, & Szegedy, 2015).

Transparency and explainability are also critical technical challenges. Generative AI models, particularly those based on deep learning, often operate as “black boxes”, making it difficult to understand how they arrive at specific outputs. This lack of transparency can hinder trust and accountability, especially in high-stakes applications such as healthcare and finance. Developing methods to

interpret and explain the decisions made by generative AI systems is essential for building trust and ensuring ethical use (Doshi-Velez & Kim, 2017).

Accountability in AI systems is another significant challenge. As generative AI systems become more autonomous, it becomes increasingly important to establish mechanisms for accountability. This includes tracing the decisions and actions of AI systems back to their developers and operators, ensuring that there are clear lines of responsibility. Implementing robust logging and monitoring systems can help achieve this goal (Marsili, & Wróblewska-Jachna, 2024).

Data privacy and security are also major technical concerns. Generative AI systems often require access to large amounts of data, which can include sensitive and personal information. Ensuring that this data is collected, stored, and used securely is paramount to protecting individuals' privacy. Additionally, there is a risk that generative AI could be used to generate synthetic data that mimics real individuals, further complicating privacy concerns (Zuboff, 2019).

Another technical challenge is the computational resources required to train and deploy generative AI models. These models often require significant computational power and energy, which can be a barrier to their widespread adoption. Developing more efficient algorithms and hardware to reduce the computational burden is an ongoing area of research (Strubell, Ganesh, & McCallum, 2019).

Finally, ensuring the ethical use of generative AI involves developing frameworks and guidelines that address these technical challenges. This includes creating standards for data quality, model transparency, and accountability, as well as implementing robust security measures to protect data privacy. By addressing these technical challenges, we can ensure that generative AI systems are developed and deployed responsibly, maximizing their benefits while minimizing their risks.

Regulatory Frameworks for Generative AI

The rapid advancement of generative artificial intelligence has prompted regulators worldwide to develop frameworks that ensure the technology's responsible use while fostering innovation. The unique nature of generative AI, which includes the ability to create realistic content autonomously, presents distinct regulatory challenges that require comprehensive and adaptive approaches.

One of the primary concerns in regulating generative AI is ensuring transparency and accountability. Regulatory frameworks must mandate that AI systems are designed with mechanisms that allow for the traceability of their outputs. This includes documenting the data sources used for training, the algorithms employed, and the decision-making processes. Such transparency is crucial for building trust and enabling oversight (Goodfellow, Shlens, & Szegedy, 2015; Doshi-Velez & Kim, 2017).

Privacy protection is another critical aspect of generative AI regulation. Given the vast amounts of data required to train these systems, regulatory frameworks must enforce stringent data protection measures. This includes ensuring that data collection, storage, and usage comply with privacy laws and that individuals' rights are safeguarded. The European Union's General Data Protection Regulation (GDPR) serves as a model for such comprehensive data protection standards (Zuboff, 2019; Marsili, & Wróblewska-Jachna, 2024).

Addressing the ethical implications of generative AI, regulatory frameworks must also focus on mitigating biases and preventing misuse. This involves setting guidelines for the ethical development and deployment of AI systems, including regular audits to identify and rectify biases in the data and algorithms. Additionally, regulations should prohibit the use of generative AI for malicious purposes, such as creating deepfakes or automating cyberattacks (Chesney & Citron, 2019; Sengar, Hasan, Kumar, & Carroll, 2024).

International cooperation is essential for effective generative AI regulation. Given the global nature of AI development and deployment, regulatory frameworks must be harmonized across jurisdictions to prevent regulatory arbitrage and ensure consistent standards.

Collaborative efforts, such as the European Union's AI Act and the Biden-Harris Administration's regulatory framework for AI, highlight the importance of international alignment in addressing the challenges posed by generative AI (Biden-Harris Administration, 2025; Kremer et al., 2023).

Furthermore, regulatory frameworks must be adaptive to keep pace with the rapid evolution of generative AI technologies. This requires continuous monitoring and updating of regulations to address emerging risks and opportunities. Establishing regulatory sandboxes, where new AI technologies can be tested in controlled environments, can help regulators understand the implications of these technologies and develop appropriate responses (Watson, Brezovec, & Romic, 2025).

Developing effective regulatory frameworks for generative AI involves ensuring transparency, protecting privacy, mitigating biases, preventing misuse, fostering international cooperation, and maintaining adaptability. By addressing these key areas, regulators can create an environment that promotes the responsible use of generative AI while maximizing its benefits for society.

Case Studies and Practical Applications

Generative artificial intelligence has demonstrated its transformative potential across various industries, providing innovative solutions and enhancing efficiency. This section explores several case studies and practical applications of generative AI, highlighting its diverse capabilities and impact.

Healthcare

In the healthcare sector, generative AI has been instrumental in advancing medical research and improving patient care. For instance, generative AI models have been used to design new drugs by predicting molecular structures that can effectively target specific diseases. This approach has significantly accelerated the drug discovery process, reducing the time and cost associated with traditional methods (Topol, 2019). Additionally, generative AI has been employed to create personalized treatment plans by analyzing patient data and predicting the most effective therapies (Watson, Brezovec, & Romic, 2025). Generative AI also supports the creation of synthetic data for training models, enhancing predictive accuracy and research capabilities (Bhuyan et al., 2025).

Automotive Industry

The automotive industry has also benefited from generative AI, particularly in the design and manufacturing processes. Companies like Ford have utilized generative AI to develop innovative vehicle designs that optimize fuel efficiency, aesthetics, and cost. By automating the design process, generative AI has enabled faster and more cost-effective production of high-performance vehicles (DigitalDefynd, 2025). Toyota has leveraged AI to enhance traffic management and road safety through real-time traffic flow optimization, significantly reducing congestion (Hardy, 2025).

Finance

In the finance sector, generative AI has been applied to enhance fraud detection and risk management. AI models can analyze vast amounts of transaction data to identify unusual patterns and flag potential fraudulent activities. This has improved the accuracy and efficiency of fraud detection systems, helping financial institutions protect their

assets and customers (Brynjolfsson & McAfee, 2014). Furthermore, generative AI has been used to develop predictive models for market trends, enabling more informed investment decisions (Kremer et al., 2023). FinScore Global, for example, implemented generative AI to improve credit risk assessment, resulting in a significant reduction in default rates and increased credit issuance to underserved segments (DigitalDefynd, 2025).

Entertainment and Media

Generative AI has revolutionized the entertainment and media industries by creating new forms of content and enhancing user experiences. For example, AI-generated music and art have opened new avenues for creativity, allowing artists to explore innovative styles and compositions. In the film industry, generative AI has been used to create realistic special effects and generate scripts, streamlining the production process (Chesney & Citron, 2019). Additionally, companies like FOX have utilized AI to generate dynamic recommendations and create sports highlights on the fly, enhancing viewer engagement (Wood, 2024).

Marketing and Customer Engagement

In marketing, generative AI has been employed to create personalized content and improve customer engagement. Retail giants like Walmart have leveraged AI to generate customized product recommendations, promotional emails, and dynamic website content tailored to individual customer preferences. This personalized approach has significantly increased customer engagement and sales, demonstrating the effectiveness of generative AI in enhancing marketing strategies (Marsili, &Wróblewska-Jachna, 2024). Generative AI also automates customer service interactions, providing instant responses and improving overall customer satisfaction (CX Today, 2025).



Education

Generative AI has also made significant contributions to the education sector by providing personalized learning experiences. AI-powered educational platforms can generate customized lesson plans and study materials based on individual student needs and learning styles. This has improved student engagement and learning outcomes, making education more accessible and effective (Watson et al., 2025). Additionally, generative AI tools have been used to create virtual simulations and interactive learning environments, enhancing the educational experience (AIMultiple, 2025).

These case studies illustrate the diverse applications and significant impact of generative AI across various industries. By harnessing the capabilities of generative AI, organizations can drive innovation, improve efficiency, and create new opportunities for growth and development.

Final Considerations

The exploration of generative artificial intelligence in this paper has highlighted its dual nature, presenting both significant opportunities and challenges. By synthesizing the findings from the previous sections, we can better understand the implications for policymakers, technologists, and society, as well as identify future research directions.

Synthesis of Findings

Generative AI has demonstrated its transformative potential across various domains, including healthcare, automotive, finance, entertainment, marketing, and education. The technology's ability to create innovative solutions, enhance efficiency, and provide personalized experiences underscores its value. However, the ethical, social, and technical challenges associated with generative AI cannot be overlooked. Issues such as bias, misinformation, privacy concerns,

and the need for transparency and accountability are critical areas that require attention.

The case studies presented illustrate the diverse applications and significant impact of generative AI. In healthcare, generative AI accelerates drug discovery, personalizes treatment plans, and creates synthetic data for research (Topol, 2019; Bhuyan et al., 2025). In the automotive industry, it optimizes vehicle designs, enhances traffic management, and supports autonomous vehicle development (Sengar et al., 2024; DigitalDefynd, 2025). In finance, it improves fraud detection, enhances risk management, and optimizes investment strategies (Brynjolfsson & McAfee, 2014; Kremer et al., 2023). In entertainment and media, it creates dynamic content, enhances special effects, and generates scripts (Chesney & Citron, 2019; Wood, 2024). In marketing, it personalizes customer engagement, automates content creation, and improves customer service (Marsili, & Wróblewska-Jachna, 2024; Kremer et al., 2023). In education, it provides personalized learning experiences, creates virtual simulations, and generates educational content (Watson et al., 2025).

Implications for Policymakers, Technologists, and Society

For policymakers, the findings emphasize the need for comprehensive regulatory frameworks that ensure the responsible use of generative AI. Regulations must address transparency, accountability, privacy protection, and ethical considerations. International cooperation is essential to harmonize regulations across jurisdictions and prevent regulatory arbitrage. Policymakers must also consider the societal impacts of generative AI, such as job displacement and the digital divide, and implement measures to mitigate these effects.

For technologists, the findings highlight the importance of developing robust, transparent, and accountable AI systems. Addressing technical challenges such as robustness, explainability, and

data privacy is crucial for building trust in generative AI. Technologists must also focus on creating ethical AI systems that minimize biases and prevent misuse. Collaboration with policymakers and other stakeholders is essential to ensure that technological advancements align with societal values and ethical standards.

For society, the findings underscore the need for awareness and education about generative AI. Understanding the benefits and risks associated with the technology is crucial for informed decision-making. Society must also advocate for ethical AI practices and support initiatives that promote equitable access to AI technologies. By fostering a culture of responsibility and ethical awareness, society can help ensure that generative AI is used for the greater good.

Future Research Directions

To address the ethical challenges and prevent misuse of generative AI, and to guide future research, several solutions and key areas for investigation can be implemented:

- **Bias Mitigation:** Use diverse and representative datasets for training, conduct regular audits, and employ fairness-aware algorithms (Buolamwini & Gebru, 2018; Doshi-Velez & Kim, 2017).
- **Misinformation Detection:** Develop advanced detection algorithms, promote digital literacy, and collaborate with media platforms to identify and remove false content (Chesney & Citron, 2019).
- **Privacy Protection:** Implement strong encryption, anonymize data, and adhere to data protection regulations such as the GDPR (Zuboff, 2019).
- **Transparency and Accountability:** Document data sources, algorithms, and decision-making

processes, use explainable AI techniques, and maintain detailed logs of AI system activities (Goodfellow, Shlens, & Szegedy, 2015).

- **Ethical Guidelines and Regulations:** Establish and enforce ethical guidelines and regulations, set standards for ethical AI practices, conduct regular audits, and implement penalties for non-compliance (Biden-Harris Administration, 2025).
- **Public Awareness and Education:** Raise public awareness, educate individuals about the risks and benefits of generative AI, promote digital literacy, and provide resources for identifying AI-generated content (Floridi et al., 2018).
- **Regulatory Frameworks:** Explore and refine regulatory approaches to ensure responsible AI development and deployment (Biden-Harris Administration, 2025).
- **Societal Impact:** Investigate the long-term societal impacts of generative AI, including effects on employment, privacy, and the digital divide (Eubanks, 2018).

By implementing these solutions and focusing on these research areas, we can address the ethical challenges associated with generative AI, ensuring its responsible use and maximizing its benefits while minimizing its risks.

Conclusions and Recommendations

This paper has explored the dual nature of generative artificial intelligence, highlighting its transformative potential across various domains such as healthcare, automotive, finance, entertainment, marketing, and education. Generative AI's ability to create innovative solutions, enhance efficiency, and provide personalized experiences underscores its value. However, the ethical, social, and technical challenges associated with generative AI,



including bias, misinformation, privacy concerns, and the need for transparency and accountability, cannot be overlooked. The case studies presented illustrate both the significant benefits and the potential risks of generative AI applications, particularly when it degenerates into “DeGen AI”.

Generative AI represents a powerful tool that can drive significant advancements and improvements across multiple sectors. Its potential to revolutionize industries and enhance human capabilities is immense. However, this potential comes with substantial ethical, social, and technical challenges that must be addressed to ensure responsible use.

The dual nature of generative AI—its capacity for both innovation and misuse, or “DeGen AI”—requires a balanced approach that maximizes benefits while minimizing risks. This balance can be achieved through comprehensive regulatory frameworks, robust technical solutions, and a strong emphasis on ethical considerations.

To harness the full potential of generative AI while mitigating its risks, stakeholders must take proactive steps:

- **Polymakers:** Develop and implement comprehensive regulatory frameworks that address transparency, accountability, privacy protection, and ethical considerations. International cooperation is essential to harmonize regulations and prevent regulatory arbitrage.
- **Technologists:** Focus on creating robust, transparent, and accountable AI systems. Address technical challenges such as robustness, explainability, and data privacy. Collaborate with policymakers and other stakeholders to ensure that technological advancements align with societal values and ethical standards.

- **Society:** Advocate for ethical AI practices and support initiatives that promote equitable access to AI technologies. Raise awareness and educate individuals about the benefits and risks associated with generative AI to foster informed decision-making.

By working together, policymakers, technologists, and society can ensure that generative AI is developed and deployed responsibly, maximizing its benefits while minimizing its risks, and preventing the degeneration into “DeGen AI”.



About the author:

Marco Marsili is a researcher and scholar with a focus on international relations, human rights, and the implications of emerging technologies on global security. He holds a PhD in History, Security Studies and Defense and has published extensively on topics related to cognitive warfare, cybersecurity, and the intersection of technology and human rights. His work emphasises the need for ethical frameworks in the development of defence capabilities, advocating for a holistic approach that integrates human rights considerations into security strategies.

As a member of NATO's Science and Technology Organization (STO) and a contributor to NATO DIANA and European Defence Agency (EDA) initiatives, he has advanced studies on cybersecurity, cognitive warfare, and human security. His research assignments, including projects for the Portuguese and Italian Ministries of Defence, have explored hybrid warfare, geopolitics, and defense technologies, bridging academic inquiry with policy-making. He has also led research funded by the European Economic Area (EEA) Financial Mechanism and co-chaired ISMS Working Group 1 on War Studies, contributing to key developments in international security. With around 50 academic publications, his work spans hybrid warfare, international law, and cognitive manipulation. Dr. Marsili is affiliated with Cà Foscari University of Venice, Italy, where he integrates the Research Institute for International Studies.

References

- Al-kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., & Alfandi, O. (2024). Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective. *Informatics*, 11(3), 58. <https://doi.org/10.3390/informatics11030058>
- Bhuyan, S. S., Sateesh, V., Mukul, N., Galvankar, A., Mahmood, A., Nauman, M., Rai, A., Bordoloi, K., Basu, U., & Samuel, J. (2025). Generative Artificial Intelligence Use in Healthcare: Opportunities for Clinical Excellence and Administrative Efficiency. *Journal of Medical Systems*, 49(10). <https://doi.org/10.1007/s10916-024-02136-1>
- Biden-Harris Administration. (2025, January 13). *Regulatory Framework for the Responsible Diffusion of Advanced Artificial Intelligence Technology*. U.S. Department of Commerce, Bureau of Industry and Security. Retrieved from <https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion>
- Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W.W. Norton & Company
- Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81, 1-15. Retrieved from <https://proceedings.mlr.press/v81/buolamwini18a.html>
- Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147-155
- DigitalDefynd. (2025). *Top 5 AI Use in Automotive Industry Case Studies*. DigitalDefynd. Retrieved from <https://digitaldefynd.com/IQ/ai-in-automotive-industry-case-studies/>
- Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv*. <https://doi.org/10.48550/arXiv.1702.08608>
- Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press
- Floridi, L., Cowls, J., Beltrametti, M. et al. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
- Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *arXiv*. <https://doi.org/10.48550/arXiv.1412.6572>
- Hagendorff, T. (2024). Mapping the Ethics of Generative AI: A Comprehensive Scoping Review. *Minds and Machines*, 34, 39. <https://doi.org/10.1007/s11023-024-09694-w>
- Hardy, T. (2025, January 21). How Generative AI in Automotive Manufacturing Boosts Quality and Precision?(2025).*GenerativeAIinAutomotiveIndustry: Benefits, Use Cases, & Process*. SparxIT Solutions. Retrieved from <https://www.sparxitsolutions.com/blog/generative-ai-in-automotive-industry/>
- Hinduja, S. (2024). Lessons Learned from Ten Generative AI Misuse Cases. *Cyberbullying Research Center*. Retrieved from <https://cyberbullying.org/generative-ai-misuse-cases>
- Kremer, A., Luget, A., Mikkelsen, D., Soller, H., Strandell-Jansson, M., & Zingg, S. (2023, December 21). *As gen AI advances, regulators—and risk functions—rush to keep pace*. McKinsey & Company. Retrieved from <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/as-gen-ai-advances-regulators-and-risk-functions-rush-to-keep-pace>

- Marchal, N., & Xu, R. (2024, August 2). Mapping the misuse of generative AI. *Google DeepMind*. Retrieved from <https://deepmind.google/discover/blog/mapping-the-misuse-of-generative-ai/>
- Marsili, M., & Wróblewska-Jachna, J. (2024). Digital Revolution and Artificial Intelligence as Challenges for Today. *Media i Społeczeństwo*, 20(1), 19-30. <https://doi.org/10.5604/01.3001.0054.6506>
- Mohamed, E.A.S., Osman, M.E., & Mohamed, B.A. (2024). The Impact of Artificial Intelligence on Social Media Content. *Journal of Social Sciences*, 12(1), 16-30. <https://doi.org/10.3844/jssp.2024.12.16>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation* or *GDPR*). OJ L 119, 4 May 2016, 1–88 (consolidated version). <https://eur-lex.europa.eu/eli/reg/2016/679>
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (*Artificial Intelligence Act*) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*), PE/24/2024/REV/1, OJ L, 2024/1689, 1 July 2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>
- Sengar, S. S., Hasan, A. B., Kumar, S., & Carroll, F. (2024). Generative artificial intelligence: A systematic review and applications. *Multimedia Tools and Applications*. <https://doi.org/10.1007/s11042-024-20016-1>
- Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. *arXiv*. <https://doi.org/10.48550/arXiv.1906.02243>
- Topol, E. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books
- Wei, Y., & Tyson, G. (2024). Understanding the Impact of AI Generated Content on Social Media: The Pixiv Case. *arXiv*. <https://doi.org/10.48550/arXiv.2402.18463>
- Wood, C.X. (2024, August 26). 5 AI Case Studies in Entertainment. VKTR. Retrieved from <https://www.vktr.com/ai-disruption/5-ai-case-studies-in-entertainment/>
- Watson, S., Brezovec, E., & Romic, J. (2025). The role of generative AI in academic and scientific authorship: An autopoietic perspective. *AI & SOCIETY*. <https://doi.org/10.1007/s00146-024-02174-w>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs

Readers' profile

- European-level representatives, sectoral agencies of the European Union, International Organisations Representatives;
- National-level officials of the Euro-Atlantic alliance, Government and Regulatory Affairs Directors & Managers;
- National and Local Government Officials as well as diplomatic representatives;
- Law Enforcement & Intelligence Officers, Military & Defence Ministries Officials;
- Legal Professionals, Representatives for Governance, Audit, Risk, Compliance, Industry leaders and innovators, active investors;
- Opinion leaders, specialised media, academic experts.

Types of contribution:

- Policy review / analysis / opinion – a Partner's article or a series of articles on crucial issues related to cybersecurity;
- Interview with Partner's representative;
- Research outcomes and recommendations;
- Advertisement of a firm, product or an event (graphical);
- Promotional materials regarding a cybersecurity conference / event (invitation, advertisement – graphical).

Do you want to share your opinion on national or European policies regarding cybersecurity? Do you want to publish outcomes of your research? Do you want to advertise?

**The European Cybersecurity Journal
is the right place to do it!**



The Kosciuszko Institute is a leading Polish think tank shaping digital and security policy in Europe. Established in 2000, the Institute is a non-profit, non-governmental organization committed to building a secure and innovative digital future. Its mission is to strengthen the resilience of democratic societies and support evidence-based policymaking in the fields of cybersecurity, international security, critical technologies, and information integrity.

The Institute provides strategic expertise, facilitates multistakeholder dialogue, and builds cross-sector partnerships at national and international levels. It is the organizer of the annual CYBERSEC Forum – one of the key European platforms for strategic discussion on cybersecurity, emerging technologies, and digital sovereignty.

Through its policy papers, expert consultations, and international cooperation projects, the Kosciuszko Institute contributes to safeguarding democratic values and enhancing Europe's technological competitiveness.

We warmly invite you to follow our initiatives and join us in building a more secure and resilient digital world. Collaborations with stakeholders from government, industry, academia, and civil society are at the heart of our mission.



THE KOSCIUSZKO INSTITUTE

is the publisher of

**European
Cybersecurity
Journal**