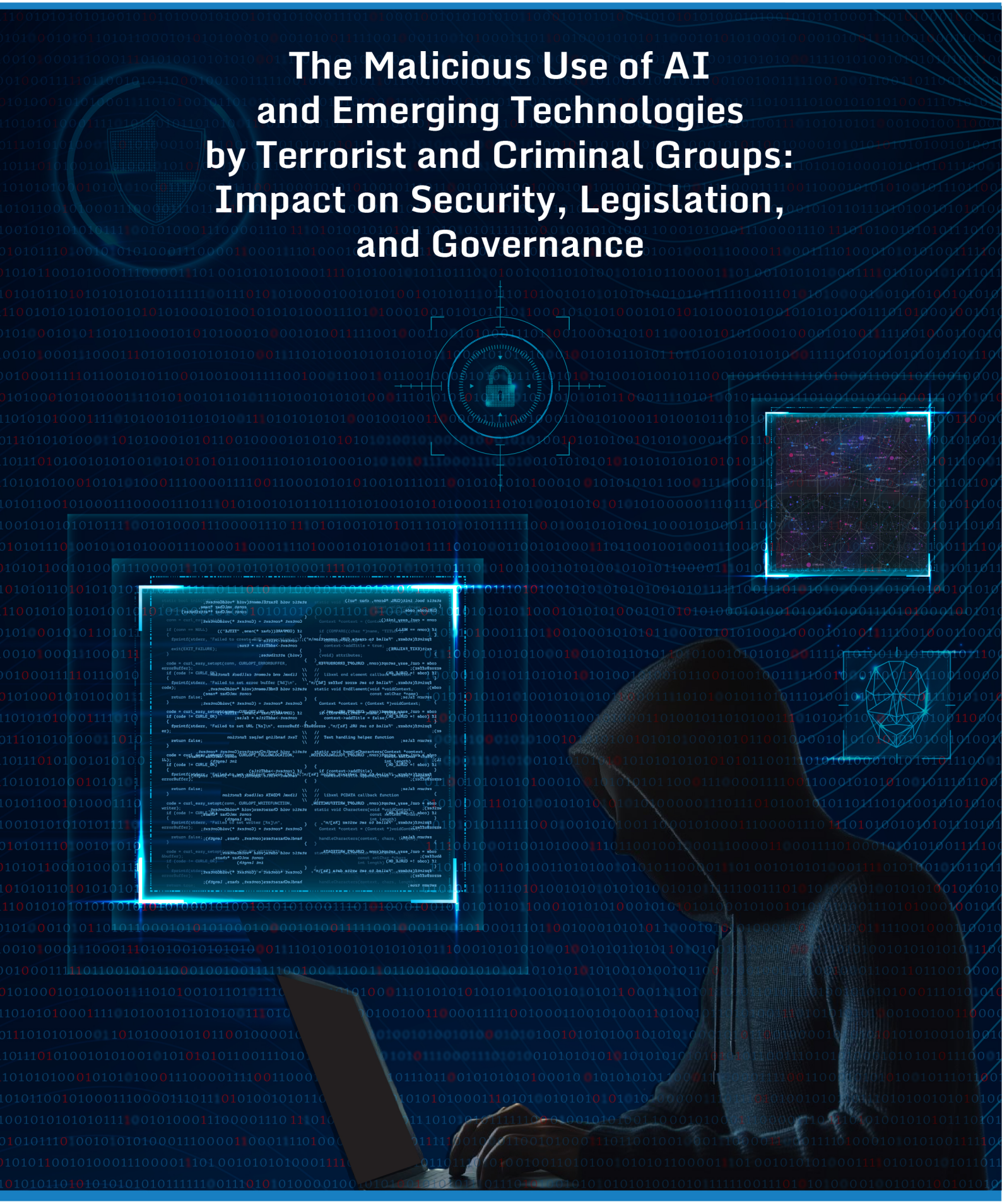
CGS™
CENTRE FOR GLOBAL STUDIES

A Program of Parliamentary Assembly of the Mediterranean

The Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups: Impact on Security, Legislation, and Governance



www.cgspam.org

Report:

The Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups: Impact on Security, Legislation, and Governance

San Marino, 18 November 2024

Disclaimer: This document is prepared by the researchers of the Centre for Global Studies (CGS) of the Parliamentary Assembly of the Mediterranean (PAM) in San Marino in their personal capacity. The opinions expressed in the note are the authors' own and may not reflect the views of PAM.

Executive summary

This document, prepared by the Center for Global Studies (CGS), a special program of the Parliamentary Assembly of the Mediterranean (PAM), attempts to sketch out key elements relative to the malicious use of Artificial Intelligence (AI) and the information ecosystem by transnational terrorists and criminal networks. Moreover, it outlines the growing and persistent inter-relationship between new and emerging technologies and security, stressing that existing regulations are inadequate to address cyberspace security, endangered by technological advancements, such as AI, Quantum Computing, and the dark web. Looking further, brain-computer interfaces and initiatives, such as Neuralink, mark the next frontier in mediating human action and technological capability. The emerging technological revolution has become essential and pervasive in today's development societies, increasingly complex and central to discussions about the future of people and the world. It is, therefore, necessary to consider the Universal Declaration of Human Rights[1], the United Nation's Secretary General's vision for a digital cooperation roadmap for the Millennial Development Goals, and the Common Agenda for the Sustainable Development Goals as the guiding principles in strategizing for the prevention of the humanitarian crises hitherto caused by armed conflicts and for the proper management of new technologies. States must ensure that any measures taken to combat terrorism comply with their obligations under international law, including international human rights law, international humanitarian law, and refugee law, as applicable. This is particularly relevant to the use of new technology in terrorism prevention and law enforcement efforts: unintended consequences and potential human rights implications evolve in tandem with technological adaptations[2]. The emerging technological revolution is part of a geo-strategic change visible from space to the social level: online and offline experiences and lives have become deeply intertwined. This report explores the application of law and jurisprudence worldwide to the malicious use of AI and, therefore, promotes reflections on the challenges and the need to regulate AI from a legal and legislative perspective.

[1] United Nations. (2023). *Universal Declaration of Human Rights | United Nations*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

[2] International Standards on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. (1996). www.ohchr.org. Retrieved October 30, 2024, from https://www.ohchr.org/en/special-procedures/sr-terrorism/international-standards-promotion-and-protection-human-rights-and-fundamental-freedoms-while

Introduction

1. In the rapidly evolving digital and Quantum landscape[3], the relationship between new and emerging technologies and security, particularly cybersecurity, is a top priority on the global agenda. With the increase in societies' dependence on digital and quantum systems comes a corresponding demand for tools of security that aim at preventing and addressing the risks posed by using these technologies for terrorist and criminal activities and illegally gaining access to critical data. In a fluid and constantly evolving environment, security risks and the growing link with the malicious use of AI threaten the political-institutional and economic sustainability of the target countries. In the era of emerging technologies, legislation capable of countering security-threatening terrorist and criminal phenomena is needed. Furthermore, this report identifies pragmatic preliminary guidelines with a global scope due to the complexity of technological tools, considering the balance between great opportunities and sensitive risks. In this framework, it is worth mentioning for its outcomes, the 2023 London Summit on AI Safety (the Bletchley Park summit), which aimed at identifying and analyzing the potentially existential risks posed by AI. Upon concluding the summit, participating countries unanimously agreed on the urgent need to collectively understand and manage the potential risks of AI, calling for a "global effort to ensure its safe and responsible use"[4].

Report

2. This report is drafted by the CGS, a special program of PAM, in cooperation with the UNSC Counter-Terrorism Executive Directorate (CTED). The report focuses on the malicious use of new and emerging technologies by terrorist groups and transnational criminal networks, as well as by non-state actors. The document examines the impact of new and emerging technologies on national and regional security, as well as the consequences on State institutions and procedures, i.e., cyber-attacks, misinformation, disinformation, political violence, a culture of hate, and systemic resilience. The concept of "computer-assisted democracy" (or 'digital democracy') emerges as a crucial bridge between traditional literary culture and emerging digital culture that

[3] Artificial Intelligence in Modern Healthcare," in *Advances in AI Research*, ed. Jane Smith (New York: Springer, 2023), 345-360. Available at: https://link.springer.com/chapter/10.1007/978-3-031-20160-8_27.
[4] Street, P. M. O. 1. D. (2023, November 1). *AI Safety Summit 2023: The Bletchley Declaration*. GOV.UK. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

promises and threatens to usher in an era of 'datacracy'. In 'computer-assisted democracy,' the benefits of data-driven decision-making can be reaped while maintaining human action and democratic principles at the core of governance systems. It also analyses the current state of national and continental security-related regulatory developments and identifies areas of improvement. The report follows the strategic directions based on the resolutions, declarations, and reports issued by the United Nations[5] and its affiliated organizations[6]. It is a "living document" to be continuously monitored and updated.

3. The innovative technology revolution-AI, machine learning, Quantum Computing, synthetic biology, video games, robots, the Dark Web, Web3, and metaverse has become essential and pervasive in contemporary societies, increasingly complex and central to discussions about the security and sustainability of the world and the implementation of the UN Development Goals[7]. It is, therefore, necessary to consider the transformation of the security concept within the framework of the UN Charter and the Universal Declaration of Human Rights. This revolution is part of a geo-strategic change visible from space to the social level. There is no longer any distinction between virtual and physical reality: *"We live in an onlife state."*[8]

4. Significant action on "onlife" security must be relaunched within a new alliance of private and institutional actors (at national, continental, and global levels), involving public opinion and civil society networks. Intelligence activities must consider technological innovation (now part of national security) and work to counter the growing risks posed by the malicious use of these technologies. Within this complex framework of a changing security environment, the opportunities and risks posed by AI and emerging technologies must be carefully and realistically balanced. Intelligence activities need to consider that social cohesion and systemic resilience are

---

[5] See, among others, Resolution 1373. Available at: http://unscr.com/en/resolutions/doc/1373; Resolution 1624. Available at: http://unscr.com/en/resolutions/doc/1624; Resolution 2178. Available at: http://unscr.com/en/resolutions/doc/2178 Resolution 2354. Available at : http://unscr.com/en/resolutions/doc/2354 ; Resolution 2617. Available at: http://unscr.com/en/resolutions/doc/2617; Malicious use of AI. *UNCCT-UNICRI.* Available at: https://unicri.it/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf; Gen-AI: Artificial Intelligence and the Future of work. *International Monetary Fund.* Available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379.

[6] United Nations. (2024). General Assembly Resolution 78/311. Retrieved July 1, 2024, https://documents.un.org/doc/undoc/ltd/n24/183/80/pdf/n2418380.pdf?token=7E224SqoH8rf69mdZW&fe=true

[7] "The transformative role of robotics in achieving Sustainable Development Goals," IFR International Federation of Robotics, last modified January 24, 2024. Available at: https://ifr.org/post/the-transformative-role-of-robotics-in-achieving-sustainable-development-goals.

[8] "Onlife" is a term coined by Italian Professor Luciano Floridi to express the lived experience of the ever-increasing pervasiveness of information and communication technologies. For more, see Floridi, L. (2005). *The Onlife Manifesto. Being Human in a Hyperconnected Era*. Springer Open: London.

part of ensuring security: respect for the privacy of individuals and human communities, protection of civil and social rights, protection of minorities, and sharing and revitalizing the UN Sustainable Development Goals.

5. The emerging technology revolution is unfolding within a growing polarized global system characterized by profound inequalities[9] in almost all areas, with implications for the future of labor markets. Fragile societies constitute fertile ground for implementing malicious activities. Therefore, principles and criteria on AI and emerging technologies can contribute to defining a framework for action for parliamentarians that is as widely shared as possible. In this regard, this report considers that it is essential to:
   - **Strategic Recommendations**
     - Identify legislative gaps in preventing and combating malicious activities by terrorist and criminal networks and non-state actors and propose realistic implementation steps.
     - Strengthen transnational cooperation on cyber security challenges between governments, parliaments, intelligence, law enforcement agencies, corporate Chief Information Security Officers (CISOs), think tanks, and universities.
     - Promote responsible design and development of large language models (LLM) and large multimodal models (LMM)[10], ensuring they prioritize security by design and prevent data bias from specific social groups. This includes addressing positive bias (better results for certain languages) and negative bias (prediction of crime in vulnerable communities), focusing on areas such as public health[11], legal[12], education[13], and digital media[14].

[9] Rebecca Riddell, "Inequality Inc.", Oxfam International, last modified January 15, 2024. Available at: https://www.oxfam.org/en/research/inequality-inc.
[10] House of Lords, *Large Language Models and Generative AI* (London: Authority of the House of Lords, 2024). Available at: https://publications.parliament.uk/pa/ld5804/ldselect/ldcomm/54/54.pdf.
[11] World Health Organization, "Who releases AI ethics and governance guidance for large multi-modal models?" *World Health Organization*, January 18, 2024. Available at: https://www.who.int/news/item/18-01-2024-who-releases-ai-ethics-and-governance-guidance-for-large-multi-modal-models.
[12] Dahl, M. et. al. (2024). Hallucinating law: Legal mistakes with large language models are pervasive. *Stanford HAI*. Available at: https://hai.stanford.edu/news/hallucinating-law-legal-mistakes-large-language-models-are-pervasive.
[13] Seita, D., and Vivek Verma, E.F. (2024). Ghostbuster: Detecting text ghostwritten by large language models. *The Berkeley Artificial Intelligence Research Blog*. Available at: https://bair.berkeley.edu/blog/2023/11/14/ghostbuster/.
[14] Gormely, I. (2023). Neutralizing bias in AI: Vector Institute's Unbias Framework Revolutionizes Ethical Text Analysis. *Vector Institute for Artificial Intelligence*. Available at: https://vectorinstitute.ai/neutralizing-bias-in-ai-vector-institutes-unbias-framework-revolutionizes-ethical-text-analysis/.

- Integrate risks related to the malicious use of AI and emerging technologies[15], cyber-attacks, and defense into national security strategies[16].
- Develop innovative industrial strategies to bridge the gap between strategic goals and technological resources.

- **Technical Recommendations**
  - Provide appropriate training for digital forensic specialists and justice system personnel about using the metaverse and related technologies to ensure the virtual environment's safety and security and protect the individual's rights.
  - Rethink trust and security-by-design approach to prevent cyber-attacks on public structures.
  - Improve coordination of national regulations for the dangers of crowdfunding activities.
- **Policy-Related Recommendations**
  - Support the international community in developing principles, guidelines, and regulations for social media and AI companies to address online racism and political violence, encouraging voluntary compliance and best practices.
  - Rethink public policies, particularly at the intersection of intellectual property, data governance, AI, and the platforms' underlying business model.
  - Promote a culture of systemic risk during the "onlife" condition. This can be achieved through the implementation of exercises and comprehensive programs for employees' cybersecurity training across various domains. This includes news and research on emerging threats and strategies for effective risk management. Enhanced awareness and preparedness enable organizations to assess potential cyberspace threats more effectively, thereby lowering overall systemic risk.
  - Ensure, as outlined by UN Women, equitable development of AI in favor of women to overcome 'gender bias'[17]. This has inevitable repercussions for policies to address

[15] Bill Drexel and Caleb Withers, "Catalyzing Crisis**.** A Primer on Artificial Intelligence, Catastrophes, and National Security.". *Center for a New American Security*. Available at: https://www.cnas.org/publications/reports/catalyzing-crisis
[16] Pierluigi Paganini, "Nation-state actors are using AI services and LLMS for cyberattacks," *Security Affairs*, February 15, 2024. Available at: https://securityaffairs.com/159147/apt/nation-state-actors-openai-ai-services-llms-cyberattacks.html.
[17] Artificial Intelligence and gender equality | UN Women – Headquarters. (2024, May 22). UN Women – Headquarters. https://www.unwomen.org/en/news-stories/explainer/2024/05/artificial-intelligence-and-gender-equality

malicious use by terrorist organizations and, more generally, to improve counter-terrorism strategies[18].

- Invest in the culture of systemic prevention of emerging risks, sustainability, and democratic resilience.

Geopolitics of (in)security

6. In recent decades, the world has seen a significant increase in crises, including armed conflicts and humanitarian disasters. These crises pose risks to human life and undermine the planet's systemic sustainability. According to the Global Risks Report[19] 2024 by the World Economic Forum, misinformation and disinformation are major short-term global risks, while climate events and critical changes to Earth's systems are the primary long-term concerns. These crises are interconnected across five strategic domains: space, cyber, air, land, and sea (especially the underwater dimension). Terrorists and criminal groups exploit these crises, taking advantage of social weaknesses, through propaganda actions, to radicalize the weakest and most deprived elements in human communities, and to carry out malicious actions that constitute a threat to the resilience of countries.

7. The ongoing technological revolution brings great opportunities to address crises but also introduces significant risks. Geopolitical tensions threaten to undermine globalization and divide the world economy into blocs. Rapid digitalization, driven by advanced technologies such as generative Artificial Intelligence, continues apace. Among several research and analyses, David Wells' work highlights the potential misuse of generative AI by terrorists and violent extremists, emphasizing the need for coordinated responses to these emerging threats[20].

---

[18] Integrating gender into counter-terrorism | Security Council - Counter-Terrorism Committee (CTC). (n.d.-b). https://www.un.org/securitycouncil/ctc/content/integrating-gender-counter-terrorism#:~:text=Including%20a%20gender%20perspective%20in%20countering%20terrorism%20and,of%20counter-terrorism%20strategies%20on%20women%20and%20women%E2%80%99s%20rights. United Nations Office for Counter-Terrorism (UNOCT) & Shura Council of the State of Qatar. (2024, June 26-27). Global Conference of Women Parliamentarians. Press release. Retrieved July 23, 2024, from https://pam.int/en/press-releases/pam-contributes-un-global-conference-women-parliamentarians-doha

[19] *Global Risks Report 2024 | World Economic Forum*. (2024, September 10). World Economic Forum. https://www.weforum.org/publications/global-risks-report-2024/

[20] Wells, D. & Middle East Institute. (2024). THE NEXT PARADIGM-SHATTERING THREAT? RIGHT-SIZING THE POTENTIAL IMPACTS OF GENERATIVE AI ON TERRORISM. In Middle East Institute. https://www.mei.edu/sites/default/files/2024-03/Wells%20-%20The%20Next%20Paradigm-Shattering%20Threat%20Right-Sizing%20the%20Potential%20Impacts%20of%20Generative%20AI%20on%20Terrorism.pdfSizing%20the%20Potential%20Impacts%20of%20Generative%20AI%20on%20Te

8. Cyberattacks are mission-critical in hybrid and asymmetric conflicts[21]. These attacks seamlessly merge military and non-military tactics and have multifaceted objectives: to interfere with critical facilities, manage data, and accomplish tactical objectives.

9. The rapid development of AI technology gives rise to several security threats, which both state and non-state actors can exploit to misuse AI and create biological weapons. However, in a recent study conducted by the RAND Corporation[22], the scientists explored the threats associated with the misuse of AI-defined large language models (LLMs) concerning biological threats. The concern arises because AI technologies, in general, and LLMs in particular, are quickly available for any state or non-state actor. However, the study indicated that employing existing LLMs did not significantly alter the operational risk of biological attack. The outputs from LLMs exhibited redundancy with the content available on the Internet, implying that LLMs do not significantly enhance the danger associated with biological weapon attack planning. Although this area remains under threat, the current generation of LLMs does not present a significant threat[23].

10. The state and non-state actors seize the opportunities provided by the gaps in the geopolitics of (in)security. Today's international system is defined by high levels of state anarchy and the possibility of incorporating new technologies into the nuclear decision-making process. Hyuk Kim (2024)[24], in a study for the James Martin Center for Non-proliferation Studies, finds that North Korea is adopting AI and machine learning technologies in multiple spheres, notwithstanding the isolation arising from the sanctions. Furthermore, the United Nations[25] is examining cyberattacks coordinated by Pyongyang on cryptocurrency firms; such attacks may have replenished North Korea's nuclear activities with as much as $3 billion. AI technologies are

---

[21] Lior Tabansky, "Offensive cyber operations as a tool of war," *The Jerusalem Strategic Tribune*, January 2024. Available at: https://jstribune.com/tabansky-offensive-cyber-operations-as-a-tool-of-war/.
[22] Mouton, Christopher A., Caleb Lucas, and Ella Guest, The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study. Santa Monica, CA: RAND Corporation, 2024. Available at: https://www.rand.org/pubs/research_reports/RRA2977-2.html.
[23] Christofer A. Mouton, "Current Artificial Intelligence Does Not Meaningfully Increase Risk of a Biological Weapons Attack", *RAND*, January 25, 2024. Available at: Current Artificial Intelligence Does Not Meaningfully Increase Risk of a Biological Weapons Attack | The RAND.
[24] Kim Hyuk, "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications," , *James Martin Center for Nonproliferation Studies*, January 23, 2024. Available at: https://nonproliferation.org/north-koreas-artificial-intelligence- research-trends-and-potential-civilian-and-military-applications/.
[25] The investigation concerns the circumvention of sanctions imposed by North Korea. For more, see: Dark Reading Staff, "United Nations digging into DPRK crypto cyberattacks totaling $3B", *Dark Reading*, February 12, 2024. Available at: https://www.darkreading.com/cyberattacks-data-breaches/un-digging-into-dprk-crypto-cyberattacks-totaling-3b.

also being leveraged by non-state actors, including terrorist organizations and criminal networks. As an example, the Islamic State Khorasan (ISIS-K), an affiliate of the Islamic State, based in Afghanistan, has intensified its use of AI for recruitment purposes. The Group has used AI to develop more sophisticated, and therefore more targeted propaganda to be used in their recruitment campaigns. The Islamic State itself released in 2023 a guide on how to use generative AI effectively, and by 2024 they were openly expressing interest in continuing to utilize AI to scale and widen the reach of their public content[26]. To increase support and recruitment in several Muslim diaspora communities in Europe and the United States, the ISIS-K has disseminated videos and articles in more than a dozen languages, including Dari and Pashto (the two main languages spoken in Afghanistan). Mr. Lucas Webber, senior threat intelligence analyst at the non-governmental organisation Tech Against Terrorism, said that ISIS-K initially focused on Tajik immigrants in the West, but has now expanded its efforts (through artificial intelligence, social networks, TikTok and the dark web) to other ethnic communities experiencing isolation and alienation.[27] Synthetic data is also a sphere where the threat of non-state terrorist actors exploiting the disinformation technology data to manipulate the information environment. Deepfake technology can be created using synthetic data, which is artificial data created by statistics, computer simulations, or other methods based upon real-life situations. When deepfakes are allowed to spread during conflict, wars, or geopolitical crises, they can spread misinformation and disinformation and increase uncertainty and chaos. Via social media and the like the large-scale dissemination of deepfakes can lead the most vulnerable to radicalism, defaming opponents, and spreading ad hoc narratives[28].

11. The growing use of AI and machine learning technologies by state and non-state actors, including terrorist organizations represents the evolving nature of security threats in the contemporary world. As these actors utilize the latest technologies to expand their capabilities, it is crucial to consider the broader implications for national security. This includes not only the immediate threats posed by cyberattacks and misinformation but also the long-term strategic importance of brain capital. In this context, optimizing national security requires integrating technological advancements with the development of human cognitive and neurological abilities. Focusing on

[26] Tejeda, G. (2024, October 2). *Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts*. The Soufan Center. https://thesoufancenter.org/intelbrief-2024-october-3/
[27] ISIS-K threat grows as it targets disaffected Muslims with sophisticated propaganda, NBC News, October 20, 024. Available at: https://www.nbcnews.com/news/world/isis-k-threat-grows-targets-disaffected-muslims-sophisticated-propagan-rcna175646
[28] CTC Sentinel, January 2024," Combating Terrorism Center at West Point, available at: https://ctc.westpoint.edu/wp-content/uploads/2024/01/CTC-SENTINEL-012024.pdf.

brain capital is essential for better preparing for and mitigating the complex and interdependent risks arising from rapidly changing technological environments.

12. A report produced by the Euro-Mediterranean Association of Economists (EMEA)[29] analyses the potential of neurological weapons. As for connections with brain security and health, neural enhancement using brain-computer interfaces and other developments of the research program relate to national security.

Risks of Emerging Technologies: Terroristic and Criminal Network Activities

13. In the introduction to the European Union Terrorism Situation and Trend Report of Europol published in 2023 (TE-SAT)[30], Executive Director Catherine De Bolle writes: "Terrorism remains a significant threat to the internal security of the European Union. Terrorists operate across borders, leveraging new technologies to target innocent people."

14. Among the key findings of the report is that the Internet and technological developments remain critical enablers of propaganda, radicalization, and recruitment of vulnerable individuals to terrorism and violent extremism. In addition to social media platforms, open messaging applications, online forums, video game platforms, and decentralized platforms appear to have gained popularity in terrorist and violent extremist circles, significantly undermining law enforcement monitoring and investigation. Mr. Brett M. Holmgren (Acting Director of the US National Counterterrorism Center), speaking at the Cipher Brief Threat Conference on 6 October 2024[31], pointed out that since Hamas's terror attack in Israel on 7 October 2023, there have been at least 19 attacks and 21 disrupted plots in more than 20 countries, as well as a considerable increase in attacks in Europe and the Five Eyes countries (Australia, Canada, New Zealand, the United Kingdom, and the United States), with the number of attacks rising from only five in the 12 months before 7 October 2023 to 21 attacks in the year following that date. In addition to Al-Qaeda, ISIS, Hizballah, and other groups, defined as malicious actors, also include racially and

[29] Harris Eyre et al., "From neuroweapons to 'Neuroshields': Safeguarding brain capital for national security," *Euro-Mediterranean Economists Association*, August 14, 2023. Available at: https://euromed-economists.org/download/from-neuroweapons-to-neuroshields-safeguarding-brain-capital-for-national-security/

[30] European Union Terrorism Situation and Trend Report 2023. *Europol*. Available at: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat.

[31] *Remarks by Acting Director of the National Counterterrorism Center at Cipher Brief Threat Conference*. (2024, October 6). www.dni.gov. Retrieved November 1, 2024, from https://www.dni.gov/index.php/nctc-newsroom/nctc-speeches-testimonies-and-interviews/4003-ad-nctc-remarks-cipher-brief-threat-conf-20241006

ethnically motivated transnational violent extremists and anti-government, anti-authoritarian, home-grown violent extremist groups. These new terrorist dynamics involve technological advances: terrorists use more secure communication platforms, cryptocurrencies, alternative payment channels, and emerging technologies (3D printing[32] and artificial intelligence). In response to MI5 Director Ken McCallum's speech (8 October 2024) on the threats brought to national security in the UK[33], Tech Against Terrorism Director Adam Hadley CBE said: "We are witnessing an alarming surge in terrorist content and disinformation online, and it's disheartening to see that many platforms seem indifferent to this growing crisis". "Our open society is uniquely vulnerable to manipulation by nation-states and terrorists. Information warfare is just as important as traditional military warfare; in that sense, we are already losing the battle. The recent warnings from MI5 highlight the urgency of this issue. We need renewed political focus to address these threats. Military leaders must recognize the importance of the digital front, the police need more resources to tackle online crimes, and regulators need stronger powers to hold tech platforms to account. At the same time, we should acknowledge and applaud those platforms that are diligently working to combat this threat. It's time for a collective effort to address this escalating problem before it's too late[34]."

15. Terrorist organizations employ AI in several activities, such as recruitment, propaganda, planning/contemplating an attack, financing, communication, procurement of weapons/material, and attack execution. One ability is predicting large volumes of data while recognizing unique patterns that will help improve decision-making. For instance, AI can be used to detect candidates who can easily be influenced to become radical. It can also write and post propaganda material and do it under the parameters of the intended group or audience. Nonetheless, the extent to which terrorist organizations have taken to leveraging AI remains a topic of contention, and policing continues to progress in addressing this relatively discreet form of threat[35].

---

[32] Veilleux-Lepage, Y. (2024, November 6). *Blocking the blueprint: Technological barriers against 3D-Printed firearms*. GNET. https://gnet-research.org/2024/11/06/blocking-the-blueprint-technological-barriers-against-3d-printed-firearms/

[33] *Director General Ken McCallum gives latest threat update*. (2024, October 8). www.mi5.gov.uk. https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update

[34] Terrorism, T. A. (2024, October 8). *Tech Against Terrorism Highlights ISKP's Escalating Online Threat in Response to MI5 Director General's Warning*. https://techagainstterrorism.org/news/tech-against-terrorism-highlights-iskps-escalating-online-threat-in-response-to-mi5-director-generals-warning

[35] Seth Harrison, "Evolving Tech, Evolving Terror," , *Center for Strategic & International Studies*, March 22, 2018. Available at: Evolving Tech, Evolving Terror (csis.org)

16. In 2021, Tech Against Terrorism found approximately 300 active terrorist and violent extremist websites[36]. These places are used in recruitment, indoctrination, communication, and propaganda spreading. The main problem is to be able to counter such websites and censor them without violating the rights to free speech and privacy. While there is ongoing cooperation between governments, the tech industry, and CSOs regarding these issues, there is still a need for more structured and enforceable guidelines. This includes the introduction of a set of rules that encourage social media and AI companies to proactively tackle online racism and political violence[37].

17. The so-called black web, or dark net, now part of the World Wide Web (WWW), contains many activities that are considered organized or serious crimes. These include fencing markets, drug hubs, cybercrime, and ransomware activities. While not all activities on the dark web are directly related to terrorism, there are connections. For instance, ransomware groups use the dark web for negotiating and providing payment channels[38]. Knowledge of this ecosystem aids the police in tracking some unlawful formations and containing their activities[39].

18. Terrorist organizations can use AI algorithms to gain strategic intelligence by analyzing large amounts of data. One ability is predicting large volumes of data while recognizing unique patterns that will help improve decision-making. For instance, AI can be used to detect candidates who can easily be influenced to become radical. It can also write and post propaganda material and do it under the parameters of the intended group or audience. Nonetheless, the extent to which terrorist organizations have taken to leveraging AI remains a topic of contention, and policing continues to progress in addressing this relatively discreet form of threat.

19. False-flag operations[40] exacerbate tensions and conflicts in community operations, which are deliberate acts of sabotage where the party bearing the blame shifts the responsibility to another,

---

[36] "Explainer: Terrorist operated website: Tech Against Terrorism (no date) Explainer: Terrorist Operated Website", *Tech Against Terrorism*. Available at: https://techagainstterrorism.org/terrorist-operated-websites.
[37] Seth G. Jones, "The Evolution of Domestic Terrorism," *Center for Strategic and International Studies*, February 17, 2022. Available at: The Evolution of Domestic Terrorism (csis.org).
[38] In 2022, around 386 monthly blog posts were published on public platforms on the dark web; in 2023, the number rose to 476, with a peak in November of 634 posts. For more, see: Sergey Lozhkin et al., "Dark web threats and dark market predictions," *Secure List*, January 17, 2024. Available at: https://securelist.com/darknet-predictions-for-2024/111763/.
[39] Sarah Bast, "Counterterrorism in an Era of More Limited Resources," *Center for Strategic and International Studies*, May 18, 2018. Available at: Counterterrorism in an Era of More Limited Resources (csis.org).
[40] "False flags: What are they and when have they been used?" *BBC*, February 18, 2022. Available at: False flags: What are they and when have they been used? (bbc.com).

hence the tradition dating from the sixteenth century. Modern usage involves planned attacks that can justify a counterattack on the alleged perpetrator; sometimes, they can be seen as propaganda or misinformation with the intention of war or otherwise. Radicalization is achieved through the use of artificial intelligence-based chatbots by terrorist organizations. In an article published in February 2023, The Nation covered the possibility of false flag operations between India and Pakistan in 2023, as well as the consequent accusations. Islamabad accused Delhi of conducting the operation in the IIOJ&K region in January 2023. Other cases allegedly occurred: the first one was in April 2023, a few days before the G20, when the Indian Presidency was the second one, in May 2023, held in Poonch district; the third one will be in September, in Islamabad district; and the last one will be in October, in Neelam. Pakistan attacked the Indian troops in the Poonch district in 2023, despite the territory being 15-20 kilometers away from the Line of Control[41].

20. The Financial Action Task Force FATF; released the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation report in 2023[42] and presented a clear and structured set of measures that countries need to take when it comes to combating money laundering, financing of terrorism, and proliferation of weapons of mass destruction against the background of inequality and differences in the legal, administrative, and financial frameworks of countries. Some of the concerns mentioned by the FATF in the Report on "Crowdfunding for Terrorism Financing,"[43] which looks at the internet and social networking sites concerning the malicious use of crowdfunding, include the complexity of crowdfunding operations, and anonymization techniques. Another factor that the FATF acknowledges is that in the crowdfunding space, there is no training and experience in identifying terrorist financing. The effects of ICT, like the negative implications of crowdfunding, have become an important field of study in the fight against terrorism financing[44].

21. Extremists use social media for fundraising activities, reaching out to their target audience, and sharing messages, among other things. Moving on to crowdfunding and its integration with

---

[41] Shaukat, R. (2024) India's false flag operations, The Nation. Available at:https://www.nation.com.pk/27-Feb-2024/india-s-false-flag-operations

[42] "Forty recommendations," *Financial Action Task Force*, 2023. Available at: FATF Recommendations 2012.pdf.coredownload.inline.pdf (fatf-gafi.org).

[43] "Report crowdfunding for terrorist financing," *Financial Action Task Force,* 2023. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

[44] "Crowdfunding for Terrorism Financing and Illicit Financial Flows from Cyber-enabled Fraud," *International Association of Lawyers*, December 14, 2023. Crowdfunding for Terrorism Financing and Illicit Financial Flows from Cyber-enabled Fraud | UIA (uianet.org).

different aspects of virtual assets, such as cryptocurrencies, raises further questions. A thorough risk evaluation matrix, organizational mobilization, and adequate exposure to knowledge are apt risk markers. Some of the ways ICT platforms support counterterrorism financing measures are through cooperation, information dissemination, and regulation[45]. The USA Department of Justice authorities have frozen terrorist-funded cryptocurrency accounts in the USA, primarily linked to al-Qassam Brigades, Al-Qaeda, and affiliated groups in Syria, as well as ISIL[46]. These have also included police arrests of suspicious accounts associated with web hosting services, donors, and funding. There has been increased use of the Internet in fundraising, as well as increased adoption of PayPal, GoFundMe, and Amazon by violence-prone individuals[47]. While continued efforts are aimed at reducing terrorism financing on social media networks and video-sharing platforms[48]. The first anti-terrorist financing system uses technology to gather and monitor data about terrorism financing. Understanding the risks posed by emerging technologies requires examining how these technologies are leveraged in the digital underworld. The following section delves into the rise of cybercrime and its implications for terrorism and organized crime.

Navigating the Digital Underworld: Cybercrime

22. There is an increase in the rate of cybercrime, and thus this has made this possibility even bigger. In the 2023 Internet Organized Crime Threat Assessment (IOCTA) Report of Europol[49], it is reported that the crime spectrum includes all individuals within the European Union and negatively impacts both the public and private sectors. The impacts include financial losses, emotional distress, and physical harm. The wide variety of cybercrimes, online child sexual exploitation, and digital fraud demonstrates their highly multifaceted nature. In the cyber age, criminals are clever and able to adapt quickly to exploit new vulnerabilities, making it difficult for law enforcement to keep up.

---

[45] "Crowdfunding for Terrorism Financing," Financial *Action Task Force*, October 31, 2023. Available at: Crowdfunding for Terrorism Financing (fatf-gafi.org).
[46] Sam Dorshimer, "The New Era in Cyber-Enabled Terrorist Financing," *Center for a New American Security*, September 29, 2020. Available at: The New Era in Cyber-Enabled Terrorist Financing | Center for a New American Security (en-US) (cnas.org).
[47] "Terrorism and Digital Financing: How Technology is Changing the Threat," Committee on Homeland Security, July 22, 2021. Available at: CHRG-117hhrg45867.pdf (congress.gov).
[48] UN News, "UN counter-terrorism body backs innovations to fight digital terror," *United Nations News*, October 27, 2022. Available at: UN counter-terrorism body backs innovations to fight digital terror | UN News.
[49] "Internet organized crime threat assessment Europol (IOCTA)", *Interpol*, 2023. Available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report.

23. During the International Conference[50] on Cyber Security hosted by Fordham Law School in New York between 8 and 10 January 2024, the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) raised an alert on the malicious use of AI to widen the spectrum of action in cyber and financial crime. This new trend adds to cyber threats since the attackers can maintain operational momentum, avoid straightforward identification, and, essentially, flip strategies as often as needed. The use of AI technologies creates threats to essential infrastructure more than ever when implemented in the finance industry and requires proper protection in addition to efforts provided by law enforcement departments and related companies.

24. By weakening social trust, cyber-attacks affect critical infrastructure in all sectors and endanger country systems' security and resilience[51]. The space industry, along with other sectors such as agribusiness, military, health, and transportation, is also vulnerable to cyber threats[52], which could affect every aspect of life. These risks range from land to sea, where state and corporate control are intertwined in some sort of a matrix, making it questionable how secure digital sovereignty is. Lack of adequate enforcement policies and, more generally, inadequate advancements in cable technologies make it quite difficult to safeguard underwater cables. Telecommunication and ICT infrastructure are similarly critical in the United Kingdom[53], where they are the backbone of various other infrastructures. Weather-related events like floods and auroras can also cause havoc to the overall systems, power outages, and unfavorable operating conditions, disrupting favorable social and physical ICT and telecoms. The direct threat of weather-related outages is not very high today; however, estimates concerning future climatic disruptions are still ambiguous. Indirect flooding can impact telecom and ICT networks, albeit less frequently than energy facilities and assets. There are risks for high temperatures and problems for underground cables, including damage from subsidence, which could potentially increase in the future.

25. Cyber-threats should be countered to maintain the efficiency and competitiveness of public services. Hence, integrating cyberattack and defense strategies into national security is

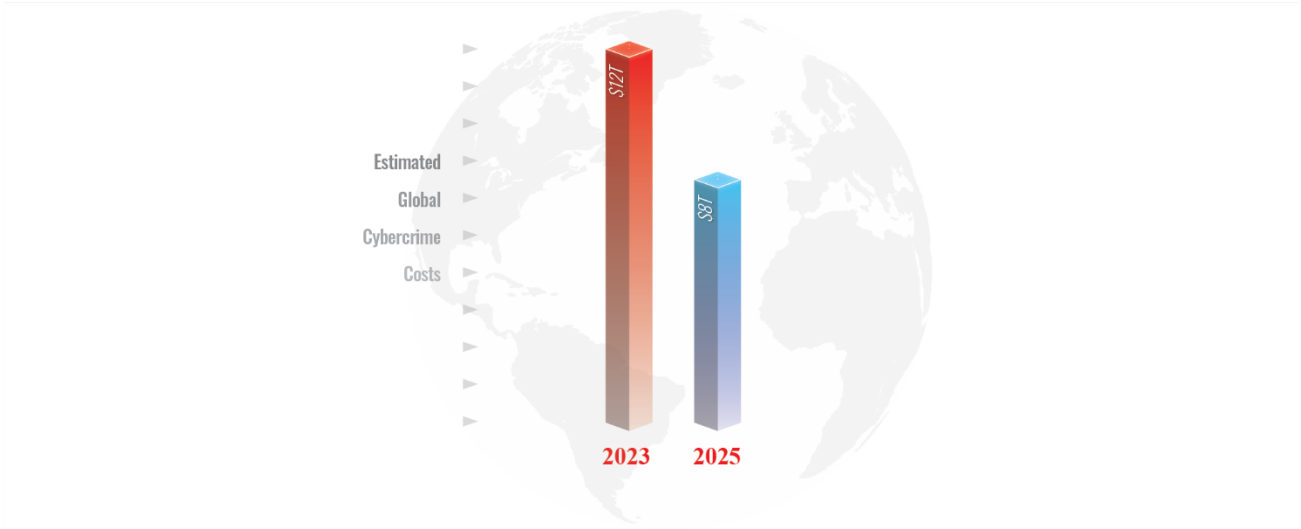
---

[50] "International Conference on Cyber Security," *Fordham Newsroom*, January 8, 2024. Available at: https://news.fordham.edu/event/2024-international-conference-on-cyber-security/.
[51] Adejumo Quadri, "The Rising Threat of AI-Enabled Cybercrimes: A Warning from the NSA and FBI," Computer *Crime Research Center*, January 10, 2024. Available at: https://www.crime-research.org/news/10.01.2024/4131/.
[52] "Space: The Final Frontier for Cyberattacks", *Dark Reading*. Available at: https://www.darkreading.com/cyber-risk/space-final-frontier-cyberattacks
[53] "United Kingdom Telecom ICT Infrastructure Market By Size, Share, Trends, Growth, Forecast 2027," *TechSci Research*. Available at: United Kingdom Telecom ICT Infrastructure Market By Size, Share, Trends, Growth, Forecast 2027 | TechSci Research.

mandatory[54]. Cybersecurity Ventures estimates that global crime costs will reach $8 trillion in 2023. According to IBM, the average data breach cost in 2023 was $4.45 million, an increase of 15% over the past three years[55]. The Computer Crime Research Center (CCRC)[56] reports that the cost of cybercrime will reach a global level of $12 trillion by 2025. In the Middle East, Türkiye, and Africa, cybersecurity spending will reach $6.5 billion by 2024. According to Deloitte[57], the lack of funding for cybersecurity remains the number one challenge for 51% of companies[58] in the Middle East, compared to 36% globally. It was noted that the US Cybersecurity and Infrastructure Security Agency (CISA)[59] triggered a pre-ransomware notice program, which generated over 1,200 alerts in the given year of 2023. Realizing the weakness of computer-based cybersecurity, the US Advanced Research Projects Activity introduced the Cyberpsychology-Informed Network Defense to safeguard against cyber threats. It was stated in February 2024 with Reimagining Security that the Cyberpsychology-Informed Network Defenses[60] initiative will attempt to make the attackers' job difficult.

[54] Emily Harding, "The United States needs a new way to think about cyber default," Lawfare, January 28, 2024. Available at: https://www.lawfaremedia.org/article/the-united-states-needs-a-new-way-to-think-about-cyber.
[55] Alex Leadbeater, "AI and 5G are defining a new era of cybersecurity," Infosecurity *Magazine*, January 31, 2024. Available at: https://www.infosecurity-magazine.com/blogs/ai-5g-new-era-of-cybersecurity/.
[56] Damien Black, "Cybercrime will cost $12 trillion next year, say experts." *Cyber news*, January 24, 2024. Available at: https://cybernews.com/news/cybercrime-will-cost-trillions-next-year/.
[57] Tariq M. Ajmal, "Our Cyber Offerings," Deloitte. Available at: https://www2.deloitte.com/xe/en/pages/risk/solutions/cyber-portfolio.html.
[58] Robert Lemos, "Middle East & Africa crisis plan to increase 2024 budgets by 10%," Dark *Reading*, February 13, 2024. Available at: https://www.darkreading.com/cybersecurity-operations/middle-east-africa-cisos-plan-to-increase-2024-budgets-by-ten-percent.
[59] For more, see: https://www.cisa.gov/.
[60] Di Molfetta, D. (2024). IARPA makes awards in 4-year effort studying Hacker Psychology. *Nextgov.com*. Available at: https://www.nextgov.com/cybersecurity/2024/02/iarpa-makes-awards-4-year-research-effort-studying-hacker- psychology/394097/

Figure 1: Estimated Global Cybercrime Costs (Values in Trillions of Dollars)[61]



26. A report from the European Commission and ENISA[62], the EU Agency for Cybersecurity, indicated that there is a need for more oversight of cybersecurity and resilience in Europe's telecommunication infrastructures and networks. The threats include wipers; ransomware attacks; pirates; supply chain attacks; physical attacks; and sabotage, as highlighted in the risk assessment matrix. These are opportunistic threats and are deemed a major security threat to the connectivity infrastructure. These issues are accompanied by a list of strategic and technical steps proposed in the report. For example, the interconnection of Britain to the global Internet should be checked for its stability, and the HIIs, including the electronic communications sector, should be evaluated for cooperative cyber exercises, as well as performing physical stress tests on other appropriate digital constructions.

27. The Pall Mall Process[63] agreement was signed in London on 6 February 2024. Dozens of countries have joined forces with Big Tech in the fight against spyware and human rights abuses in cyberspace. Signatories include the United States, the United Kingdom, France, and 22 other nations; the Gulf Cooperation Council; the African Union; academics; and representatives from 14 commercial and technology companies (Google et al.).

---

[61] Figure 1: Graph and sources by GCS team research. Among others, see footnotes 49, 50, and 51.
[62] "Report on the cybersecurity and resiliency of the EU communications infrastructures and networks," *European Commission*, February 21, 2024. Available at: https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks.
[63] Ministère de l'Europe et des Affaires étrangères, "The Pall Mall process: Tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities (Lancaster House, London, 6 Feb. 2024)," *France Diplomacy, Ministry for Europe and Foreign Affairs*, February 6, 2024. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall- mall-process-tackling-the-proliferation-and-irresponsible-use-of.

28. The incorporation of AI into cyber attacks poses a severe threat to the normal functioning of the State[64]. An exceptional report[65] – published by the UK's National Cyber Security Centre (NCSC) on 24 January 2024 - states that the impact of AI on cyber threats will be offset by using AI to improve cybersecurity resilience. It also states that cyber risks are a critical challenge for institutions and private companies in the short and medium term, and AI can play a crucial role in preventing and managing this threat.

Risks and Solutions for Cybersecurity at the Time of AI:

29. Risks: Cyber-attacks and electronic breaches are the shortcomings of AI. Although AI brings many benefits, the disadvantages cannot be ignored. One of the main risks of AI is the increased liability for sophisticated cyber-attacks and electronic infiltration. When AI systems gain more power and connectivity, they become attractive targets for hackers and hacktivists. The consequences of cyber-attacks may include data breaches, unauthorized access to sensitive information, and disruption of vital jobs. Organizations need to perceive these risks proactively and thus take reinforced security measures to face cyber threats. Researchers at the Rochester Institute of Technology launched CTIBench, the first benchmark to assess the performance of LLMs in malware intelligence applications[66].

30. Among the solutions are:

- Antivirus software: Protect the system from harmful software viruses.
- Firewalls: Play as a wall between the network and probable threats.
- Software for identity and access management: Provides functionality for user access management over sensitive data and system resources.
- Authentication and certified verification of data and images/videos.
- Data encryption: Protect data by translating it into a cipher.

---

[64] David DiMolfetta, "Expect 'AI versus AI' conflict soon, Pentagon Cyber Leader says," , *Defense One*, January 26, 2024. Available at: https://www.defenseone.com/threats/2024/01/expect-ai-versus-ai-cyber-activity-between-us-and-adversaries-pentagon-official- says/393654/.

[65] NCSC, "The near-term impact of AI on the cyber threat," *National Cyber Security Center*, January 24, 2024. Available at: https://www.ncsc.gov.uk/report/impact-of- ai-on-cyber-threat.

[66] Kevin Poireault. "Academics Develop Testing Benchmarks for LLMs in Cyber Threat Intelligence." *Infosecurity Magazine*. Available at: https://www.infosecurity-magazine.com/news/testing-benchmark-llm-cyber-threat/

- Cybersecurity awareness training: Acquaint users with safe practices on the internet.
- Cybersecurity analysis: Periodically checks for and finds weaknesses.
- Malware protection tools: shield against malicious software and attacks.

Navigating Online Security Challenges

31. While investing in innovation is crucial, it is also necessary to employ emerging technologies for the common good, expanding technologies entails making them available and functional for a greater number of people. Cost-effective technologies are less costly and, therefore, cheaper and more advantageous. They are not as complex as other types of designs, making them easily understandable by anyone without prior experience. Open-source development is possible and can be adapted to meet the requirements of different needs. Education and training provide skills for people. Share an emerging risk culture and define dynamic rules for "onlife" security.

32. According to the annual report of the International Center for Counterterrorism (ICTT)[67], released in December 2023, the far-right militant groups are using deepfakes. A positional finding of the European Union Terrorism Situation and Trend Report 2023 (TE-SAT)[68], is that right-wing terrorists and extremists engage in the spreading of multiple narratives mainly on the internet.

33. The most intense form of disinformation campaign can be likened to cognitive warfare, a hostile attempt to alter thinking and critical skills. Regulation of a complex ecosystem requires consideration of corporate responsibility at the design stage, including addressing issues such as election-specific deepfakes and voter education initiatives[69]. Furthermore, social media networks are contributing to the proliferation of hate culture. The Center for Countering Digital Hate (CCDH)[70] identifies five types of online racism: anti-Semitism, anti-Muslim hate, anti-black hate, white supremacy, and AI racism. The spyware appears to be used aggressively periodically,

[67] Jacob Ware et al., "The weaponization of deep fakes: digital deception on the far right,", *ICCT*, December 13, 2023. Available at: https://www.icct.nl/publication/weaponization-deepfakes-digital-deception-far-right.
[68] Europol, "European Union Terrorism Situation and Trend Report 2023," *Europol*, December 19, 2023. Available at: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat.
[69] Valerie Wirtschafter et al., The Impact of Generative AI in a Global Election Year," *Brookings*, January 30, 2024. Available at: https://www.brookings.edu/articles/the-impact-of-generative-ai-in-a-global-election-year/.
[70] CCDH, "Understanding five types of racism online," *Center for Countering Digital Hate*, January 3, 2024. Available at: https://counterhate.com/blog/understanding-5-types-of-racism-online/.

which is not a good sign. These tools, illustrated by the Pegasus application[71], can turn most smartphones into constant surveillance gadgets 24/7. Although spyware was designed to be used as a tool against terrorism and crime, the act was used as a tool against those who were considered rebels against the government, such as journalists, opposition political members, and human rights activists. Some particular steps regarding spyware include the prohibition of spyware and the sale of spyware since there are insufficient measures to protect the public at large[72]. Moreover, spyware may only target a limited number of individuals. Still, its consequences can significantly impact society[73], including threats to freedom of speech, freedom of the press, and the integrity of elections worldwide.

Navigating Systemic Resilience: Intelligence and Systemic Resilience

34. In a world of crises and the revolution in emerging technologies, the need to identify potential future situations that could indicate risks is becoming increasingly crucial. The technological revolution is both the cause of the problem and the solution to it. Technology affects intelligence by redefining the social, political, and economic spaces in different strategic domains and their interrelationships. In addition, technological progress is crucial to security as a deterrent in today's strategic scenario.

35. As the Director of the US Central Intelligence Agency (CIA), William J. Burns wrote in an article published on Foreign Affairs[74] in January 2024, "Emerging technologies are transforming the world, including the profession of intelligence. Success will depend on creatively blending traditional human intelligence with emerging technologies." Moreover, in a speech[75] in June 2023 at the British Embassy in Prague, the Head of the Secret Intelligence Service (MI6), Richard Moore, said, "Human intelligence in the age of Artificial Intelligence will increasingly be defined

---

[71] Tamar Kaldani, Zeev Prokopets, *Pegasus Spyware, and its Impacts on Human Rights* (Information Society Department: Council of Europe, 2022), 1–28. Available at: Pegasus spyware and its implications on human rights (coe.int).
[72] United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach* (United Nations, 2023), 1-96. Available at: position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf (ohchr.org).

[73] Google's Threat Analysis Group, *Buying Spying: Insights into Commercial Surveillance Vendors* (Google). Available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.
[74] William J. Burns, "Spycraft and Statecraft," *Foreign Affairs*, January 30, 2024. Available at: https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns.
[75] "Speech by Richard Moore, head of SIS", British Government, gov.uk, last modified 19 July 2023. Available at https://www.gov.uk/government/speeches/speech-by-sir- richard-moore-head-of-sis-19-july-2023.

as those things that machines cannot do, although should expect the frontiers of machine capability to advance with startling speed. In the future, as AI begins to overtake some aspects of human cognition, digital tools may come to understand—or rather, predict—human behavior better than humans can."

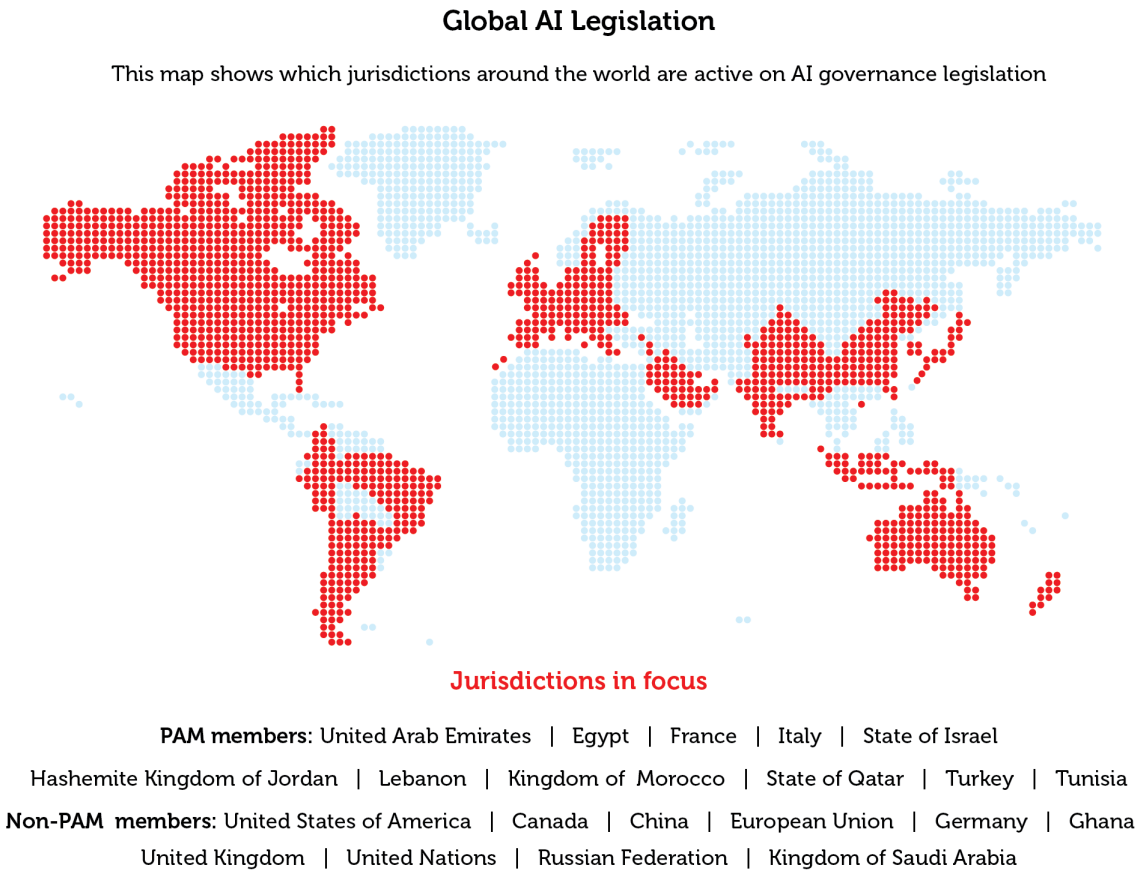
36. The new security frontiers belong to the development of the technological revolution. Three concomitant dynamics need to be explored in greater depth: the role of AI in national security; how AI applied to the military sector and productions could influence the competition of opposing parties; the threats of innovation; and the role of states in maintaining national security.
    - The Role of AI in National Security: AI improves intelligence collection, threat identification, and decision-making while helping to battle terrorism and cybercrime.
    - Military AI and the Competition of Opposing Parties: Military AI results in the enhancement of military operations through autonomous drones and AI-based surveillance.
    - The Threats of Innovation and the Place of States in National Security: Civilian use of innovations is faster and presents novel risks that call for strong structural and global solutions aimed at countering non-state actor misuse.

Navigating Disruption: Legislators and Fluid Environments

37. This section addresses the issue of AI and emerging technology regulation, highlighting already existing international legislation and identifying what those are most addressed. The report's editors acknowledge that regulation is increasingly confronted with complicated issues in a highly dynamic innovation ecosystem[76], where AI and emerging technologies have shifted from more specialized tools aimed at specific sectors to general-purpose tools. This situation makes planning by design more problematic, making preventing discrimination and malicious use more controversial[77].

[76] Kevin Poireault, "US Senators Propose Cybersecurity Agriculture Bill", *Infosecurity Magazine*, January 31, 2024. Available at: https://www.infosecurity-magazine.com/news/us-senators-cybersecurity/.
[77] Aylin Caliskan and Kristian Lum, "Effective AI regulation requires understanding general-purpose AI", *Brookings*, January 29, 2024. Available at: https://www.brookings.edu/articles/effective-ai-regulation-requires-understanding-general-purpose-ai/.

Figure 2: This map shows which jurisdictions worldwide are active on AI governance legislation[78]



38. **United Arab Emirates:** Since the launch of the "Smart Dubai Initiative" in March 2014, the United Arab Emirates has been at the forefront of establishing policy principles to guide data usage towards sustainable social benefits conferred by technologies such as AI. In 2017, the UAE pioneered international affairs by allocating the position of Minister of State for Artificial Intelligence. The UAE Cabinet established a future-oriented focus on AI and, in April 2019, approved the National Artificial Intelligence Strategy 2031[79]. The UAE is currently putting a massive emphasis on zero-trust security. As per the Dark Reading, a manifestation of Zero Trust security will surge over 10-fold by the end of 2025. Nader Henein, vice-president and analyst at Gartner, predicts that about 10% of major companies in the region will have a "completely,

[78] Figure 2: Graph by CGS research team. Based on OECD.AI (2021), powered by EC/OECD (2021), database of national AI policies, accessed on 31/10/2024, https://oecd.ai.
[79] "Smart Dubai 2021 Strategy," The Official Portal of the UAE Government, 2021. Available at: Smart Dubai 2021 Strategy | The Official Portal of the UAE Government.

mature, and measurable Zero Trust program by as early as the start of next year"[80]. This is a stark contrast to the less than 1% of companies that had the same program in 2023. This approach allows a check to be performed each time, even if a user or device is already authenticated by checking every attempt to access company resources. As the cloud implementation expands every day, the same is anticipated for the zero-trust model. Some of the objectives of Strategic National Artificial Intelligence 2031 include establishing the UAE as an international AI hub, integrating AI in strategic sectors, developing and establishing an enabling environment for AI, applying AI in government services, attracting and nurturing AI talents, researching and developing AI technologies in partnership with selected industries, and ensuring the availability of data, infrastructure, and stakeholders for effective AI governance and regulation.

39. **Egypt:** The National AI Strategy is a plan intended to harness the powers of AI for the betterment of Egyptian citizens or to put Egypt on the map of countries exploring and implementing the technology known as AI[81]. Key points include:
    - AI for Government (AI4G): In Egypt, its objectives are about using technology, especially AI, to streamline government activities by introducing the technology in the governmental decision-making system so that performance and efficiency can be enhanced along with better accountability. In this context, it aims at improving ON's public services as well as its governance by trying to minimize fraud incidences.
    - AI for Development (AI4D): They propose to apply AI to achieving the sustainable development goals of the country. The planning model allocates fields like agricultural planning, water, clinical, economic planning, production, and infrastructural planning, among others. That is why it creates improvement and caters to the needs that are vital to society.
    - Capacity Building: Egypt seems to have a clear implication of the importance of human capital in today's economy. They also engage in the following: promoting or creating awareness of developments in AI; advocating for the institution of formative education/training on AI, and undertaking a search and analysis of AI development within the country. It guarantees a competent human resource capable of promoting pro-AI human development as envisaged in the country's vision and mission statements.

---

[80] Alicia Buller, "Gulf Region Accelerates Adoption of Zero Trust," *Dark Reading*, February 26, 2024. Available at: https://www.darkreading.com/cloud-security/gulf-region-accelerates-adoption-of-zero-trust.

[81] "Egypt Moves Up 55 Places on Government AI Readiness Index," , Egyptian Ministry of Communications and Information Technology, last updated November 12, 2020. Available at: https://mcit.gov.eg/en/Media_Center/Press_Room/Press_Releases/53006.

- International Activities: Hence Egypt is not dormant and engages in international collaboration to exchange experience and ethical aspects of AI. They also collaborate with the AU and LAS partners to ensure that they harmonize and align themselves towards the establishment of a regional approach for the right use of AI technology.

However, it has recently been noted that Egypt has created an AI strategy and a Charter on Ethical Conduct for Artificial Intelligence, which shows its readiness to use this tool safely. Such initiatives are coming in line with similar countries and emphasize Egypt's pledge to use AI for the betterment of society.

40. **Italy**: The EU released the AI EU Act in March 2024[82], and all the EU member states are in the course of making their own national AI laws that would also take effect. In detail, on 23 April 2024, the Italian government passed Italy's draft AI law, which is a comprehensive blueprint of the Italian approach to AI and its social impact, regulation, privacy, and economic aspects. Although the draft law is yet to be enacted as it is still in the parliamentary process, it indicates several aspects of the AI Act and includes certain national factors. An especially strong focus is given to the requirement for fairness, for transparency, and for the accountability of AI technologies. The book comprises 25 articles and addresses five key areas: the national plan, national bodies, advertising campaigns, the rights of authors and demands, and penalties. Also, provisions include powers for the government to synchronise it with the EU Regulation on the national system. This includes spreading the understanding of AI among citizens within the framework of school and university education, as well as continuing the education of professionals and facility operators. This delegation also includes reformulating criminal law[83] to adapt the offenses and sanctions concerning the unlawful employment of AI systems. Italy has been rather engaged in the subject of new and emerging technologies regarding academic research as well as regulatory changes. Key AI regulations include:

[82] "EU AI Act.". Available at: https://www.credo.ai/eu-ai-act?utm_term=eu%20ai%20legislation&utm_campaign=EU+AI+Act&utm_source=bing&utm_medium=ppc&hsa_acc=9234903900&hsa_cam=20678021731&hsa_grp=1328212367439342&hsa_ad=&hsa_src=o&hsa_tgt=kwd-83014371791021:loc-93&hsa_kw=eu%20ai%20legislation&hsa_mt=p&hsa_net=adwords&hsa_ver=3.

[83] DLA Piper. "AI Regulation in Europe: Italy's New Draft AI Law Introduces Local Peculiarities Compared to the EU.". Available at: https://www.dlapiper.com/en-la/insights/publications/2024/04/ai-regulation-in-europe-italys-new-draft-ai-law-introduces-local-peculiarities-compared-to-the-eu.

- National AI Strategy: On 15 October 2020[84], the Italian Ministry of Economic Development put out a consultative version of the National AI Strategy. Proposing actions on four sectors of AI education, AI academic research, AI data, and AI regulation.
- Strategic Program for AI 2022-2024: The Strategic Program, approved in November 2021[85], is focused on the improvement of skills and the attraction of talents for the creation of an AI ecosystem in Italy. It comprises proposals to increase investment in enhanced AI research and explores AI opportunities in many government areas.

Moreover, Italy has strengthened civil liberties regarding AI with Law No. 205/2021, where the installation and application of a video surveillance system with facial identification in open spaces are forbidden. In February 2022, the Italian Data Protection Authority sanctioned Clearview[86] AI for unlawful processing of biometric data to commit identity theft; consequently, there is a need for transparency and legal compliance regarding AI (Global Legal Post).

41. **State of Israel:** In December 2023, Israel initiated its new policy on AI governance and the ethics of its usage[87], which are discussed below key points include:
    - Comprehensive approach: AI use in the private sector is mentioned in the AI policy as having seven issues: discrimination, oversight by humans, reporting of the interactions between the human being and the AI tool, safety and liability responsibility, confidentiality, and privacy.
    - Collaborative development: The AI Policy is created jointly with the involvement of several stakeholders, such as the Ministry of Innovation, Science, and Technology, the Ministry of Justice, the Israel Regional Council for Local Government, the PPIA Israel National Cyber Directorate Privacy Protection Authority; tech companies leading full-time investors who mainly support innovation.
    - Policy principles: Conforming to the OECD AI Recommendations, Israel's AI Policy presents shared policy guidelines and practical recommendations for solving issues that prevent responsible innovation in AI.

---

[84] European Commission. "Italy: AI Strategy Report.". Available at: https://ai-watch.ec.europa.eu/countries/italy/italy-ai-strategy-report_en.
[85] Government of Italy. "Executive Summary." In *National Strategic Program for Artificial Intelligence*. Available at: https://docs.italia.it/italia/mid/programma-strategico-nazionale-per-intelligenza-artificiale-en-docs/en/bozza/executive-summary.html.
[86] European Data Protection Board. "Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million." Available https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en
[87] See, among others, Israel's Policy on AI, Regulation, and Ethics. Available at: https://www.gov.il/BlobFolder/policy/ai_2023/en/Israels%20AI%20Policy%202023.pdf; Israel's Responsible Innovation. Available at: https://www.gov.il/BlobFolder/policy/ai_2023/en/Press%20Release%20AI%2018.12.23%20docx.pdf

- Responsible innovation concept: Highlighting the principle of "responsible innovation" proposed by Johnson, AI Policy stresses that innovation and ethics are valuable goals but not necessarily competitive.

42. **Hashemite Kingdom of Jordan:** The Artificial Intelligence Strategy and Implementation Plan of 2023-2027 is new, despite being an extension of the previous strategies in digital technology that have been implemented by Jordan's government. This strategic plan allows for the identification of strategies and a plan on how to develop and integrate AI technologies in the country. In addition, Jordan has adopted a National Charter for AI Ethics (NCAIE) that seeks to establish an ethical code and framework based on universal values, religious practices, and Jordanian traditions. The country aims to control the development and use of AI while upholding moral values. Jordan notes that AI has legal activities and ethical standpoints as strategies aimed at the adoption of AI in Jordan. Its course entails embracing the AI potential for economic development, invention, and human society[88]. The key points include:
    - Capacity-building and Expertise Development: Jordan wants to produce AI-trained human capital. Many training programs, workshops, and educational projects will motivate people to engage with the AI Ecosystem System.
    - Promoting Scientific Research and Development: The speaker pointed out that innovation should provoke the creation of research in the AI field. Jordan promotes partnerships between different sectors, such as academia, industries, and research institutions, for the creation of AI knowledge.
    - Creating an Enabling Environment for Investment and Entrepreneurship: It is a plan concerning the attraction of investments and the provision of assistance to new companies to succeed in the market of artificial intelligence. In this respect, Jordan is ensuring the kinds of preparations that are required to reposition the country to the optimal position of an AI hub for the region.
    - Legislative and Regulatory Framework: The strategy highlighted several issues that need to be addressed in the sphere of the interaction of artificial intelligence with current. Its

[88] See, among others, Jordan presents its AI strategy and Implementation Roadmap. Available at: https://www.unido.org/news/jordan-presents-its-ai-strategy-and-implementation-roadmap; The Jordanian National Ethics Charter for AI and its Guiding Ethical principle. Available at: https://www.karajahlaw.com/sites/default/files/2022-11/The%20Jordanian%20National%20Charter%20of%20Ethics%20for%20AI%20-%20Legal%20Note%20Nov%201%202022.pdf.

major goal is to build the legal frameworks for the proper formation of AI if it's to be safe and rightful.

- Enhancing Government Services through AI: The Governor of Jordan sees the possibility of upgrading the delivery of public services the governance by using AI.

43. **Lebanon:** On December 2023, usage of AI[89] was provided with its first policy in Lebanon, known as ADM-143 Use of Artificial Intelligence; this shows that Lebanon is ready to put efforts into creating the advantageous mechanism called AI with standards, principles, laws, and secure measures at the governmental level. The AI strategy created by the MoI tries to strategize sustainable development and innovation due to the adoption of AI. The focus areas are economic dependence, the knowledge economy, and the advancements in digital currencies The strategy outlines eight pillars for AI implementation in the industry. Key points include:
    - Economic boosting and the knowledge economy.
    - Innovation for Sustainable Industrial Development.
    - Dabbling in digital currency applications.
    - Utilization of nanotechnology for industrial development.
    - Promoting knowledge-based economic development.
    - Undertaking intensive studies on topics of interest.

44. **Kingdom of Morocco:** "Morocco Digital 2030"[90] is the general strategic vision of the kingdom of Morocco in the use of digital technology, which includes utilizing digital technology to transform governmental services, supporting technology and innovation in the country, and creating employment and enterprise.[91] For instance, the 2022 Morocco AI Annual Conference[92] outlined 44 recommendations aimed at Morocco's specific approach to increasing the use of AI, including regarding the country's development objectives. Morocco has recently seen a parliamentarian group suggest one year to create a National Agency for Artificial Intelligence, for instance. Thus, it becomes apparent that many of these initiatives evidence Morocco as being one of the actively developing nations when it comes to AI, despite having no formally

[89] See, among others, Use of AI. Available at :ADM-143 Use of AI - Effective 19-Dec-2023; National AI Strategy in the Lebanese Industry (2020-2050). Available at: https://andp.unescwa.org/sites/default/files/2021-
[90] Samira Njoya, " Morocco Unveils Key Pillars of "Maroc Digital 2030" Strategy," *WeAreTech.africa*, February 8, 2024. Available at: https://www.wearetech.africa/en/fils-uk/news/tech/morocco-unveils-key-pillars-of-maroc-digital-2030-strategy.
[91] "Morocco - Country Profile", Global AI Ethics and Governance Observatory, UNESCO. Available at: https://www.unesco.org/ethics-ai/en/morocco.
[92] "National AI Strategy Report: Recommendations," ,Morocco AI, last modified 2023. Available at: https://morocco.ai.

acknowledged official national AI strategy. This agency would be central to the aspect of global governance of the science of AI development, leading the world in the proper development of AI applications, and informing the public on the potential of AI and the ills that can come with it.

45. **State of Qatar:** Artificial Intelligence is at the forefront of the State of Qatar's fast-paced innovations. The Qatar National AI Strategy focuses on six pillars: education, data access, employment, business, research, and ethics, paving Qatar as the ideal destination for building up an AI-inspired future[93]. Qatar is committed to embracing new and emerging technologies responsibly and adhering to ethical AI measures, thereby positioning the country as a regional leader in innovative technologies and AI development[94]. Qatar's AI initiatives in 2024 include:
    - Qatar Foundation's Investment in Local AI Technologies: The Qatar Foundation outperforms by allocating local AI technology to address global necessities. Their areas of research cover the Internet and cyber security, Arabic language processing, and social and economic concerns.
    - AI Research and Education at various Universities: From this viewpoint, Qatar can be considered outstanding compared to other countries, as most of them have universities that teach AI and conduct research.
    - National AI Committee: On these aspects of AI regulation, the Qatari government is interested in putting forward a purely national committee for AI affairs. This committee works in conjunction with such organizations as the Qatar Computing Research Institute to enhance AI's ongoing research and innovation activities.
    - Ethics and Responsible Innovation: After outlining the global growth of AI,Qatar has been developing local research centers for AI and focusing on the education of AI alongside the establishment of ethical benchmarks for the utilization of AI. These measures are all meant to try and tap the prospects of AI to generate more possibilities in the drive of the citizens as well as in the development of the region.

    The Qatar National AI Strategy focuses on six pillars: education, data, employment opportunities for people, business, research, and ethical aspects that would prepare Qatar to become the right place for adapting to an AI-based future[95]. The aforementioned projects illustrate Qatar's

[93] Ministry of Communications and Information Technology, Qatar, "Qatar's National AI Strategy," Ministry of Communications and Information Technology. Available at: https://www.mcit.gov.qa/en/about-us/qatar%E2%80%99s-national-ai-strategy .
[94] Zealai Series, "Qatar," Zealai Series. Available at: https://qatar.zealaiseries.com/.
[95] Ministry of Communications and Information Technology, Qatar, "Qatar's National AI Strategy," Ministry of Communications and Information Technology. Available at: https://www.mcit.gov.qa/en/about-us/qatar%E2%80%99s-national-ai-strategy .

intentions to leap in the right direction towards leveraging modern technologies to power the economy while acting responsibly in the best practices provided for in the ethical AI measures, thus transforming this little nation into a leader in innovative technologies and AI development in the region[96].

46. **Türkiye**: The National Artificial Intelligence Strategy of Türkiye, created by the Digital Transformation Office powered by the Presidency and the Ministry of Industry and Technologies, includes plans that are aimed at the development of AI research in the country during 2021-2025[97]. It also involves assessing the position that the stakeholders have towards it and then enlightening Türkiye to position itself well for the best out of these changes happening around the world due to AI technologies. NAIS has stressed the value in AI systems that can be designed concerning values for value addition, about which more can be said regarding Türkiye's civilizational setting. Key priorities include:

- Human Capital and Employment: To raise ordinary citizens' awareness of AI, and another is to increase employment in the sector.
- Research, Entrepreneurship, and Innovation: Defending and supporting research activities and applications as well as fostering the establishment of novel AI relationships.
- Data and Technical Infrastructure: Informing linkages, good information sources, and general technical strong creations.
- Socioeconomic Adaptation: Intensification of the measures to advance the process of its functioning and adjustment on the socioeconomic level.
- International Cooperation: Promoting global cooperation in the advancement of artificial intelligence.
- Structural and Workforce Transformation: Leading is to manage change in organizations and among people.

47. **Tunisia:** Tunisia's National AI Strategy recognizes AI as a pivotal driver of the ongoing transformations associated with the Fourth Industrial Revolution (4IR)[98]. Within this framework,

[96] Zealai Series, "Qatar," Zealai Series. Available at: https://qatar.zealaiseries.com/.
[97] Türkiye Ministry of Industry and Technology, *National Artificial Intelligence Strategy 2021-2025* (Ankara: OECD, 2021). Available at: https://wp.oecd.ai/app/uploads/2021/12/Turkey_National_Artificial_Intelligence_Strategy_2021-2025.pdf.
[98] Tunisia, The National Artificial Intelligence Strategy of Tunisia, 2022, Lawyers Hub. Availabe at: https://www.lawyershub.org/AI%20Policy/National%20Strategies/The_National_Artificial_Intelligence_Strategy_of_Tunisia%202022.pdf.

AI is perceived as a knowledge-based industry with the potential for sustainable and inclusive development[99]. Key points include:

- Vision and Ambitions: Tunisia aims to be an active participant in the elaboration of new AI, and this corresponds to its potential and ambitions. It seeks to harness AI for collective development and tackle the problems of ethics. The country understands that the country defining the winner of the AI race will determine the future, and Tunisia seeks to carve out a decent place.
- National AI Strategy Creation: The Secretary of State for Research created a Task Force and a Steering Committee to outline Tunisia's National Artificial Intelligence Strategy.
- The strategy majorly entails methodologies, action plans, activities, and frameworks for the management of AI.
- Ethical Considerations: Tunisia relies on ethical norms and frameworks when developing digital policies, aiming to protect its citizens and promote ethical virtual futures as its digital environment is changing.

48. **United States of America:** The United States of America has seen significant advancements in AI regulation, driven by federal and state legislative efforts. On 30 October 2023, President Biden pursued a landmark Executive Order (EO) to address the possible and perilous effects of AI[100]. The order seeks to bolster AI safety, security, and privacy, promote equality and civil rights, and encourage innovation. The EO directed a sweeping range of actions within 90 days to address some of AI's biggest threats to safety and security. Agencies reported in January 2024 that they had completed all of the 90-day actions set out in the EO and made progress on other key directives set out in the order over a longer timeframe[101]. Key points of the EO include:
    - Disclosure Requirements: The developers themselves must undertake this responsibility for reporting pertinent information, and the Department of Commerce would graduate from the safety test examination.
    - Risk Assessments: Agencies have examined AI's sectoral vulnerability (e.g., the electric grid) to safeguard AI's integration into overall society.

---

[99] "National AI Strategy: Unlocking Tunisia's capabilities potential", Agence Nationale de la Promotion de la Recherche scientifique, République tunisienne. Available at: http://www.anpr.tn/national-ai-strategy-unlocking-tunisias-capabilities-potential/.
[100] The White House, "Fact Sheet: Biden-Harris Administration Announces Key AI Actions Following President Biden's Landmark Executive Order," The White House, published January 29, 2024. Availabe at: https://www.whitehouse.gov/briefing-room/statements-releases/2024/01/29/fact-sheet-biden-harris-administration-announces-key-ai-actions-following-president-bidens-landmark-executive-order/.
[101] *Ibidem*

- Foreign AI Training: Documents of the proposed regulation imply that the USA web compulsions include built-in surveillance, which may be targeting dangerous AI training.
- Public Discussion and Accountability: The OSTP (Office of Science and Technology Policy) has orchestrated public talks to shed light on the effects of AI.

The National Telecommunications and Information Administration has now requested the views of the public related to the accountability policy covering AI and thereby trust in such systems, this confirms America's attempt to ensure that AI is used ethically and legally. On 24 October 2024, the Biden Administration issued the first National Security Memorandum (NSM) on artificial intelligence (AI). In view of the fact that advances in AI will have decisive repercussions for national security and foreign policy, the NSM promotes the safe and reliable development of AI to ensure that the US is at the forefront in embracing the potential and governing the risks of AI[102].

49. **Canada:** In 2024, Canada took significant steps to ensure that AI employees adhered to high moral and ethical standards. The government has provided well-structured guidelines to protect public health, emphasizing transparency, accountability, and human-centric design[103]. Key points include:
    - Compliance with Safety and Human Rights Standards: Canada stresses the applicability of AI systems across various fields while upholding existing safety and human rights standards. This ensures that AI technologies are properly developed and used so that human interests, needs, and welfare are protected from negative impacts that might arise during the process.
    - Preventing Wasted and Inhumane AI Uses: The guidelines are specifically designed to inhibit AI abuse by stressing the right kind of conduct. This, in turn, allows Canada to avoid cases where AI systems exude vices such as waste and are deleterious.
    - Ministerial Oversight: The Minister of Innovation, Science, and Industry is responsible for conducting control to ascertain that the government has regulatory authority while ensuring AI technologies adhere to an acceptable standard.
    - Directive on Automated Decision-Making: Canada adheres to the Directive on Automated Decision-Making, which prescribes the exact terms under which the administration can base

[102] House, W. (2024, October 24). *FACT SHEET: Biden-Harris administration outlines coordinated approach to harness power of AI for U.S. national security*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/

[103] Cox & Palmer, "AIDA 2024," Cox & Palmer. Availabe at: https://coxandpalmerlaw.com/publication/aida-2024/.

decisions on automated decision-making systems. This ensures that AI decisions are made transparently, guided by ethical principles, legality, and respect for human rights[104].

The outlined policies are Canada's steps towards applying responsible AI usage to all sectors, thus ensuring the effectiveness and ethicality of these technologies. Furthermore, the initiatives that were implemented confirm Canada's resolve to make responsible use of AI, which leads to benefits for citizens but also maintains ethical standards.

50. **China:** On 15 August 2023, China outlined a complete regulatory framework for AI that covers privacy and security issues and a human-centered approach to robotics[105]. This law, the latest in a series of regulations addressing different aspects of AI, tends to strike a balance between innovative use and responsible innovation. The law introduced new restrictions for companies regarding both the training data and the outputs produced. Moreover, the framework emphasizes the necessity of partnerships between industry and academia, noting that technological breakthroughs in AI require a joint effort. Chinese legal experts are actively striving to build a strong, progressive, and future-oriented regulation on AI within domestic territory[106].

51. **European Union:** On 13 March 2024, the European Parliament adopted the AI Act[107], first proposed in April 2021, representing the world's first comprehensive regulation governing AI. The Act highlights the need for transparency, safety, and ethical considerations and emphasizes the importance of AI in driving innovation in sustainable activities, energy technologies, and environmental management[108]. In the upcoming months and years, the EU AI Act will be further developed through secondary EU legislation[109]. Key points of the AI Act include:
    - Legal Structure for AI Systems: The AI Act lays down the legal framework that AI systems should have when they pose a risk to the individual, public safety, or human rights. This calls

---

[104] Government of Canada, "Responsible Use of Artificial Intelligence (AI)," Government of Canada. Available at: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html.
[105] Matt Sheehan, "Tracing the Roots of China's AI Regulations," *Carnegie Endowment for International Peace*, February 27, 2024. Available at: https://carnegieendowment.org/research/2024/02/tracing-the-roots-of-chinas-ai-regulations?lang=en.
[106] Qiheng Chen, "China's Emerging Approach to Regulating General-Purpose Artificial Intelligence: Balancing Innovation and Control", *Asia Society Policy Institute*, February 7, 2024. Available at: https://asiasociety.org/policy-institute/chinas-emerging-approach-regulating-general-purpose-artificial-intelligence-balancing-innovation-and.
[107] See, European Parliament, "European Parliament Legislative Resolution of 24 April 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence and Amending Certain Union Legislative Acts," *European Parliament,*
[108] "EU Parliament Approves Landmark AI Act: Setting the Stage for Ethical and Sustainable AI Innovation," *Environment and Energy Leader*, March 14, 2024. Available at: https://www.environmentenergyleader.com/2024/03/eu-parliament-approves-landmark-ai-act-setting-the-stage-for-ethical-and-sustainable-ai-innovation/
[109] TA-9-2024-0138_EN. Available at : https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html

for providing necessary explanations and availing of data so that the public can get involved in the formation and decision-making of these technologies.

- Human Supervision and Control: The Act stipulates the necessity of the presence of a human being when any AI system is being supervised and controlled. Such a condition makes humans the ultimate authority supervisors and therefore able to take the initiative and step in whenever the need arises, thereby mitigating against excessive use of automatic decision-making.
- European AI Development: The EU will engage in developing its state-of-the-art AI at the level of its member states. With this purpose, the European Commission wants to focus on reaching the innovation level, research and development, and AI-related issues within the European AI ecosystems.
- Penalties for Offenders: The law contains provisions for sanctions on anyone who goes against the measures established to regulate AI. The lack of this enforcement concept will result in the violation of regulations, which may have serious consequences for organizations and their AI practices.
- Balancing Innovation and Ethics: The AI Act simultaneously supports AI invention and investment initiatives, and its main renewing objectives are responsible AI development. AI technologies need to embrace ethical rules so they can better people's lives without infringing on human rights.
- Safeguarding Individual Freedoms: The law first protects several rights and limitations related to AI systems. This safeguard should be provided so that individual liberties can be guaranteed, which include protection of privacy and non-discrimination.

52. **Council of Europe**: The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Vilnius, 5 September 2024) is the first legally binding international treaty in this field. This Framework Convention complements existing international standards on human rights, democracy and the rule of law, and aims to fill legal gaps that can arise from rapid technological advances. Work began in 2019, when the Ad Hoc Committee on Artificial Intelligence (CAHAI) was mandated to examine the feasibility of such an instrument. The Framework Convention was drafted by the 46 member states of the Council of Europe, with the participation of all observer states: Canada, Japan, Mexico, the Holy See and the United States of America, as well as the European Union, and a significant number of non-member states. In addition, 68 international representatives from civil society, academia and

industry, as well as several other international organizations, actively participated in the development of the Framework Convention.

53. **Germany**: The Artificial Intelligence Strategy was first adopted in Germany in November 2018 and then updated in December 2020. It comprises several critical elements; firstly, it presents the state-of-the-art AI development provided within the context of the country in question; secondly, it enshrines very specific goals for future AI advancement into law; and lastly, the cross-cutting strategy presents policy steps for getting these objectives in order. Furthermore, the German Federal Government has committed to raising the planned expenditures for AI promotion from 3 billion EUR to 5 billion EUR by 2025 under the Economic Stimulus and Future Package[110]. This investment aims to enhance Germany's position in the AI market and foster innovation across industries.

54. **Ghana:** The Government of Ghana formulated the Ghana National AI Strategy in 2022 and implemented it in 2023[111]. The outlined strategy is set to span a decade from 2023 to 2033, and it is to act as a long-term guideline and frame for leveraging the AI applicability towards fostering the country's economic and social growth with a focus on inclusiveness and sustainability, as well as reducing the adverse effects posed by the disruptive technologies[112]. Content-wise, Ghana's AI strategy has eight pillars and 31 corresponding key policy recommendations, seven target sectors, an action plan, and a responsible office for implementing the strategy. The strategy document also presents a diagnostic assessment of Ghana's AI ecosystem, which identifies opportunities and constraints and existing concrete cases of AI applications in some sectors of the country. The AI Strategy aims to impact the lives of ordinary Ghanaians in various sectors such as education, health, agriculture, and commerce[113]. As outlined in the strategy, key priorities include equipping students and educators with tools and technologies to support learning and advance research; offering incentives to businesses, particularly startups, that incorporate AI tools and technologies to bolster Ghana's digital economy; and ensuring the distribution of medical supplies to healthcare facilities in rural regions. It must be noted that since the delivery in October

[110] European Commission, "Germany AI Strategy Report,". Availabe at: https://ai-watch.ec.europa.eu/countries/germany/germany-ai-strategy-report_e.
[111] "Putting the Spotlight on Ghana's AIStrategy," PenPlusBytes, 2024. Available at: Putting-the-Spotlight-on-Ghana's-AI-Strategy.pdf (penplusbytes.org).
[112] *Ibidem*
[113] "Stakeholder consultation workshops drive insights for national AI strategies in Tunisia and Ghana," , *The Future Society*, June 9, 2022. Available at: https://thefuturesociety.org/stakeholder-consultation-workshops-drive-insights-for-national-ai-strategies-in-tunisia-and-ghana/.

2022 of the National AI Strategy, internet searches show no trace of a digital copy of Ghana's AI Strategy, not even the Ministry of Communication and Digitalization website that fronted it.

55. **United Kingdom:** The UK government has embraced a contextual approach to regulating AI that is geared towards the achievement of a balance between innovation and the use of AI systems in a responsible manner[114]. The UK advocates for the following outcomes-oriented approach to the development of AI. Key points include:
    - Algorithmic Transparency: The Central Digital and Data Office (CDDO) has introduced some of the world's first guidelines for achieving algorithmic transparency at a national level.
    - AI Standards Hub: The emergence of new technologies aimed at standardizing AI technologies.
    - Guidance for the Public Sector: Service providers in the United Kingdom adhere to government regulations regarding the use of AI in public services.
    - Research and Auditing: Academic research on AI governance is conducted at the Center for Data Ethics and Innovation, while the Information Commissioner's Office (ICO) provides resources for auditing AI systems.
    - Transparent Decision-Making: ICO and ATC are collaborating on solutions to explain AI outputs.

56. **United Nations**: On 21 March 2024, the United Nations General Assembly adopted Resolution A/78/L.49[115] on "Seizing the opportunities of safe, secure, and trustworthy Artificial Intelligence systems for sustainable development," which is the first-ever resolution adopted by the UN on AI. While the resolution has no immediate binding effect, its content will guide the regulatory development of AI technologies at the national and international levels in the coming years[116]. The strategy sets out how the UN system can support the use of new and emerging technologies to accelerate the achievement of the 2030 Sustainable Development Goals and facilitate their

[114] United Kingdom, "AI Regulation: A Pro-Innovation Approach," Government of the United Kingdom, March 29, 2023. Available at: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach.
[115] "UN Resolution on AI," A/RES/2406592, New York: United Nations, 2024, Available at: https://www.un.org/en/documents/a/res/2406592.pdf.
[116] Baker McKenzie, "International: The United Nations Adopts Its First Resolution on AI," Baker McKenzie InsightPlus. Available at: https://insightplus.bakermckenzie.com/bm/data-technology/international-the-united-nations-adopts-its-first-resolution-on-ai#cntAnchor1.

alignment with the UN Charter, the Universal Declaration of Human Rights, and the principles of international law[117]. Key points include:

Five Guiding Principles:

- Protect and promote global values: The resolution underscores the significance of human rights and international law as essential values and responsibilities for regulating AI.
- Foster inclusion and transparency: Create conditions that enable groups to make informed decisions.
- Work in partnership: Collaborate with several actors to increase the existing knowledge.
- Build on existing capabilities and mandates: Utilize new technologies to enhance the UN's current mandates and functions.
- Be humble and continue to learn: Remain open to diverse perspectives and continuous learning opportunities.

Strategic Commitments:

- Internal capacity: Enhances the UN's understanding and integration of new and emerging technologies.
- Advocacy and dialogue: Raise awareness of critical issues and initiate discussion.
- Cooperative frameworks and norms: Foster normative discussion, support, and cooperation.

The resolution recognizes that AI's impact may extend to fundamental rights such as the right to life, privacy rights, and freedom rights of expression. Paragraph 13 of the resolution highlights the primary objective of the United Nations system in AI governance as the establishment of a worldwide framework that aligns with international law and human rights[118]. The resolution emphasizes the risks of biased data in reinforcing hate culture and discrimination and urges international cooperation in developing and implementing safe AI systems, encouraging further collaboration among stakeholders. Moreover, on 25 June 2024, the 78th session of the UN General Assembly (UNGA) unanimously adopted a resolution[119], proposed by China and co-sponsored by over 140 countries, on "Enhancing International Cooperation on Capacity-building of Artificial Intelligence." The resolution aims to achieve inclusive, beneficial, and sustainable development of artificial intelligence, thereby contributing to the realization of the United

[117] United Nations, "New and Emerging Technologies," United Nations. Available at: https://www.un.org/en/newtechnologies/.
[118] Baker McKenzie, "International: The United Nations Adopts Its First Resolution on AI," Baker McKenzie InsightPlus. Available at: https://insightplus.bakermckenzie.com/bm/data-technology/international-the-united-nations-adopts-its-first-resolution-on-ai#cntAnchor1.
[119] N2418380.pdf. (n.d.). Google Docs. https://drive.google.com/file/d/1xxWlN6mt2BzkoQppFicjFBR6fs0ENyxZ/view

Nations' 2030 Agenda for Sustainable Development. In this context, at its 18th Plenary Session, PAM delegates unanimously adopted a resolution on AI, highlighting its opportunities for innovation and growth, while addressing the ethical and security challenges posed by uncontrolled development of generative AI tools. Furthermore, on 9 August 2024, after three years of negotiations, the committee established ad hoc by the UN General Assembly, under the leadership of Ambassador Faouzia Boumaiza-Mebarki (Permanent Representative of Algeria to the United Nations), approved the draft UN Convention against Cybercrime[120]. The secretariat for the negotiations was established at UNODC. The document must now go through formal adoption by the General Assembly and must be ratified by at least 40 countries to become operational. The text is part of a tight global debate. Originally proposed by Russia in 2017, it has faced strong opposition from, among others, the United States, Europe, and numerous private actors. Issues related to cybersecurity and the governance of emerging technologies represent a decisive geostrategic asset. Central to the discussions, including this draft Convention, are concerns about safeguarding human rights. PAM-CGS has been following the evolution of this convention in recent months and will continue to study its contents and subsequent political-diplomatic steps.

57. **Russian Federation:** Federal Law No. Law 258-FZ[121], which took effect in January 2021, addresses issues such as liability in the event of an AI malfunction or error and unintentional disclosure, overtaking intelligence technology that may be used in future regulations. Federal Law No. Law 123 FZ30[122], regulating "digital sandboxes" in Moscow, came into force on 1 July 2023. Digital sandboxes are places where technologies can be developed and tried out even do not comply with the existing legislation. This experimental regime enables firms to create innovative AI technologies beyond legal categories. Practical governance will also facilitate the realization of the Moscow government's project "Smart City 2030"[123], as part of the Sustainable Development Goals, focused on advancing urban development, particularly to raise local living standards and ensure more effective management and service delivery solutions.

---

[120] United Nations: Member States finalize a new cybercrime convention. (n.d.). United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

[121] Federal Law of the Russian Federation No. 258-FZ. Available at: https://cis-legislation.com/document.fwx?rgn=126433

[122] See, among others, Federal Law of the Russian Federation No. 123-FZ. Available at: https://cis-legislation.com/document.fwx?rgn=1240; Artificial Intelligence in Russia. (2021). Available at: https://apps.dtic.mil/sti/trecms/pdf/AD1151100.pdf.

[123] "Moscow Presents an English-Language Catalog of Smart City Solutions with an Indication of Relevant UN Sustainable Development Goals," The Smart City Journal. Availabe at: https://www.thesmartcityjournal.com/en/cities/moscow-presents-an-english-language-catalog-of-smart-city-solutions-with-an-indication-of-relevant-un-sustainable-development-goals.

58. **Kingdom of Saudi Arabia:** The Kingdom of Saudi Arabia has proposed a Draft Intellectual Property (IP) law in July 2023 which is one of the first in North Africa and the Middle East area to provide protection for AI-created IPRs. The law comprises a set of regulations that support the promotion of AI as well as new and emerging technologies. AI is a core pillar of Saudi Arabia's Vision 2030 plan, whereby 66 of the 96 strategic objectives revolve around data-based technologies. The country aims to guarantee that the benefits of AI are optimized towards achieving Vision 2030's goals. In September 2023, the Saudi Data and Artificial Intelligence Authority (SDAIA) published AI Ethics Principles[124], which focused on seven key areas: fairness, privacy and security, humaneness, social benefits, and environmental implications; reliability and safety; transparency of information or thrust inherently right in itself with no need for judgment.

AI Trends in cybersecurity are to be monitored in 2024

59. Monitoring unwanted trends and developments in AI is vital to inform cybersecurity experts about the latest developments.
60. Detecting and responding to AI-powered threats: AI-powered threat detection and response systems should be monitored and further developed to counter threats effectively.
61. Building trust in AI systems: Trust is a vital prerequisite contributing to the adoption and efficacy of AI technology for cybersecurity operations. Ensure that AI algorithms and models are transparent and comprehensible, allowing users and stakeholders to understand their capabilities and trustworthiness.
62. AI in data backup and recovery: AI developments can be monitored to facilitate better information protection systems and advanced recovery speeds when cyber incidents occur.
63. Rise of adversarial AI: The importance of monitoring adversarial AI cannot be overemphasized, as it will help to develop strong defenses against adversarial attacks and protect AI systems from manipulation.
64. Human augmentation of security operations: AI provides complementary human assessment capabilities to cyber operations. Observing critical areas, such as the integration between AI and

[124] See, among others, Saudi Arabia Regulations AI. Available At: https://www.twobirds.com/en/insights/2023/global/saudi-arabia-pioneers-regulation-of-artificial-intelligence;
Saudi Arabia AI Ethics Principles, Available at: https://www.google.com/url?q=https://www.dataguidance.com/news/saudi- arabia-sdaia-publishes-ai-ethics- principles&sa=D&source=docs&ust=1707844455539803&usg=AOvVaw2rKgot1cqlOPddQSbFanOg;
Brian Meenagh et al., "A general introduction to Artificial Intelligence Law in Saudi Arabia," *Lexology*, January 3, 2024. Available at: https://www.lexology.com/library/detail.aspx?g=376990da-7f7f-465f-b1e9-be732225363f.

human expertise, will enable organizations to keep their security operations running properly to achieve total cyber resilience.

65. Ensuring secure data practices: Tracking the developments in AI technologies related to data privacy and encryption would ensure the implementation of proper protection measures.
66. Regulatory compliance in AI-supported cybersecurity: It will be vital to watch for state controls and adjust practices while adhering to appropriate standards and lawful dangers or ruining an organization's image.
67. Prepare for cybersecurity AI trends in 2024: Organizations should anticipate emerging AI developments in cybersecurity. These also involve investing in AI technologies, training cybersecurity professionals in AI, and developing robust AI governance frameworks to ensure people do not abuse them[125].
68. Including AI in cybersecurity: AI can protect networked systems from cyber threats, attacks on them, spoiling, and unauthorized access. Using widely adopted AI methods like machine learning, deep learning, or neural networks, NLP (formerly SNNs)[126], KR, and RS can also sufficiently cover the cybersecurity challenges. However, AI deployment is not an end-all, be-all solution for all cybersecurity woes and comes with potential threats of automation failed attacks, possibly caused by dirty robots. It is essential to create rules and standards regulating the growth process of AI system deployment within this area and supervise these processes. EU AI Act is a landmark in terms of regulation aimed at governing the useability of AI within the European continent.

Prosecution

69. Among other regional and international instruments to prevent, contrast, and prosecute cybercrime it is important to mention the Convention on Cybercrime, the Budapest Convention, adopted by the Council of Europe in 2001. It represents a fundamental tool that aims to help combat crimes that can only be committed through the use of technology, where the devices are both the instrument for committing the crime and the target of the crime, and crimes where the technology has been used to facilitate another crime, such as fraud. It also provides guidance for any country developing national cybercrime laws and serves as a basis for international

[125] See, among others, Justin Rende, “Track These 7 Trends for Proactive Cybersecurity in 2024," *ISACA, December 26, 2023*. Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2023/track-these-7-trends-for-proactive-cybersecurity-in-20.
[126] Stephen Weigand, "Biggest AI Trends of 2024: According to Top Security Experts", *SC Media*, January 2, 2024. Available at: https://www.scmagazine.com/news/2024-tech-predictions-defenders-adversaries-will-fine-tune-artificial-intelligence-to-their-advantage; Simplilearn, "20 Emerging Cybersecurity Trends to Watch Out for in 2024," *Simplilearn*, April 15, 2024. Available at: https://www.simplilearn.com/top-cybersecurity-trends-article.

cooperation between the parties to the Convention[127]. For further information about formal international cooperation mechanism, please visit:

Table 1: Summary table of the main issues addressed in the report:

Issue	Summary
Malicious use of emerging technologies	The report explores the malicious use of AI, including machine learning, and other technologies by state and non-state actors, including terrorist and criminal networks, in security and global stability.
Geopolitics of (in)security	The report takes into consideration global crises, military conflicts, and humanitarian issues related to cybersecurity, space, air, land, and maritime domains.
Risks from emerging technologies: Activities of authoritarian regimes, terrorists, and criminal networks	The report examines how terrorist and criminal organizations can benefit from emerging technologies such as AI (including deepfakes), drones, and cyber-physical emerging technologies, resulting in threats to societal stability, national security, and critical infrastructure.
Navigating the digital underworld: Cybercrime	The report discusses the rise of cybercrime enabled by the Internet and advanced technologies, including online terrorist recruitment, financial crime, and the challenges for law enforcement in countering cyber threats.
Navigating Disruption: Legislators and Fluid Environments.	The report lists available AI legislation, emphasizing variations in approach. It starts with European regulations and extends to the

[127] *Convention on Cybercrime*. (2001). rm.coe.int. Retrieved November 13, 2024, from https://rm.coe.int/1680081561

	Mediterranean and Gulf regions. At the end, there are the UN strategic directions.
Navigating Systemic Resilience: Intelligence and Systemic Resilience	The report highlights the uniqueness of AI in predicting risks in the face of global crises, such as pandemics and digital revolutions. It also underscores the need for human-AI collaboration, building trust in AI systems, and proactive cybersecurity measures.
AI Trends in cybersecurity are to be monitored in 2024	The report examines the manifestations and solutions to AI-powered cyberattacks, including antivirus software, firewalls, and cybersecurity awareness training.

Conclusions

70. PAM-CGS is pursuing a transdisciplinary and complex path to "onlife" security in the age of AI and emerging technologies. The interrelationship of opportunities, risks, and threats makes the technological revolution a "two-faced Janus"[128]. Working on AI and emerging technologies from the perspective of their malicious use by transnational terrorist and criminal networks cannot deny the crucial role of the same technologies in preventing and tackling terrorist and criminal activities.
71. Considering the extremely dynamic and transformative nature of AI and emerging technologies, this report delves into the increasing impact on terrorist organizations and transnational criminal operations. It examines their malicious use of technologies, the growing potential for financing their activities, the transformation of armed conflict practices, and the interrelationship between cyber-attacks and the use of AI.
72. In an era marked by the geopolitics of (in)security, it is essential to integrate national regulations, each reflecting a different political-strategic vision on the issue, with clear and mandatory guidelines. Legislation, by its very nature, is confronted with dynamics of increasing complexity and speed that might render obsolete existing legislation in relatively short time. Therefore,

[128] Tong, Shuye, Phanish Puranam, Omar A. El Sawy, and Daiki Ariyachandra. "The Janus Face of Artificial Intelligence Feedback: Deployment Versus Disclosure Effects on Employee Performance." *Strategic Management Journal* 42, no. 9 (2021): 1600-1631.

building effective and lasting cooperation among all the stakeholders involved—international organizations, governments, private companies, intelligence services, police forces, think tanks and research centers, universities, civil society organizations, and public opinions—is critical.

73. As a "living document," the findings in this report constitute the basis for the establishment of a Global Permanent Parliamentary Observatory, served by PAM/CGS, which, working in collaboration with the UN, IGOs, Parliaments, Governments, Universities, Think Tanks, and civil society organizations, will serve as an essential support tool to promote and advocate for effective legislation and governance on a global scale (principles, non-binding guidelines and practices), providing key data to anticipate and address the effects of malicious use of AI and emerging technologies. As part of its efforts, the PAM/CGS offers, through its Observatory, a daily and weekly "digest" of information and analyzes from open sources on AI and emerging technologies, from the perspectives of their malicious use, security, governance, legislative developments, and defense. The digests are available at the following link: PAM-CGS Digest on AI and Emerging Technologies – Pam / https://www.cgspam.org/digest/

74. The PAM-CGS is committed to reaching the objectives of the Summit for the Future held on 22 and 23 September 2024 in New York. On that occasion, the Pact for the Future was adopted, which includes a Global Digital Compact and a Declaration on Future Generations[129]. The purpose of the Global Digital Compact is for signatory actors to work towards an open, free, safe, and people's digital future, based on human rights and in accordance with the Sustainable Development Goals[130]. At the eve of the Summit of the Future, at the UN Headquarters in New York, PAM, with the support of its CGS, organized a High-Level Parliamentary Side Event entitled "Parliamentary Support in Re-Establishing Trust and Reputation in Multilateral Governance," in partnership with the UN Security Council Counter-Terrorism Executive Directorate (CTED) and the Permanent Missions of the Kingdom of Morocco and Italy to the UN[131]. PAM/CGS initiatives to promote these goals help in enhancing parliamentary participation and setting the necessary parameters for the institutional use of the technologies while being as inclusive as possible. Therefore, as a parliamentary platform, PAM/CGS helps to build a stronger and interconnected digital society, which is one of the key subjects of the Global Digital Compact and the Summit. PAM and PAM-CGS, as part of the process of researching, reflecting on and

[129] United Nations. (n.d.). Summit of the Future 2024 - United Nations | United Nations. https://www.un.org/en/summit-of-the-future
[130] Global Digital Compact | Office of the Secretary-General's Envoy on Technology. (n.d.). https://www.un.org/techenvoy/global-digital-compact
[131] *PAM High-Level Parliamentary Event at the UN Summit of the Future*. (2024, September 22). www.pam.int. https://pam.int/pam-high-level-parliamentary-event-at-the-un-summit-of-the-future/

sharing the United Nations strategic process on the issues of governance of artificial intelligence and emerging technologies, will be present at the Internet Governance Forum to be held in Riyadh in December 2024: in collaboration with CTED, the focal points of the report will be presented.

Next steps

75. PAM and CGS stand ready to continue assisting the UNSC/CTED in presenting the key findings of this report to its constituency and providing regular updates to the CTED due to the constant and rapidly evolving nature of the issues covered. The CGS will undertake several activities during the year 2024: i) Research and collection of open source materials, ii) Research on several topics, including the frontiers of emerging technologies and the growing complexity of opportunities and risks, the new threats posed by malicious state and non-state actors, the constant updating of national and continental regulations, and the evolving global governance of the phenomenon; iii) the establishment of the PAM-CGS "Global Parliamentary Observatory for ICT and AI", which, through the monitoring of global news, academic reports, and legislative initiatives, will regularly provide key data to anticipate and face the adverse effects of the malevolent use of AI and emerging technologies, as well as of the best practices put in place; iv) Provide higher awareness among target groups of digital forensic specialists and justice systems on the risks of threats coming from AI, and their methods of combating them; v) Foster the development of policies to govern AI, and encourage the use of security by design, and elimination of data bias; vi) The organization of *ad hoc* seminars with international experts to develop further guidelines; vii) the presentation of the report to the members of CTED at UNHQ.
76. In conclusion, the PAM Secretariat also recorded with satisfaction the many requests from its national parliamentary delegations to organize 2025 a dedicated meeting on the many applications and challenges posed by AI, as a result of the topics raised by the PAM rapporteur on AI, and the ongoing work that PAM has been conducting with CTED.

The report was peer-reviewed by international experts from the following organizations (in alphabetical order): AWS Public Policy Europe, Middle East and Africa (EMEA); Interpol; Media Duemila; NATO Strategic Direction - South HUB; NATO Defense College Foundation; Parliamentary Assembly of the Mediterranean; Policy Center for the New South; the UN Security Council Counter-Terrorism Executive Directorate (CTED)