Issue Brief
February 21, 2024

Must Regulate the AI Trifecta: Security, Business, and Privacy

Kiran Bhatt, Aniruddha Inamdar, and Sanjay Pattanshetty

Photo credit: Deemerwha studio / Shutterstock

The enormous amount of research and development in AI technologies has led it to grow to a level that impacts security, business, and privacy concerns. The proliferation of artificially intelligent weaponry raises the potential for arms races, the possibility of non-state actors obtaining such weapons, and security issues. From the business lens, AI has catalyzed decision-making and operational strategies that have enabled efficiency. However, as the functioning of AI is dependent on data, deliberating privacy issues has become necessary. Discussions around AI governance are still in their infancy, which presents a chance to create frameworks for governance that encompass every step of the process, from development to deployment. While a few states have initiatives on AI principles and ethics, the fragmented landscape results in a lack of coordination of AI governance at the international level. Therefore, to sustain international peace and security, there is a need for a comprehensive framework that encompasses the legal, political, ethical, economic, and security dimensions.

Introduction

Artificial Intelligence (AI) has become pivotal in the contemporary geopolitical landscape. Its wide-ranging applications, from household assisting devices (Google Assistant, Apple's Siri, Amazon's Alexa) to revolutionizing defense, cybersecurity, healthcare, banking, and education, have made it a strategic imperative for countries to invest in its research and development to gain a competitive edge. The intersectoral application of AI also makes it an important element in the achievement of Sustainable Development Goals (SDGs).[1] This strategic interest in AI has gained traction and has become a "new race" among countries to ensure the proliferation of AI in security, business, and privacy. With both state and private players playing a major

role in the development and adoption of the new technology in the three domains, there is a need to regulate its use by establishing legal instruments at the national, regional, and global levels that consider the economic, security, and legal aspects along with political will and consensuses.[2]

Why Do We Need Regulation?

Security Dimension

In the security domain, AI has shifted the development of traditional military machines to the development and deployment of new algorithms and machine-learning models. While AI applications in the military are expected to bring in a wide range of benefits, there are striking risks associated with them. The pursuit of outweighing the adversaries could result in proliferation and arms racing among states, due to which it is critical to assess the AI being employed in warfare. Further, the application of AI technologies in the non-conventional mode of warfare, especially by non-state actors could reap benefits in asymmetric warfare against state actors. The numerical and ammunitions superiority of a state actor can be nullified through the usage of AI-based weapon systems. The ability of AI to penetrate through trackers and jammers has opened multiple opportunities for non-state actors to conduct high-profile assassinations, sabotage state security systems, and inflict damage on critical security systems without human involvement.[3]

"The ability of AI to penetrate through trackers and jammers has opened multiple opportunities for non-state actors to conduct high-profile assassinations, sabotage state security systems, and inflict damage on critical security systems without human involvement.

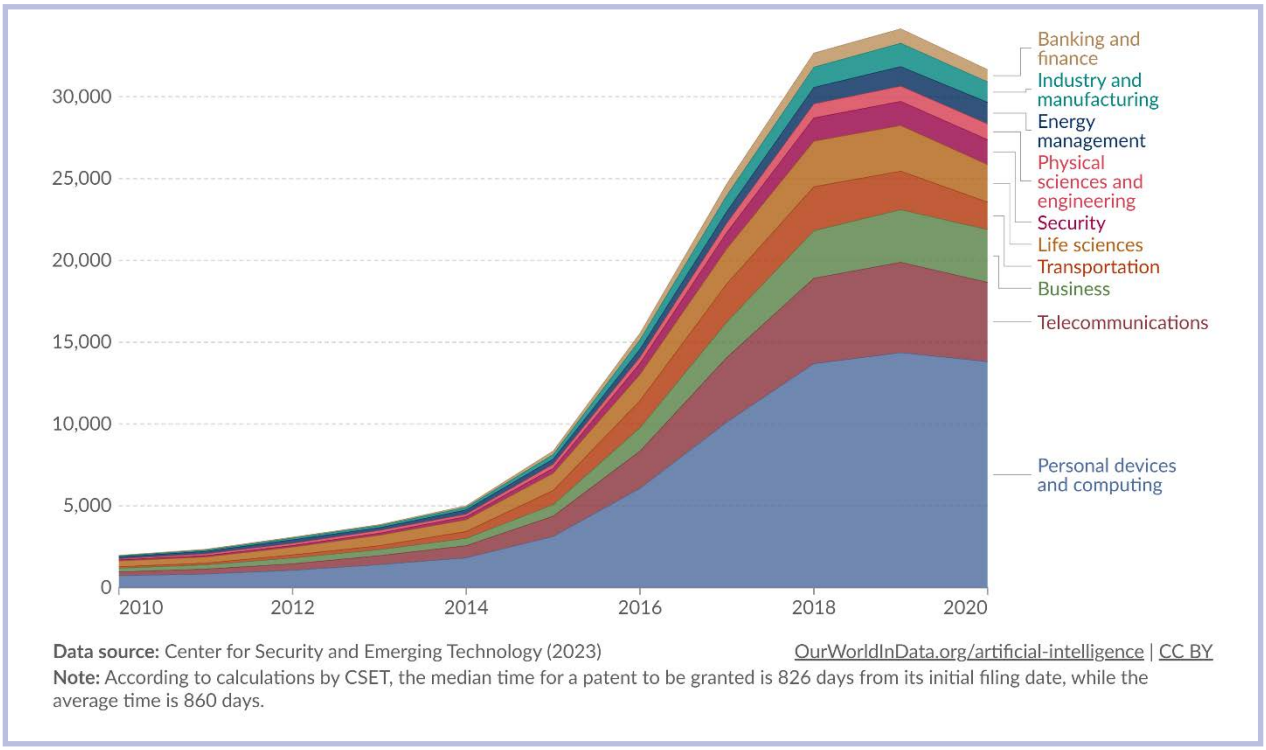
The need to safeguard data is also important from the prism of national security, as adversaries could use cyberattacks to achieve their objectives. In April 2007, Estonia experienced a series of attacks causing the denial of services for both the public and the private sector, ranging from commercial websites to critical services like banks and ministries.[4] The attack forced Estonia to close its digital borders and international web traffic, resulting in the incident being tagged as the first instance of cyber operations being used by a foreign player to threaten the national security of another actor.[5] The advances in AI have reignited thoughts about such incidents reoccurring more frequently and with more intensity, highlighting that data security should be paramount for governments to ensure the smooth and seamless adoption of digital technologies.

Business Domain

The role of AI and machine learning is also crucial for businesses, which require data to fuel their decision-making, growth, and operational strategies.[6] The increased demand for AI and data-driven functioning by businesses is due to its capability to predict sales, develop marketing strategies, tackle competitors and find collaborators. Figure 1 depicts the increasing focus of various industries and businesses across the world on developing, patenting, and adopting AI. In 2020 alone, 13,813 AI-related patents were filed by the personal devices and computing industry followed by 4,848 by the telecommunications sector. While adopting AI in industry and business is a positive from the financial standpoint, the lack of transparency in the use of personal data and sensitive information collected by these businesses, without formal consent, raises a red flag about privacy.[7]

Figure 1: **Annual Granted Patents Related to Artificial Intelligence, by Industry, World**

Granted patents were first submitted in the selected country's patent office, but could have subsequently been granted by any country's patent office.



Source: Center for Security and Emerging Technology (2023) – processed by Our World in Data[8]

Privacy Concerns

The use of data is important for AI to make inferences, however, this also poses a challenge since information such as medical data, location, and personal preferences could be accessed. Thus, there is a need to address the privacy challenge, especially in managing personal information to protect individual rights and prevent unauthorized use and data disclosure.[9] An associated issue is the misuse of data by a few actors to create and circulate fake images and videos, which could have serious consequences since in most cases the data used is without consent, violating individual privacy.[10] The usage of data by AI algorithms is complex and not necessarily transparent, making it difficult for individual users to understand how their data is being utilized.[11]

Additionally, issues such as identity theft and AI-based surveillance are a few more concerns that are posing threats to privacy and civil liberties, requiring organizations, governments, and multilateral forums to focus on proactive measures such as the implementation of protocols for data security, usage of data for intended purposes, and foremostly ensure AI systems are developed by adhering to ethical standards and principles.[12] Ensuring trust among end-users and having transparency is key while developing AI especially when the ethical, legal social, and economic concerns associated with AI are still being researched.[13] The Interim Report of the UN Secretary-General's AI Advisory Body also highlighted the need for better alignment between norms and the development and deployment of AI. It further noted that there is a need for better inclusive engagement in international discussions on regulatory and policy initiatives concerning AI.[14] Therefore taking cue from the report, it is imperative

to incorporate a multi-stakeholder perspective in developing a governance framework that promotes inclusion, transparency, and trust to ensure a smooth and successful adoption of AI technology. Figure 2 depicts the three key areas of focus for an effective AI Governance Framework along with the list of suggested avenues to address in each domain.

Way Forward and Conclusion

Along with the evolution of AI technologies, the threat of weaponization is also rapidly increasing. There is a looming fear of AI-influenced warfare due to its ability to traverse domains from space to cyberspace.[15] While technological development will continue, it is the collective responsibility of the international community to take necessary steps to prevent the use of AI in the development of lethal weapons by actively acknowledging the risks associated with its proliferation. Although the possibility of such instances is increasingly debated, the present weapon systems are susceptible to cyber-attacks making them equally fatal.[16] Therefore, a regulatory framework for using AI and its application in weapons needs to be formulated at the earliest.

Despite efforts on AI ethics and principles from industry, a few states, and civil organizations, there is a lack of international coordination on AI governance due to the fragmented landscape. Figure 3 shows the states that have already implemented AI strategies at the national level, which also highlights the need for an inclusive approach since most of the developing countries are lagging. Thus, there is a need for multilateral forums to address the challenges posed by AI and its applications through a collective approach.

The UN hence needs to lead the ongoing initiatives under its aegis of a credible multilateral track. One way to understand the current situation is to draw a parallel between nuclear technology/weapons during the mid-twentieth century and AI currently. Both technologies were developed to aid peaceful civilian purposes. AI has the potential to be used in a wide range of activities which need to be harnessed rather than focusing on its applicability of weapons thereby instigating a new era of arms race. Thus, learning from history, the international community comprising governments along with UN agencies needs to step in to address the impact of AI development and deployment.

Figure 2: **Key Areas of Focus for an Effective AI Governance Framework**

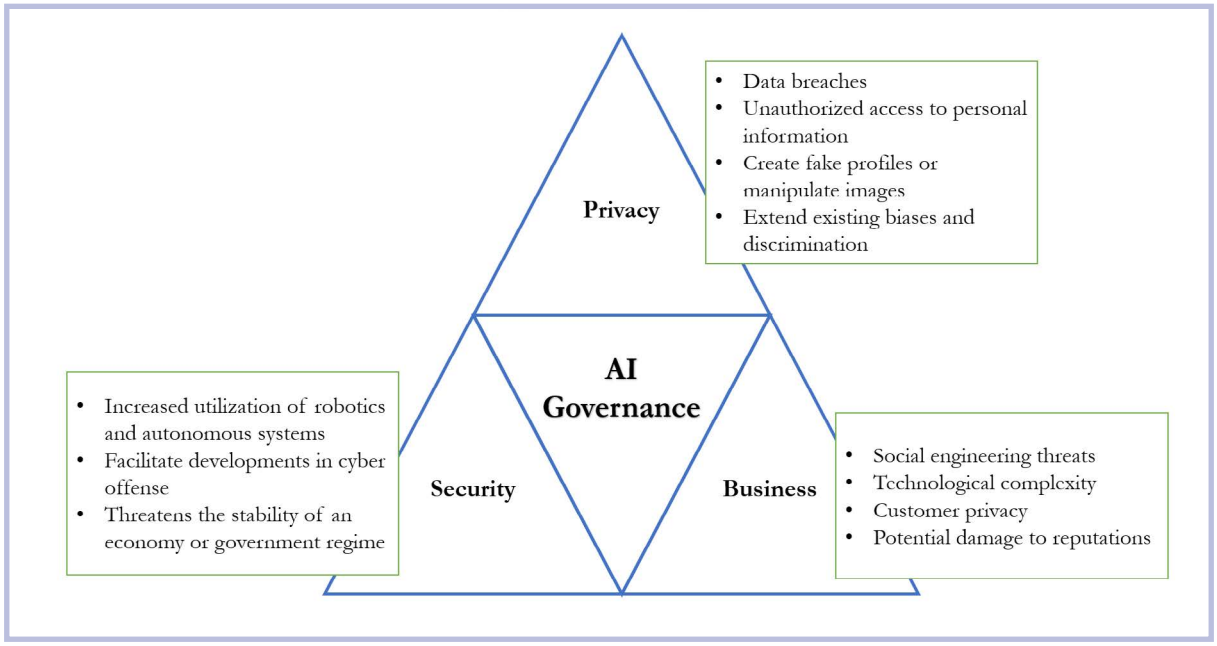
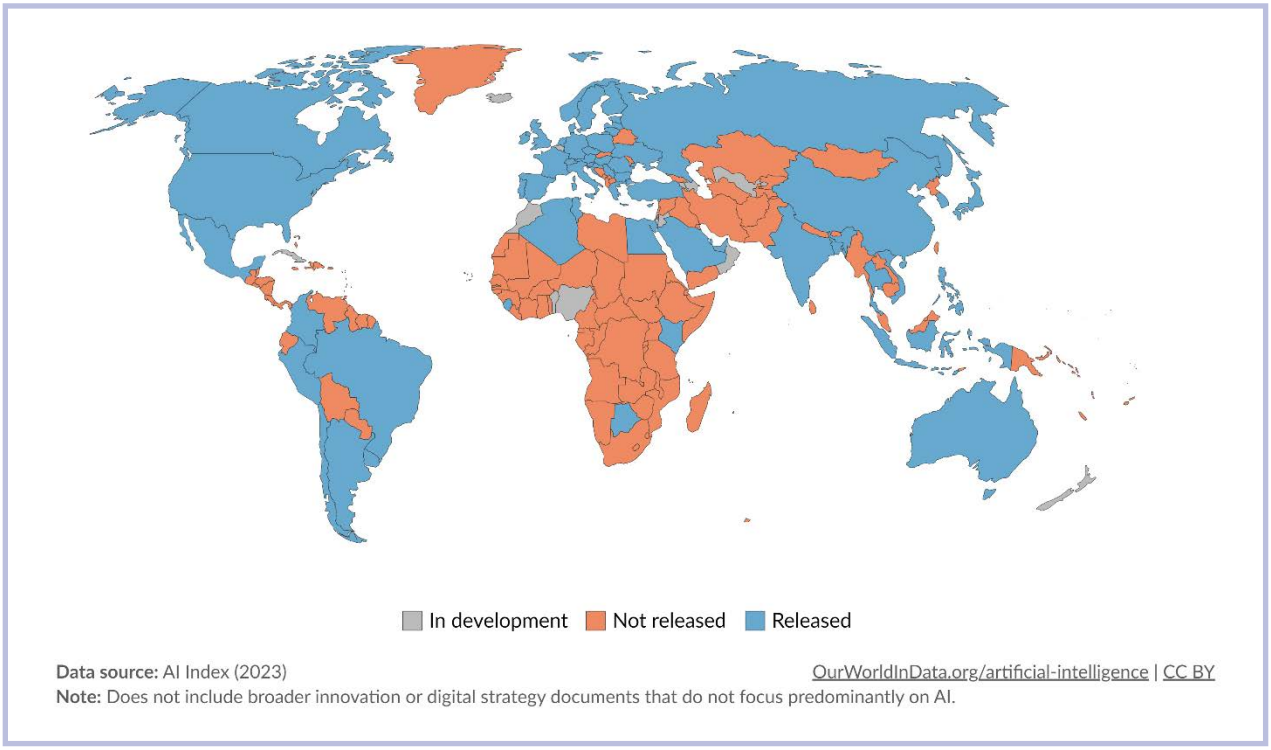


Figure 3: **World Map Showing States that have Implemented National AI Strategies (as of 2022)**

An AI strategy is a policy document that communicates the objective of supporting the development of AI while also maximizing the benefits of AI for society.



Source: Our World in Data[17]

One such example is the case of the International Atomic Energy Agency (IAEA), an intergovernmental body, which functions autonomously towards increasing the peaceful use of nuclear technology. The body was established to tackle the rising tensions among the then-existing nuclear powers.[18] But in the current scenario, not just two or three but multiple countries are aiming for supremacy in AI technology which accentuates the need for an international regime, a supranational entity governing AI and its usages. The agency thus created can be entitled to regulate and curb the hostile usage of AI and all the states could comply with a commonly agreed safeguard mechanism, much like the IAEA. Furthermore, while enabling development in AI for peaceful purposes, it should oversee how the armed forces are utilizing and deploying it through regular inspections. Such an organization, if established, can be an Attaché to the United Nations General Assembly and Security Council.

In addition to the regulation of AI applications, and large language models, there is a need to secure the supply chain networks powering the development and operationalization of these technologies. In this regard, India, during its G20 presidency summit highlighted the grouping's intentions toward an effective and equitable global regulation of AI.[19] Additionally, in December 2023, India also led and hosted the Global Partnership of Artificial Intelligence (GPAI), during which the need for securing technologies such as semiconductors and graphics processing units was discussed.[20] Platforms such as G20 and GPAI encourage responsibility by the members to develop and deploy trustworthy, safe, and secure AI.[21] However, the onus is on the member-states

to ensure compliance with such declarations and frameworks.

Assurance of data security is a crucial link for enabling individuals, the private sector, and governments to seamlessly use digital infrastructure. The increasing geopolitical tensions, cybercriminals, and state-sponsored attacks undermine the trust in these systems and technologies. Hence, to ensure the security of data, the use of data embassies is one solution. Data embassies are data centers situated outside the territory enabling them to operate even in case of crises such as cyberattacks or military invasions.[22] In 2016, Estonia became the first country to establish its data embassy by signing an agreement with Luxembourg to safeguard threats to its data sovereignty. The Estonian Data Embassy holds critical servers and data of the government including land registry, business registry, and treasury information systems. The choice of Luxembourg also highlights the key aspect of diplomatic relations of both the home and host nations.[23] While there are debates on the potential use of AI to fuel distrust between states, the data embassies of Estonia and Monaco stand as examples of how strong diplomatic relations can help states overcome threats that challenge their sovereignty and security while ensuring the continuity of critical services.[24]

"While adopting AI in industry and business is a positive from the financial standpoint, the lack of transparency in the use of personal data and sensitive information collected by these businesses, without formal consent, raises a red flag about privacy.

"The sphere of AI and emerging technologies is beyond physical and geographical boundaries, making a standard and universal regulation desirable. However, the materialization of such a framework faces challenges as the field by its nature is fast developing and very little is understood by all players.

The sphere of AI and emerging technologies is beyond physical and geographical boundaries, making a standard and universal regulation desirable. However, the materialization of such a framework faces challenges as the field by its nature is fast developing and very little is understood by all players. The geopolitical challenges, great power tensions, and competition between players at higher stages of development make it difficult to arrive at an all-encompassing agreement. Political differences within a region and around the world could hamper the development of a consensus-based framework as evident in the case of the European Union (EU).[25] The EU had to face multiple roadblocks while enacting the EU AI Act as it was not an easy task to get all the member-states on board for an effective governance mechanism.[26] Another major issue is that AI has been researched by several states, which are at different stages of development. In such scenarios, reducing the technology gap would be given a preference over the constraining regulations. Another example of collaborative effort is the Bletchley Declaration on AI safety, which includes 28 states from across the globe, including Africa and the Middle East.[27] The Declaration signed at the AI Safety Summit 2023 aims at collectively managing risks and ensuring secure AI deployment.[28] A global

effort hailed by many due to the participation of a wide spectrum of stakeholders from developing countries to individuals leading AI development, the Declaration could not resolve disagreements on how to regulate AI and who should be leading the initiative despite establishing a consensus on the need for it.[29]

Despite such challenges, there is a need for collective participation in the efforts to have global AI governance since the technology if left unregulated could have negative impacts. The negative outcomes due to the lack of an effective framework could lead to a deepening of inequality, privacy loss, and ethical concerns at individual and societal levels. With discussions around AI being a catalyst for the next industrial revolution, there is a need to look back at the socioeconomic and political implications of the previous instances. With these technologies touted to bring new norms of development, it is necessary to adopt an inclusive approach to ensure that the developing states, lower and middle-income countries, and the Small Island Developing States have equitable access to these innovations.

Authors –

Kiran Bhatt *is a Research Fellow at the Centre for Health Diplomacy, Department of Global Health Governance, Prasanna School of Public Health, Manipal Academy of Higher Education (MAHE), at Manipal in Karnataka, India.*

Aniruddha Inamdar *is a Research Fellow at the Centre for Health Diplomacy, Department of Global Health Governance, Prasanna School of Public Health, Manipal Academy of Higher Education (MAHE) at Manipal in Karnataka, India.*

Prof Dr Sanjay Pattanshetty *is Head of the Department of Global Health Governance and Coordinator - Centre for Health Diplomacy at Prasanna School of Public Health Manipal Academy of Higher Education (MAHE), at Manipal in Karnataka, India. Additionally, he has an affiliation with the Department of International Health Care and Public Health Research Institute (CAPHRI) Faculty of Health Medicine and Life Sciences, Maastricht University in Maastricht, The Netherlands as an External PhD candidate.*

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

Endnotes

1 Ricardo Vinuesa, Hossein Azizpour, Iolanda Leite, Madeline Balaam, Virginia Dignum, Sami Domisch, Anna Felländer, Simone Daniela Langhans, Max Tegmark, and Francesco Fuso Nerini, "The role of artificial intelligence in achieving the Sustainable Development Goals," *Nature Communications* 11, no. 1 (2020): 1-10.

2 Dow Jones Risk & Compliance, "What are Dual-Use Goods?," Dow Jones, https://www.dowjones.com/professional/risk/glossary/dual-use-goods-definition/#:~:text=Dual%2Duse%20guse.s%20are%20items,or%20worse%2C%20used%20for%20terrorism

3 World Economic Forum, "Why we need to regulate non-state use of arms," May 18, 2022, https://www.weforum.org/agenda/2022/05/regulate-non-state-use-arms/.

4 Council on Foreign Affairs, "Estonian denial of service incident," Cyber Operations, Council on Foreign Affairs, May 2007, https://www.cfr.org/cyber-operations/estonian-denial-service-incident.

5 Patrick Howell O'Neill, "The cyberattack that changed the world," Daily Dot, May 20, 2016, https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/.

6 Entrustech Inc, "Data as a Strategic Weapon: How AI and ML Can Help You Gain a Competitive Advantage," Medium, October 25, 2023, https://medium.com/@entrustech/data-as-a-strategic-weapon-how-ai-and-ml-can-help-you-gain-a-competitive-advantage-5da018bdea05.

7 SingleStore, "AI's Secret Weapon: The Data Corpus," June 6, 2017, https://www.singlestore.com/blog/ai-secret-weapon-the-data-corpus/.

8 Center for Security and Emerging Technology (2023) – processed by Our World in Data, "Banking and finance," https://ourworldindata.org/grapher/artificial-intelligence-granted-patents-by-industry.

9 Abdulmohsen Almalawi, et al., "Managing Security of Healthcare Data for a Modern Healthcare System," *Sensors, MDPI, March 30, 2023, https://www.mdpi.com/1424-8220/23/7/3612.*

10 Mark van Rijmenam, "Privacy in the Age of AI: Risks, Challenges And Solutions," The Digital Speaker, February 17, 2023, https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/.

11 Deloitte, "A call for transparency and responsibility in Artificial Intelligence," Deloitte Netherlands, 2019, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovation-bringing-transparency-and-ethics-into-ai.pdf?ref=thedigitalspeaker.com.

12 Jose Ramon Saura, et al., "Assessing behavioral data science privacy issues in government artificial intelligence deployment," Government Information Quarterly, October 4, 2022, https://doi.org/10.1016/j.giq.2022.101679.

13 Edmund Ofosu Benefo, et al., "Ethical, legal, social, and economic (ELSE) implications of artificial intelligence at a global level: a scientometrics approach," *AI and Ethics* 2 (2022): 667-682, https://doi.org/10.1007/s43681-021-00124-6.

14 AI Advisory Body, "UN AI Advisory Body calls for grounding artificial intelligence in universal principles, suggests tasks for a potential institution on AI governance [Press Release]," UN Advisory Body on Artificial Intelligence (AI), December 21, 2023, https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_interim_report_press_release.pdf.

15 Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world," The Brookings Institution, April 24, 2018, https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/.

16 UNIDIR, "The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations," UNIDIR Resources, 2017, https://unidir.org/files/publication/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf.

17 Charlie Giattino, et al., "Artificial Intelligence," Our World in Data, 2023, https://ourworldindata.org/grapher/national-strategies-on-artificial-intelligence.

18 IAEA, "History," International Atomic Energy Agency, https://www.iaea.org/about/overview/history.

19 "G20 leaders call for global governance for AI, inclusive digital public infra for service delivery," *The Economic Times*, September 10, 2023, https://telecom.economictimes.indiatimes.com/news/policy/us-fcc-chair-says-chinas-quectel-fibocom-may-pose-national-security-risks/103448336.

20 Ministry of Electronics & IT, "Three-Day GPAI Summit concluded today at Bharat Mandapam! - India Shines as Global Hub for AI Innovation," PIB Delhi, December 14, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1986475#:~:text=India%2C%20the%20Chair%20of%20the,Bharat%20Mandapam%20in%20New%20Delhi.

21 Arvind Gupta, et al., "AI governance outlook: A Global South perspective," Observer Research Foundation, January 4, 2024, https://www.orfonline.org/expert-speak/ai-governance-outlook-a-global-south-perspective.

22 Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Cooperative Cyber Defence Centre of Excellence, 2018, https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

23 Arindrajit Basu, "How data embassies can promote data security for all," Datasphere Initiative, July 20, 2023, https://www.thedatasphere.org/news/how-data-embassies-promote-data-security-for-all/.

24 Yuliya Talmazan, "Data security meets diplomacy: Why Estonia is storing its data in Luxembourg," *NBC News*, June 25, 2019, https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171.

25 Thorsten Ammann and Constantin Orth, "EU AI Act Update - Latest developments and potential roadblocks ahead," DLA Piper, November 29, 2023, https://www.lexology.com/library/detail.aspx?g=98821b9c-f97c-40c4-b2b1-362177771e76; Jedidiah Bracy, "After unexpected roadblock, AI Act negotiations move forward under pressure," International Association of Privacy Professionals (iapp), November 15, 2023, https://iapp.org/news/a/after-unexpected-roadblock-ai-act-negotiations-move-forward-under-pressure/.

26 "Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world [Press Release]," Council of the EU and the European Council, December 9, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/.

27 "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023," AI Safety Summit 2023, Gov.UK, November 1, 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

28 Prime Minister's Office, "AI Safety Summit 2023: Chair's statement – safety testing, 2 November," AI Safety Summit 2023, Gov.UK, November 2, 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-chairs-statement-safety-testing-2-november.

29 Martin Coulter and Paul Sandle, "AI summit a start but global agreement a distant hope," *Reuters*, November 6, 2023, https://www.reuters.com/technology/ai-summit-start-global-agreement-distant-hope-2023-11-03/.