



POLICY REPORT · 2026

Artificial Intelligence *and* Cybersecurity

*Systemic risks, governance and pathways
towards a strategic cooperation between Brazil and the United Kingdom*

TURING CLUB · BRAZIL CHAPTER

British Embassy · Brasília

12 March 2026

Disclaimer



This report is a synthesis of the open discussions held during the Turing Club · Brazil Chapter seminar. The document reflects the diversity of perspectives, themes and possible areas for future dialogue raised by participants from different sectors.

The views and opinions expressed herein correspond to the individual contributions of the participants in the dialogue and do not reflect the institutional position of the government bodies, companies, universities or other organisations eventually mentioned or represented by the participants.

It should not be interpreted as a UK Government policy statement, as a formal UK Government proposal, or as a commitment by the UK Government or any other participant to specific positions, recommendations, programmes or forms of future cooperation.

References to United Kingdom institutions, publications or experiences are included solely for contextualisation, comparison and exchange of experiences.

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME (INCC)

Artificial Intelligence and Cybersecurity: systemic risks, governance and pathways towards a strategic cooperation between Brazil and the United Kingdom. Brasília ; São Paulo : INCC, 2026.

32 p. : col. ill.

Report produced by the Instituto Nacional de Combate ao Cibercrime (INCC) under the Turing Club · Brazil Chapter, an initiative supported by the UK Government in cooperation with INCC.

1. Artificial Intelligence. 2. Cybersecurity. 3. Digital governance. 4. Brazil, United Kingdom cooperation. I. Title.

Contents

1. Executive Summary	3
2. Introduction: architecture of the debate and strategic relevance	5
3. Artificial Intelligence and the reconfiguration of the threat ecosystem	7
4. The dual nature of AI: risk amplification and defensive potential	10
5. Disinformation, AI and the fragility of democratic trust	13
6. The impact of deepfake technology and institutional responses	14
7. Brazil: institutional coordination, normative framework and challenges	16
8. International governance of AI and cybersecurity	19
9. Cooperation between Brazil and the United Kingdom: a strategic agenda	22
10. Strategic areas for Brazil and cooperation opportunities	25
10.1 Pathways towards integrated governance	26
10.2 Regulatory integration between AI and cybersecurity	27
10.3 Building AI and cybersecurity skills	28
10.4 AI applications for critical infrastructure resilience	29
10.5 Threat intelligence sharing	30
10.6 Centrality of information integrity	31
10.7 A structured Brazil and United Kingdom cooperation agenda	31
10.8 Security standards and certifications	32
11. Conclusion	33
References	35

1. Executive Summary

The convergence of artificial intelligence (AI) and cybersecurity marks a structural transformation of the global digital environment, reshaping the nature of risks, the dynamics between offensive and defensive actors, and the foundations of technology governance.

Unlike previous cycles of innovation, AI not only expands existing capabilities: it also lowers the technical barriers required to launch sophisticated attacks, accelerates vulnerability exploitation and increases the scale of malicious operations. This shift takes place against a backdrop of growing dependence on critical digital infrastructure and intensifying technological competition among States.

The *Global Risks Report 2025*, published by the World Economic Forum (2025), identifies disinformation and cyberattacks among the leading short-term global risks. Convergently, the *National Cyber Security Centre* assessment of the impact of AI on the cyber threat to 2027 (NCSC, 2025a) projects an increase in both the volume and the impact of intrusions, as the technology enhances existing tactics, techniques and procedures.

In Brazil, this landscape unfolds within an institutional environment in evolution, marked by significant progress, including the Lei Geral de Proteção de Dados (LGPD, Brazilian General Data Protection Law), the Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet), the Estratégia Brasileira de Inteligência Artificial (EBIA, Brazilian AI Strategy) and the Estratégia Nacional de Segurança Cibernética (E-Ciber, National Cybersecurity Strategy), alongside the continued strengthening of coordination, implementation and capacity building.

In parallel, the country is entering a significant phase of normative consolidation, reflected in the passage of the AI Regulation Bill through the National Congress and of the Cybersecurity Legal Framework through the Federal Senate. These legislative debates point to potential structural adjustments in Brazilian digital governance, whose implementation offers opportunities to broaden the integration of the different instruments and actors involved.

The launch of the Turing Club · Brazil Chapter, an initiative supported by the UK Government, highlighted that the risks associated with AI transcend the technical dimension and directly affect information integrity, institutional resilience and trust in democratic systems.

Early conversations also revealed a shared perception that, in the short term, AI is likely to enhance the capabilities of malicious actors, reinforcing the importance of approaches oriented towards risk anticipation, prevention and the development of adaptive governance models, in line with ongoing international debates.

Key messages

- AI lowers the technical barriers for offensive operations and expands the scale of disinformation campaigns, reinforcing the need for adaptive governance.

- Brazil has a robust regulatory and strategic framework in AI and cybersecurity, with opportunities to promote greater integration among the initiatives and instruments in development.
- The Brazil, United Kingdom cooperation offers space for the co-creation of good practices, anchored in United Kingdom expertise, including the NCSC and the *AI Security Institute* (AISI).
- Information integrity emerges as a form of critical infrastructure and deserves integrated strategic treatment.

Global context · numbers that frame the agenda

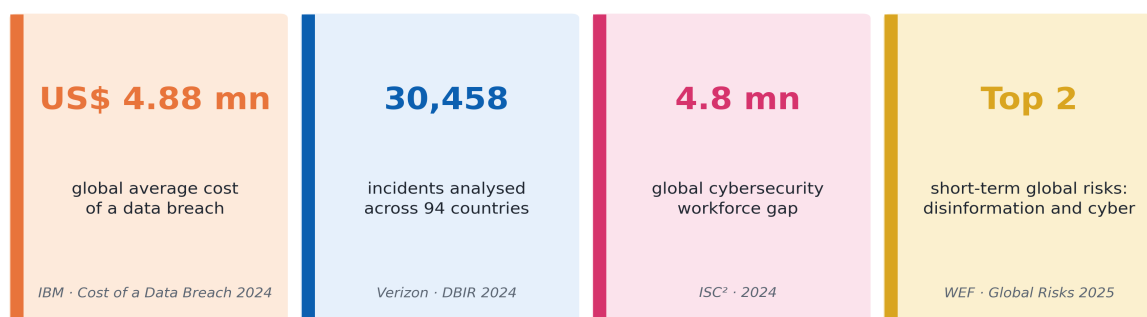


Figure 1: Global context of the cybersecurity and AI agenda. Sources: IBM Cost of a Data Breach 2024, Verizon DBIR 2024, ISC² 2024, WEF Global Risks 2025.

2. Introduction: architecture of the debate and strategic relevance

The Turing Club · Brazil Chapter was conceived as a high-level multi-stakeholder space for strategic discussion at the interface of emerging technologies, including artificial intelligence, cybersecurity and intellectual property, with the aim of bringing distinct institutional perspectives together and fostering common agendas between Brazil and the United Kingdom.

Held at the British Embassy in Brasília, the first meeting brought together representatives working on public policy formulation, academic research and the operation of critical systems. The plural composition, with contributions from government, diplomacy, the private sector and academia, articulated through specialised moderation, allowed for a multidimensional analysis of the challenges linked to the convergence of AI and cybersecurity.



Photo: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Image 1: Opening of the Turing Club · Brazil Chapter. British Embassy, Brasília, 12 March 2026.

The debate brought together Guilherme Fitzgibbon, Special Adviser at the Ministry of Foreign Affairs with experience in the international governance of emerging technologies, including AI, and a Chevening¹ alumnus; Danielle Ayres, representative of the Institutional Security Office (GSI), with a focus on information security and public policy coordination; Alexandre Cardoso, from British Telecom, bringing to the debate an operational perspective of a multinational group active in markets with different levels of digital maturity; and Dr Beatriz Buarque, from the London School of Economics, whose contribution centred on the ethical, social and political dimensions of artificial intelligence.

The discussion was moderated by Eduardo Paranhos, a specialist in digital law, artificial intelligence and governance, who leads the AI working group at the Associação Brasileira das Empresas de Software (ABES, Brazilian Software Companies Association) and coordinates the regulation strand of the Brazilian AI Strategy.

The dynamics of the meeting, structured around guiding questions and short interventions, favoured a fluid and interactive debate, allowing different perspectives to emerge and enabling the identification of relevant convergences and divergences.

The approach adopted favoured an in-depth and analytical discussion. The reflections indicated that the convergence of artificial intelligence and cybersecurity does not present itself as an isolated or sectoral challenge, but rather as a systemic issue that involves technical, institutional,

¹Chevening: the UK Government international scholarships programme aimed at emerging leaders from over 160 countries, with an active alumni network in Brazil, particularly in public policy, diplomacy and technology.

economic and geopolitical dimensions, thereby reinforcing the need for coordinated and multidisciplinary responses.

The plural composition of the group enabled a comprehensive analysis of the challenges linked to the convergence of AI and cybersecurity. The dialogue incorporated institutional, academic and operational perspectives, covering issues ranging from coordination and capacity building in the public sector to ethical, social and democratic implications, as well as the practical challenges faced by organisations operating in complex digital environments.

CONTEXT

About the Turing Club · Brazil Chapter

Inspired by Alan Turing and the United Kingdom tradition of computational intelligence, the Turing Club · Brazil Chapter materialises, in a bilateral format, the exploratory and collaborative character proposed by the UK Government for the international dialogue on AI. The initiative seeks to facilitate the exchange of good practices and the co-creation of common agendas between Brazil and the United Kingdom, in line with international efforts on digital governance and security.

3. Artificial Intelligence and the reconfiguration of the threat ecosystem

Artificial intelligence is driving a qualitative transformation of the cyber threat ecosystem, altering not only the scale but also the nature of the risks faced by States, companies and individuals. Unlike previous cycles of technological innovation, in which attack sophistication was directly linked to the technical expertise of the actors involved, AI tends to lower that barrier, enabling actors with less technical knowledge to carry out complex operations. This assessment is supported by Parihar (2025), who analyses how AI systems applied to cybersecurity alter both detection and response mechanisms and observed attack patterns.

Throughout the Turing Club discussions, academic contributions noted that AI tools allow, through seemingly simple interactions, access to sensitive operational knowledge, including means of exploiting vulnerabilities or developing illicit artefacts. During the debate, this phenomenon was described as a democratisation of technological risk, in which specialised knowledge ceases to be a limiting factor for malicious action.

Ecosystem of AI-amplified threats

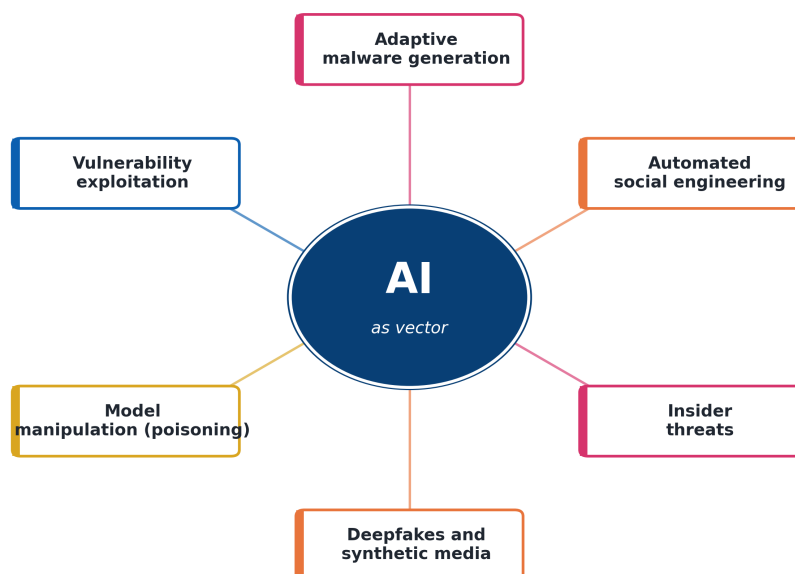


Figure 2: The ecosystem of AI-amplified threats. Original elaboration drawing on the Turing Club discussions.

This reading echoes the assessment by the *National Cyber Security Centre*² (NCSC, 2025a) on the impact of AI on the cyber threat to 2027, according to which, in the short term, only highly capable State actors will be able to fully exploit the offensive potential of AI, even though the proliferation of AI-enabled tools tends to broaden access to such capabilities to a wider range of actors. Complementing this threat assessment, the *Code of Practice for the Cyber Security of AI*³, published by the *Department for Science, Innovation and Technology* of the United Kingdom (DSIT, 2025a), sets baseline security principles applicable throughout the life cycle of AI systems.

The international literature confirms this trend. As Bisht (2024) demonstrates in his analysis of the *Data Breach Investigations Report 2024* from Verizon, the study examined 30,458 security incidents across 94 countries, with 10,626 confirmed breaches, evidencing the scale and recurrence of the threats. Complementarily, the *Cost of a Data Breach 2024* published by IBM (2024) reports that the average global cost of a breach reached US\$ 4.88 million, reflecting not only the frequency of attacks but also their growing economic impact.

In the Brazilian context, data consolidated by the Instituto Nacional de Combate ao Cibercrime (INCC) and by sectoral reports indicate a consistent increase in the sophistication of digital attacks, particularly in financial fraud and social engineering. The incorporation of AI in these processes

²NCSC (National Cyber Security Centre): the United Kingdom body responsible for national cybersecurity, created in 2016 as the public arm of GCHQ. Publishes guidance, threat assessments and technical guidelines for public and private sectors in the United Kingdom.

³Code of Practice for the Cyber Security of AI (DSIT, 2025): voluntary code of practice created by the Department for Science, Innovation and Technology (United Kingdom) together with the NCSC. Its scope covers the entire life cycle of AI systems, from design to decommissioning, and it served as the basis for the technical specification ETSI TS 104 223, an emerging international reference.

expands their efficiency, allowing the automation of attacks at scale, the personalisation of approaches and faster vulnerability exploitation.

Contributions from private-sector organisations highlighted that this transformation manifests itself in the corporate environment, particularly in the challenges linked to incident management and the protection of critical infrastructure. Episodes involving insider threats, such as attempts by employees to compromise systems, evidence that the attack surface is not limited to external actors. AI amplifies this risk by facilitating credential exploitation, automating internal processes and bypassing security mechanisms.

This scenario suggests a partial inversion of the traditional cybersecurity logic. Historically, defenders benefited from asymmetry, requiring attackers to find a specific vulnerability, while defenders could rely on multiple layers of protection. With AI, this asymmetry tends to narrow, favouring offensive actors who can test multiple vulnerabilities simultaneously and adapt their strategies in real time.

The direct implication for public policy and organisational strategies is the need to migrate from reactive to predictive and preventive models. Concepts such as *security by design*, *zero trust architecture* and continuous monitoring⁴ cease to be desirable good practices and become fundamental requirements for digital resilience, as evidenced both by Parihar (2025) in the academic literature and by the NCSC (2023) guidelines for the secure development of AI systems.

From reactive response to predictive defence · institutional cybersecurity maturity

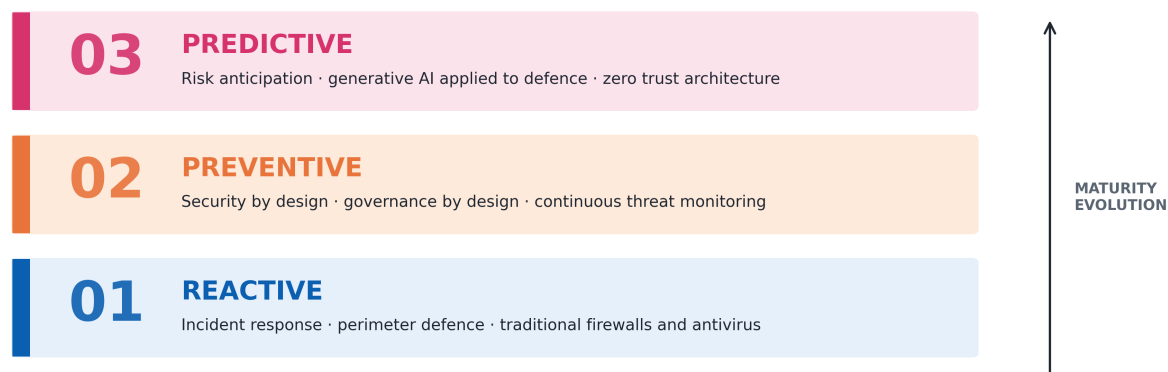


Figure 3: Institutional cybersecurity maturity: from reactive to predictive models.

⁴Security by design: incorporation of security requirements from the design stage of systems. Zero trust architecture: principle that assumes no implicit trust among devices and users, requiring continuous verification. Continuous monitoring: permanent collection and analysis of events for rapid incident detection and response (NCSC, 2023).

4. The dual nature of Artificial Intelligence: risk amplification and defensive potential

One of the central threads of the debate was the dual nature of artificial intelligence in cybersecurity: the same technology that enhances attacks can simultaneously strengthen defensive mechanisms. At the Turing Club, contributions from governmental and diplomatic perspectives underscored that AI-based defensive capability depends directly on the level of institutional and technological maturity of countries. This reading converges with the analysis by Akhtar et al. (2021), which examines the use of AI as a dual-use capability in cybersecurity, at times amplifying defensive potential and at others sophisticating offensive tools.

The dual nature of AI · simultaneously risk vector and defensive capability

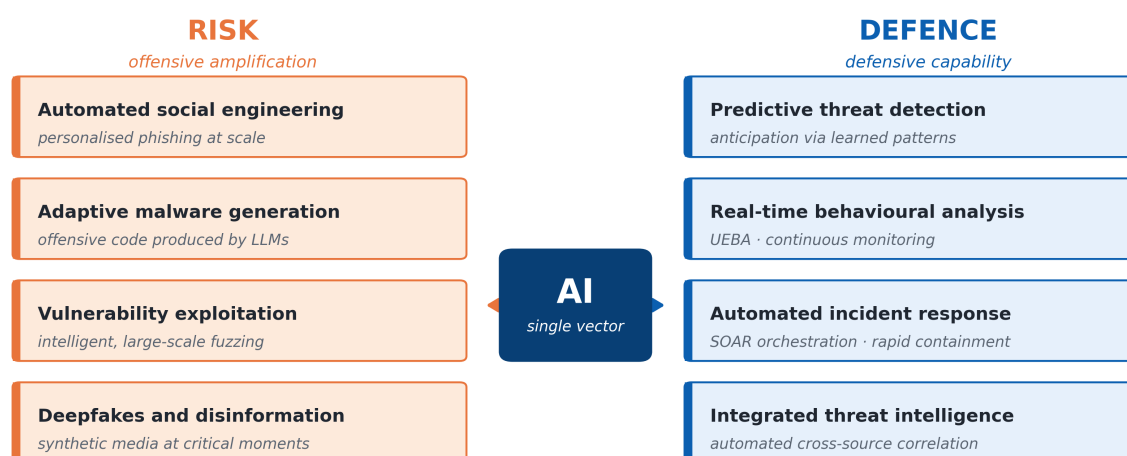


Figure 4: The dual nature of AI: risk vectors and defensive capabilities coexist within the same set of technologies.

In contexts where there is investment in infrastructure, workforce qualification and the development of proprietary solutions, AI can represent a significant advance in incident detection and response capability. In the absence of these conditions, however, the technology tends to widen vulnerabilities, leaving States and organisations more exposed to sophisticated attacks.

This asymmetry is a central element of the contemporary debate on digital security. While offensive actors can concentrate their efforts exclusively on vulnerability exploitation, defensive actors must balance multiple dimensions, including systems protection, operational continuity, regulatory compliance and user experience.

During the Turing Club discussions, it was noted from the governmental perspective that the development of AI-based solutions for legitimate use requires their creators to consider, simultaneously, the potential for misuse. This alignment between debate and literature is reinforced

by the study by Radanliev et al. (2024), which examines security frameworks for the development of AI solutions applied to cybersecurity. This need for anticipation, incorporating risks from the design stage, reinforces the importance of approaches such as *safety by design* and *governance by design*⁵, which integrate security and governance considerations into the life cycle of technologies.

International references illustrate the practical operation of this principle. The Cabinet Office (2025) of the United Kingdom, through the *Mitigating Hidden AI Risks Toolkit*, offers a step-by-step model for identifying, monitoring and mitigating behavioural and organisational risks associated with AI adoption. Complementarily, DSIT (2025a), in the *AI Cyber Security Code of Practice*, establishes security principles applicable throughout the life cycle of AI systems, from design to decommissioning. The *AI Security Institute* (AISI, 2025), a United Kingdom public institution working on research and assessment of systemic AI risks, further reinforces the UK Government intent to treat AI security as a primary matter of public policy.

The perspective brought by the private sector during the meeting evidenced that even organisations with advanced security structures face significant challenges in implementing AI-based defence systems. The need to balance automation and control, avoid false positives and guarantee operational continuity makes this process complex and highly dependent on governance and institutional maturity.

In this context, the analysis suggests that artificial intelligence is not inherently either a risk vector or a means of protection. Its effects depend largely on the quality of governance arrangements, the level of institutional maturity and the degree of integration among public policies. Different levels of development of these capabilities can result in asymmetric impacts, both in terms of benefits and of risks associated with the adoption of the technology.

UK REFERENCE

Featured UK references

- **NCSC, *Guidelines for secure AI system development* (2023)**: principles for designing, developing, deploying and operating AI systems with security from the outset.
- **DSIT, *AI Cyber Security Code of Practice* (2025)**: the first voluntary code of practice focused on the cybersecurity of AI systems, with an internationalised version through ETSI TS 104 223.
- **Cabinet Office, *Mitigating Hidden AI Risks Toolkit* (2025)**: practical guidance for mitigating the behavioural and organisational risks arising from AI adoption.
- **AI Security Institute (AISI, 2025)**: public institution dedicated to advancing the scientific evidence base on the most serious AI risks.

⁵Safety by design: incorporation of user safety considerations and harm mitigation from the design of the system. Governance by design: analogous principle applied to governance, with prior definition of rules, roles and oversight mechanisms from the architecture of the technology.

5. Disinformation, AI and the fragility of democratic trust

The relationship between artificial intelligence and disinformation was one of the most sensitive and strategic topics of the debate, showing that the risks associated with AI extend beyond the technical dimension and reach the core of institutional and democratic stability.

The ability to generate highly convincing synthetic content, including audio, video and text, raises concerns about the manipulation of information and the erosion of public trust in institutions and media platforms. The United Kingdom has treated this issue as a political priority: the guidance on artificial intelligence (2024) and the NCSC (2025b) note on preserving integrity in the generative AI era underline that the proliferation of these systems amplifies the loss of trust in data and media and intensifies reputational and social engineering risks.

The perception of risks and trust in AI technologies are fundamental to their social acceptance. As Gerlich (2023) points out, this dimension is also highlighted by the European Commission trustworthy AI principles, which emphasise security and responsible governance. The review by Lockey et al. (2021) on trust in AI systems, in turn, indicates that building this trust depends on adequate mechanisms of governance, transparency and risk management, as well as on consideration of the vulnerabilities and expectations of different stakeholders.

In keeping with this perspective, the *Trusted Third-Party AI Assurance Roadmap*, published by DSIT (2025b) in September 2025, proposes quality assurance models for AI systems and seeks to structure a UK AI assurance ecosystem that may serve as an international reference.

Trust can be compromised by factors such as the opacity of algorithms and limited accountability in their implementation, aspects that require careful reflection on the impact of AI on disinformation and social stability.

Reinforcing this scenario, the *Global Risks Report 2025*, published by the World Economic Forum (2025), positions disinformation and cyberattacks among the leading short-term global risks, underscoring their potential to impact democratic processes and generate social instability.

6. The impact of deepfake technology and institutional responses



Photo: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Image 2: Audience engaged with contributions on information integrity and deepfakes (synthetic media) during the Turing Club.

Deepfake technologies and generative models enable the creation of false narratives with a high degree of verisimilitude, making it harder to distinguish legitimate information from manipulated content. This phenomenon carries profound implications for the integrity of circulating information.

Academic perspectives shared during the debate, including those anchored in the United Kingdom tradition of research on risk and democracy, illustrated scenarios in which synthetic content may be disseminated at critical moments, such as electoral periods or institutional crises.

The academic literature corroborates these concerns raised in the debate: the study by Pandey (2025), entitled "AI's Dark Side: The Rise of Deepfakes and the Battle for Truth", analyses how the proliferation of *deepfakes* is intensifying the challenges of public opinion manipulation and the erosion of trust in information ecosystems, offering independent academic evidence to the qualitative accounts presented by participants.

The difficulty of verifying content authenticity in real time can compromise the response capacity of governments and public trust in institutions. This challenge is widely recognised in international analyses. The NCSC (2024), in the *Artificial Intelligence* section of its portal, organises guidance and warnings for managers and decision-makers, explicitly highlighting media manipulation for *deepfake* campaigns as a growing risk vector. Complementarily, NCSC (2025c), through the *Defending Democracy* collection, consolidates guidance for high-risk individuals and organisations responsible for elections.

In the Brazilian context, this discussion connects directly with the Marco Civil da Internet (Law 12,965/2014), which establishes principles for internet use, and with ongoing regulatory debates on the responsibility of digital platforms. The growing sophistication of AI technologies invites an update of these discussions, incorporating new risk vectors and mitigation mechanisms.

FOR REFLECTION

A particularly relevant point of the debate

Democracy can be treated as a form of critical infrastructure. As with energy, telecommunications and financial systems, the information environment is essential to the functioning of the State and society, being therefore vulnerable to attacks and demanding structured protection.

This diagnosis, formulated during the debate, points to the importance of integrated approaches that combine cybersecurity, institutional communication, digital education and platform regulation. It resonates with the academic literature: Modupeola et al. (2025), by proposing an index for *deepfake* detection and cybersecurity, demonstrate how the coordination between these domains contributes to mitigating information risks while preserving fundamental rights and trust in the digital environment.

7. Brazil: institutional coordination, normative framework and implementation challenges

Brazil does not start from an institutional vacuum with regard to digital governance. On the contrary, over the past decade the country has built a relevant set of normative and strategic instruments focused on internet regulation, data protection, digital transformation and information security. As evidenced throughout the debate, the central challenge lies less in the absence of policies and more in the opportunities for articulation and implementation among them. This reading converges with the analysis by Nicolás and Sampaio (2024) on the impact of AI automation on public policy in Brazil, which also identifies coordination challenges as a central element of the Brazilian agenda.

Timeline · Brazilian regulatory framework for AI and cybersecurity

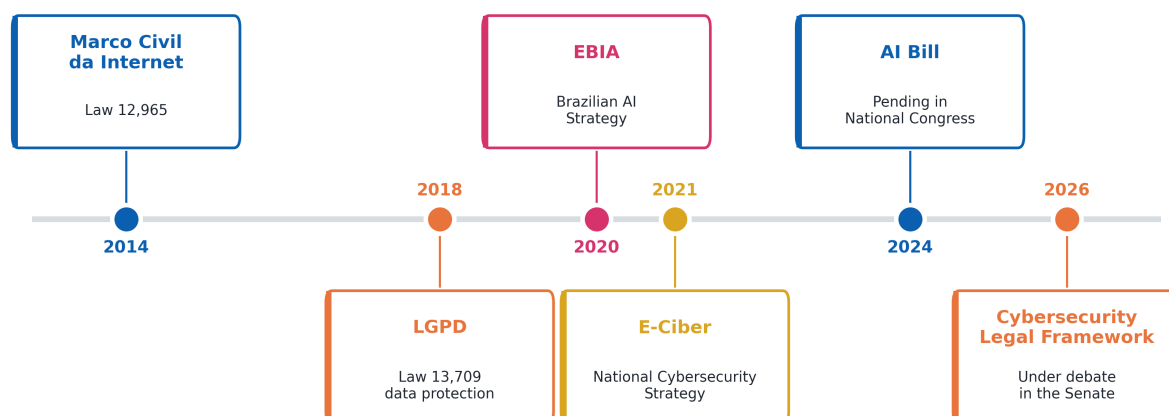


Figure 5: Timeline of the Brazilian regulatory framework for AI and cybersecurity (2014-2026).

The Marco Civil da Internet (Law 12,965/2014) established fundamental principles for internet use in Brazil, including protection of freedom of expression, net neutrality and the responsibility of actors involved in the digital ecosystem. Subsequently, the Lei Geral de Proteção de Dados Pessoais (Law 13,709/2018) introduced a comprehensive regulatory framework for data processing, aligning the country with international privacy protection standards. Bioni, Garrote and Guedes (2023), in their study on regulatory interoperability, show how this Brazilian framework articulates with local, regional and global regulatory movements on AI.

More recently, the Brazilian federal government advanced in the design of specific strategies for artificial intelligence and cybersecurity. The Brazilian AI Strategy (EBIA), instituted by the Ministry of Science, Technology and Innovation, sets guidelines for the development and ethical use of AI in the Brazilian context, with a focus on innovation, competitiveness and inclusion. In parallel, the National Cybersecurity Strategy (E-Ciber), part of the National Information Security Policy (PNSI), establishes objectives to strengthen the country resilience against digital threats.

AI and cybersecurity governance in Brazil

In light of this framework, the Turing Club discussions suggested that the different initiatives underway in Brazil are at distinct stages of development and articulation. It was noted during the dialogue that one of the recurrent challenges in the public debate concerns the articulation among multiple agendas, including artificial intelligence, cybersecurity, data protection and digital transformation, that evolve in parallel within the State.

The need for greater alignment among these domains takes on particular relevance now, given the passage of structuring legislative proposals. The AI Regulation Bill, currently under discussion in the National Congress, aims to establish principles, rights and duties for the development and use of AI in the country, including provisions on risk classification and the attribution of responsibilities, dimensions that the work of Cavalcante (2024), published by the Blavatnik School of Government

(Oxford), analyses under the lens of algorithmic *accountability*. In parallel, the Cybersecurity Legal Framework, under debate in the Federal Senate, is intended to consolidate guidelines for the protection of critical infrastructure, incident response and coordination among different actors, a topic addressed by Krasodonski et al. (2024) in their essay collection on responsible global AI governance.

An aspect highlighted during the debate was the importance of promoting articulation among the different initiatives under development in the areas of artificial intelligence and cybersecurity. As these normative frameworks advance, opportunities for alignment among regulatory instruments, public policies and governance structures can contribute to greater coherence and effectiveness in their implementation.

FOR REFLECTION

Legislative window: the importance of articulation

- **AI Bill:** risk classification, duties of actors and supervision.
- **Cybersecurity Legal Framework:** protection of critical infrastructure, incident response, coordination.
- **LGPD / ANPD:** personal data protection and data processing governance.
- **UK reference:** DSIT (2025c) introduced, in November 2025, the *Cyber Security and Resilience Bill*⁶, an instrument that illustrates how a broad update to the Network and Information Systems (NIS)⁷ regime can bring the agendas of digital security, AI and critical infrastructure closer together within a single legal instrument.

Beyond the normative dimension, the debate highlighted structural challenges linked to State capacity. The shortage of qualified cybersecurity professionals is one of the main bottlenecks. Data from the International Information System Security Certification Consortium (ISC2, 2024) indicate a global shortfall of approximately 4.8 million professionals in the field, a scenario that is felt particularly acutely in developing countries.

In Brazil, analyses produced by INCC indicate that the difficulty of retaining talent in the public sector undermines the capacity for policy implementation and incident response. Differences in remuneration compared with the private sector, combined with the rapid pace of technological change, tend to create additional pressures on the public sector's ability to attract and retain specialised skills, in a context of constantly evolving threats.

⁶Cyber Security and Resilience Bill: introduced by the United Kingdom in November 2025. It updates the Network and Information Systems (NIS) regime and brings the agendas of digital security, AI and critical infrastructure protection closer together. Available at: gov.uk/collections/cyber-security-and-resilience-bill

⁷Network and Information Systems (NIS): European Directive (Directive 2016/1148) that established the first mandatory security regime for operators of essential services and digital service providers in the European Union. The United Kingdom, following Brexit, retains its domestic transposition (NIS Regulations 2018), updated by the Cyber Security and Resilience Bill.

Another aspect underlined was the asymmetries among different levels of government. While federal-level initiatives advance in the design of strategies and reference frameworks, states and municipalities often operate under greater constraints in terms of resources and technical capacity for implementing digital security policies. This challenge is particularly relevant in sectors such as health, education and public security, all increasingly dependent on digital infrastructure.

In this context, the discussions suggest that the consolidation of the AI and cybersecurity agendas in Brazil will benefit from continued efforts aimed at capacity building, institutional coordination and the implementation of initiatives at different levels of government.

8. International governance of AI and cybersecurity: models, convergences and limitations

The governance of artificial intelligence and cybersecurity is evolving rapidly on the international stage, reflecting both the urgency of the risks and the different approaches adopted by States and regional blocs. As Qader, Ashfaq and Sarwar (2025) note, emerging technologies such as AI are rapidly transforming the dynamics of power and security globally.

The Turing Club debate showed that, although there are relevant advances in terms of principles and frameworks, no consolidated and fully effective model yet exists to deal with the complexity of global governance. The research by Barakat (2025), on AI-driven threat intelligence in international cybersecurity frameworks, reinforces this shared perception: the author demonstrates the relevance of integrating AI solutions into cybersecurity structures and indicates that international collaboration is essential to address these challenges effectively.

International models for AI and cybersecurity governance

JURISDICTION	CENTRAL INSTRUMENT	APPROACH
European Union	AI Act	Risk-based · prescriptive
United Kingdom	Pro-innovation	Principles · adaptive · NCSC
United States	NIST AI RMF	Technical frameworks · sectoral
Brazil	AI Bill + LGPD	Consolidating · multi-stakeholder

Figure 6: Comparison of international models for AI and cybersecurity governance.

CONTEXT

Comparative box: three international approaches

European Union, a prescriptive and risk-based approach. The *AI Act* establishes obligations by risk level and prohibitions for unacceptable uses, as analysed by Kaur, Gabrijelčič and Klobučar (2023) in their review of AI for cybersecurity. Under revision, the AI Act evidences the challenge of maintaining stable regulation in a dynamic technological environment.

United Kingdom, a principles-based and adaptive approach, with a strong role for technical bodies such as the NCSC and the AISI. The *AI Cyber Security Code of Practice* (DSIT, 2025a), the *Trusted Third-Party AI Assurance Roadmap* (DSIT, 2025b) and the *Cyber Security and Resilience Bill* (DSIT, 2025c) illustrate a model of *layered governance*⁸ that combines *soft law*, *hard law* and capacity building.

United States, governance strongly supported by technical frameworks from the *National Institute of Standards and Technology* (NIST), such as the *Cybersecurity Framework* and the *AI Risk Management Framework*. Non-binding in nature, they exercise significant influence on good practices and global standards.

The diversity of approaches reflects not only institutional differences but also geopolitical and economic factors. Countries and regional blocs seek to balance the protection of their digital ecosystems with the promotion of innovation and international competitiveness.

In particular, the *Code of Practice for the Cyber Security of AI* of the United Kingdom (DSIT, 2025a), articulated between DSIT and the NCSC, was converted into the basis for *Technical Specification ETSI TS 104 223*, an emerging international reference for the security of the life cycle of AI systems. This movement illustrates how flexible, principles-based approaches can be translated into internationally recognised standards.

Contributions from diplomatic actors highlighted, complementarily, the role of multilateral mechanisms in building shared references and minimum standards. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) represents a relevant example of an effort to establish shared principles, encompassing themes such as human rights, transparency and accountability.

The discussions also indicated that, in an international scenario marked by greater geopolitical complexity, different formats of cooperation tend to coexist. The difficulty of reaching broad consensus in multilateral fora has been accompanied by the appreciation of plurilateral and bilateral arrangements among countries with convergent interests, often described as *like-minded partners*.

In this context, the debate indicated that Brazil, United Kingdom cooperation is situated within a broader alignment of strategic priorities in digital governance. The shared commitment to

⁸Layered governance: a layered governance model that combines instruments of different natures. Soft law: non-binding norms (codes of practice, guidance). Hard law: legally binding norms (laws, regulations).

responsible innovation, digital security and participation in the design of international norms positions bilateral cooperation as a relevant vector for capacity building and the exchange of good practices, complementing multilateral efforts.

9. Cooperation between Brazil and the United Kingdom: a strategic agenda for governance, security and innovation

The convergence of artificial intelligence and cybersecurity, evidenced throughout the Turing Club · Brazil Chapter, cannot be addressed in isolation by individual States. This perception, shared by the participants, is corroborated by Fauziyyah et al. (2025), whose evaluative study on cybersecurity risks in AI-based systems applied to government digital infrastructure demonstrates the transnational nature of vulnerabilities. The speed of technological change, in turn, suggests the relevance of international cooperation models that are agile, adaptable and based on mutual trust, as Kurniati (2024) argues in her study on the role of AI in the security of critical information infrastructure.

The relationship between Brazil and the United Kingdom presents particularly favourable characteristics for the development of a structured cooperation agenda. Both countries share democratic values, have relevant technological ecosystems and demonstrate an interest in strengthening their engagement in global digital governance.

Strategic complementarity · Brazil and United Kingdom

What each side brings and where cooperation meets

BRAZIL	CO-CREATION	UNITED KINGDOM
<i>what Brazil brings</i>	<i>where cooperation materialises</i>	<i>what the United Kingdom brings</i>
- Continental scale - Agile implementation - Consolidated LGPD - AI Bill in Congress	- Interoperable standards - Bilateral capacity-building - Threat intelligence - Critical infrastructure	- NCSC · DSIT · AISI - Risk-based frameworks - AI Cyber Security Code of Practice - CyberFirst (talent pipeline)

Figure 7: Strategic complementarity between Brazil and the United Kingdom: spaces for co-creation identified during the debate.

The strategic potential of Brazil, United Kingdom cooperation

The debate highlighted that this cooperation could evolve into a more structured model, capable of generating concrete impact on public policy, technological development and institutional security. One of the central elements of this agenda is the complementarity between the approaches of the two countries.

KEY MESSAGE

Summary: complementarity between Brazil and the United Kingdom

- **United Kingdom:** analytical rigour, principles-based models, frameworks such as the *AI Cyber Security Code of Practice* (DSIT, 2025a) and the *AI Assurance Roadmap* (DSIT, 2025b).
- **Brazil:** scale, agility in implementing public policies and regulatory frameworks, experience in adapting normative instruments to complex contexts, and rapid response capability to emerging challenges.
- **Space for co-creation:** combining analytical rigour, execution capability and evidence exchange to inform policies, standards and joint capacity building.



Photo: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Image 3: Panel "Brazil, United Kingdom cooperation": bilateral dialogue among representatives from government, diplomacy, private sector and academia.

Academic perspectives shared during the debate underscored that the United Kingdom tends to adopt a more structured and analytical approach to policy formulation, with a strong emphasis on diagnosis, stakeholder mapping and framework construction. This characterisation is reinforced by the analysis of Hurzhii (2023), who examines the specific features of AI use in cybersecurity matters

from a UK perspective. Brazil, in turn, demonstrates significant agility in implementation and adaptability to complex contexts, often described as a capacity for rapid response to emerging challenges. This complementarity, identified by the participants of the Turing Club, represents a strategic opportunity.

The combination of analytical rigour and execution capability can contribute to innovative governance models capable of dealing with the complexity of AI and cybersecurity more effectively. In the governance field, there is scope for the construction of interoperable standards and regulatory alignment.

As a key *takeaway* from the discussions, Brazil experience with the Lei Geral de Proteção de Dados (LGPD), inspired by the European GDPR, illustrates the feasibility of normative convergence processes, a dynamic examined by Craglia et al. (2018) in the Joint Research Centre report on the European perspective on AI. A similar movement could be explored in the fields of AI and cybersecurity, particularly in the context of the discussions around the AI Bill and the Cybersecurity Legal Framework, drawing inspiration from the principles consolidated by the United Kingdom *AI Cyber Security Code of Practice* (DSIT, 2025a).

In addition, the cooperation can benefit from United Kingdom experience in institutional capacity building. The NCSC (2025d), in its Annual Review 2025, documents the model of coordination among government, private sector and academia sustained by the Centre, including technical support, practical guidance and incident response; adapting elements of this arrangement to the Brazilian context could help strengthen response capability and inter-institutional coordination in the country.

Another relevant strand is knowledge sharing and talent development. The shortage of qualified cybersecurity professionals is a global challenge, but particularly acute in Brazil. Joint capacity-building initiatives, academic exchange and skills development, including those inspired by United Kingdom programmes such as *CyberFirst*, which, according to the NCSC (2025d), has already reached over 350,000 students, could help narrow this gap and strengthen the digital security ecosystem.

At the operational level, there are opportunities for cooperation in areas such as threat intelligence, incident response and critical infrastructure protection. The global nature of cyber threats makes information sharing an essential element in the prevention and mitigation of risks. Cooperation models that enable secure and agile data exchange can significantly enhance the response capability of both countries, in line with the priorities set out in the United Kingdom *Cyber Security and Resilience Bill*.

Contributions from diplomatic perspectives reinforced the importance of exploring different levels of cooperation, combining multilateral, plurilateral and bilateral initiatives. In a geopolitical scenario marked by tensions and fragmentation, agreements among countries with convergent interests, known as *like-minded partners*, can advance more rapidly and generate concrete results.

In this context, strategic areas of common interest between Brazil and the United Kingdom were identified, including the use of AI in combating crime, data protection in AI-driven environments and the development of standards for the security of automated systems. Deepening the dialogue on these themes can, in an incremental manner, feed initiatives in multilateral spaces and contribute to strengthening international governance.

10. Strategic areas for Brazil and cooperation opportunities with the United Kingdom

The discussions held at the Turing Club · Brazil Chapter indicate that the challenges at the interface of AI and cybersecurity would benefit from structural, coordinated and implementation-oriented responses. This reading converges with the academic literature: Rios-Campos et al. (2024) provide a comprehensive review of cybersecurity and AI, and Urbanovics (2022) undertakes a comparative analysis of cybersecurity policies in Latin America; both studies suggest the relevance of holistic approaches integrating capacity building, cybercrime detection and governance.

The section below presents strategic elements identified through the analytical systematisation of the debates, combining participants' contributions with empirical evidence and international experiences. The subtitles were formulated as invitations to dialogue, in keeping with the exploratory and collaborative character of the Turing Club.

10.1 Exploring pathways towards integrated AI and cybersecurity governance

Throughout the debate emerged the perception that limited levels of institutional articulation may constitute a challenge for the effectiveness of public policies in Brazil. The coexistence of different strategies, such as EBIA, E-Ciber and data protection initiatives, at distinct stages of implementation reinforces the importance of coordination mechanisms, particularly in view of emerging risks associated with the convergence of AI and cybersecurity. The need for these mechanisms, discussed at the Turing Club, is also supported by Cavalcante (2024), who examines governance measures proposed to address potential risks associated with AI and algorithmic accountability.

Along the debate, the importance of promoting synergies among the different initiatives related to artificial intelligence, cybersecurity and data protection was underscored. The continued evolution of strategies such as EBIA, E-Ciber and other digital governance instruments offers opportunities to strengthen institutional coordination and support more integrated approaches to emerging challenges that account for hybrid threats.

Among the alternatives discussed, mention was made of formal coordination structures with clear mandates, which could involve central government instances such as the Chief of Staff Office (Casa Civil) or the Office of Institutional Security (GSI), as well as the participation of bodies with

relevant activity in the field, including the Ministry of Foreign Affairs, the Ministry of Science, Technology and Innovation, and the Brazilian Data Protection Authority (ANPD).

As an international reference, the NCSC (2025d), sustained by cooperation among DSIT, GCHQ⁹ and the United Kingdom academic ecosystem, illustrates an approach based on the articulation among technical capabilities, policy formulation and cooperation with different sectors, an arrangement also analysed by Krasodonski et al. (2024) in their essay collection on responsible global AI governance. The Turing Club discussions suggested that the exchange of such experiences and good international practices may inform reflections on possible paths to strengthen coordination and policy effectiveness in the Brazilian context.

10.2 Regulatory integration between AI and cybersecurity: opportunities

The parallel progress of the AI Bill and the Cybersecurity Legal Framework was identified in the debate as a relevant moment to reflect on the articulation among different regulatory initiatives related to digital governance.

The academic literature suggests that, in contexts in which multiple normative instruments evolve simultaneously, the promotion of complementarity among principles, definitions and obligations contributes to greater regulatory coherence and effectiveness (Olanrewaju and Onianwa, 2025; Kulothungan, 2024).

In this context, the discussions pointed to the relevance of regulatory harmonisation mechanisms that favour coherence among the principles, definitions and obligations established across different normative instruments, including the articulation of concepts such as risk classification, liability for damages and security requirements from design.

Additionally, the discussions indicated the relevance of incorporating, into regulatory frameworks, principles associated with *security by design* and *governance by design*, so as to consider risks throughout the entire life cycle of technologies. In this sense, the *AI Cyber Security Code of Practice* and the *Cyber Security and Resilience Bill*, both led by DSIT (2025a and 2025c, respectively), offer relevant practical references for this integration.

10.3 Building AI and cybersecurity skills

The development of specialised skills was identified, in the debate, as a relevant element for strengthening national capacities in cybersecurity and artificial intelligence. In a context marked by rapid technological change and growing demand for qualified professionals, initiatives for training, continuous updating and talent retention take on strategic importance, a dimension examined by Velev and Zlateva (2024) in their multi-sector analysis of workforce challenges in cybersecurity and AI.

⁹GCHQ (Government Communications Headquarters): the United Kingdom signals intelligence and cybersecurity agency. The NCSC (National Cyber Security Centre) is the public arm of GCHQ responsible for United Kingdom cybersecurity.

The Turing Club discussions suggest the value of exploring a national strategy for talent training and retention, with a focus on large-scale capacity-building programmes in partnership with universities and the private sector; incentives for retaining professionals in the public sector; the creation of specific career tracks for cybersecurity and AI specialists; and international exchange programmes, particularly with the United Kingdom.

The potential of these initiatives is illustrated by the *CyberFirst* programme of the NCSC (2025d), which involved over 350,000 students and generated £41.4 million in social value in 2024-2025, with a return of £5.94 per pound invested, figures used by Condrut (2024) in her analysis of the validation and prioritisation of competencies for cybersecurity intelligence to argue for structured training programmes in this field.

In Brazil, programmes such as "Hackers do Bem" represent relevant advances; their scale and integration into a broader national strategy can be strengthened, taking into account the essential competencies to face cyber threats. AISI (2025), in its *Year in Review*, signals that bilateral cooperation models with the United Kingdom, including through the learnings of *CyberFirst* and AISI itself, could offer relevant pathways for this expansion.

10.4 AI applications for critical infrastructure resilience

The debate highlighted that the protection of critical infrastructure, including energy, telecommunications, financial services and public services, is a central priority in the cybersecurity agenda. Chinelo, Umeanozie and Alozie (2025), in their study on threat intelligence applied to critical infrastructure protection through AI, argue in a converging direction that a proactive cyber defence approach is essential to address these strategic assets.

The discussions suggested that AI applications can contribute to strengthening the resilience of these assets, through predictive threat detection, integration of real-time monitoring systems, definition of minimum-security standards for operators and large-scale incident simulation exercises. This perspective finds support in Yu (2024), who treats AI itself as critical infrastructure and discusses mechanisms to safeguard national security in the AI era. Practical illustrations come from the Alan Turing Institute (2025), through its *AI for Cyber Defence Research Centre* (AICD) and the *Autonomous Cyber Defence Innovation and Research Lab* (ACD-IRL), which explore how AI models can be applied to the active protection of critical infrastructure.

The combination of a renewed legal framework, capacity building and the intelligent adaptation of United Kingdom principles, such as those consolidated by DSIT (2025c) in the *Cyber Security and Resilience Bill*, could represent a promising vector for Brazil to advance in the resilience of its essential services. The reference to the United Kingdom model must, however, be calibrated to the Brazilian reality, considering the country regulatory, institutional and operational specificities, otherwise it risks losing effectiveness when applied without that adaptation.

10.5 Threat intelligence sharing: practices and opportunities

The dynamic and transnational nature of cyber threats highlights the relevance of cooperation and information sharing among government, private sector, academia and civil society.

The Turing Club discussions indicated that mechanisms aimed at the secure exchange of information and the strengthening of multi-sector collaboration could contribute to expanding the understanding of risks and support more efficient responses to incidents. This is a widely recognised approach in the literature, as demonstrated by the review by Ansari, Dash, Sharma and Yathiraju (2022) on the impact and limitations of AI in cybersecurity, which identifies threat intelligence sharing as a central factor for the advance of cybersecurity across several industries.

International models demonstrate that collaboration among different sectors tends to significantly expand prevention and response capabilities. The Tao, Akhtar and Zhang (2021) survey on the future of AI in cybersecurity evidences this dynamic by mapping initiatives that use AI to monitor, detect and mitigate threats. In Brazil, arrangements of this kind could be designed to include not only large organisations but also small and medium-sized enterprises, which often represent vulnerable points in productive chains.

10.6 The centrality of information integrity in the digital ecosystem

The discussion on disinformation evidenced the relevance of the integrity of the information environment for public trust, institutional resilience and the functioning of societies increasingly dependent on digital ecosystems. This is a theme that receives growing international recognition as an essential component of social and institutional resilience.

The debate suggested the value of treating information integrity as a form of critical infrastructure, with specific policies for monitoring disinformation campaigns, rapid response to information incidents, cooperation with digital platforms and media and digital education of the population. This formulation resonates with the analysis by Yu (2024), who discusses AI as critical infrastructure and its implications for national security. The United Kingdom experience offers relevant references in this strand: the NCSC (2024), in its *Artificial Intelligence* section, and the same NCSC (2025c), in the *Defending Democracy* collection, consolidate guidance for the protection of electoral processes and the response to synthetic media manipulation.

This approach can benefit from the integration between cybersecurity policies, institutional communication and platform regulation, ensuring a coordinated and proportionate response to the risks, an aspect examined by Hunnewell (2024) in his study on national security concerns involving AI and civilian critical infrastructure.

10.7 Consolidating a structured Brazil and United Kingdom cooperation agenda

Bilateral cooperation between Brazil and the United Kingdom offers opportunities to deepen dialogue and the exchange of experiences in AI and cybersecurity. The Turing Club discussions highlighted areas of shared interest, including capacity building, digital governance, exchange of specialists, sharing of good practices and critical infrastructure protection, dimensions that Tao, Akhtar and Zhang (2021), in their survey on the future of AI in cybersecurity, point to as pillars of effective cooperative agendas.

As Craglia et al. (2018) suggest in their report on the European perspective on AI, this type of bilateral cooperation could serve as a basis for plurilateral initiatives, expanding the impact in international fora and contributing to the diffusion of interoperable standards such as the Technical Specification ETSI TS 104 223, derived from the United Kingdom *AI Cyber Security Code of Practice* (DSIT, 2025a).

10.8 Security standards and certifications: international references and good practices

The adoption of internationally recognised standards and frameworks plays a relevant role in promoting consistency, interoperability and trust in digital security practices. Hamon, Junklewitz, Soler Garrido and Sánchez (2024), in their analysis on the challenges of securing AI systems in the context of the applicable regulations, evidence the importance of these international references for the design of coherent policies.

The discussions highlighted the relevance of widely used references, including the ISO/IEC 27001 and ISO/IEC 27701 standards, the frameworks developed by NIST and the *Implementation Guide for the AI Cyber Security Code of Practice* from DSIT (DSIT, 2025a).

Public policies may include fiscal incentives, regulatory requirements and certification programmes to encourage the adoption of these practices, especially among small and medium-sized enterprises. The *Trusted Third-Party AI Assurance Roadmap* (DSIT, 2025b) offers an additional reference by consolidating three complementary quality assurance models for AI systems: (i) *first-party assurance*, in which the developer itself attests to conformity; (ii) *second-party assurance*, in which clients or contractual partners perform assessments; and (iii) *third-party assurance*, with independent audit. By articulating these three levels, the *Roadmap* broadens market trust while reducing information asymmetries among suppliers, purchasers and regulators. It further foresees an *AI Assurance Innovation Fund* aimed at strengthening the United Kingdom *AI assurance* market, financing tools, methodologies and capacity building, a model whose logic of structured incentives may inspire analogous arrangements in other jurisdictions.

11. Conclusion: from technological convergence to a new governance paradigm



Photo: UKinBrazil / Flickr, Turing Club, Brasília, 12/03/2026

Image 4: Closing of the Turing Club · Brazil Chapter: record of the bilateral dialogue.

The convergence of artificial intelligence and cybersecurity represents one of the most profound transformations of the contemporary digital era. Along the discussions of the Turing Club · Brazil Chapter, it became evident that this transformation is not limited to the expansion of technological capabilities: it redefines the foundations upon which security, trust and governance are structured in highly digitalised societies, a dynamic also observed by Fauziyyah et al. (2025) in their empirical study on cybersecurity risks in AI-based systems applied to government digital infrastructure.

The debates evidenced that the risks associated with artificial intelligence are not merely incremental, but systemic. The capacity to automate attacks, to exploit vulnerabilities at scale and to manipulate information environments introduces a new level of complexity, in which the distinction between technical security and institutional stability becomes increasingly blurred. In this context, the protection of critical infrastructure comes to include not only physical and digital systems but also the information environment that sustains democratic processes.

At the same time, artificial intelligence remains one of the main vectors of innovation and economic development. As Widaningsih, Abdurrahman and Busairi (2025) demonstrate in their comparative analysis on AI and cybersecurity governance in national defence strategies, this duality of risk and opportunity invites a paradigm shift in public policy formulation. This is not about

containing technological progress, but rather about structuring it responsibly, integrating security, governance and innovation from the design of the technologies.

In the Brazilian context, the discussions indicated that the governance of AI and cybersecurity draws on a relevant set of initiatives, strategies and normative instruments in evolution. Among these, notable examples include the regulation of artificial intelligence, the Brazilian AI Strategy (EBIA), the National Cybersecurity Strategy (E-Ciber) and other frameworks oriented towards data protection and digital transformation. The consolidation of these agendas offers opportunities to broaden institutional coordination, capacity building and implementation at different levels of government.

In this context, the Turing Club highlights the value of international dialogue and cooperation among multiple sectors in promoting the exchange of experiences, the sharing of good practices and the construction of common understandings on emerging challenges in digital governance. The continuity of these dialogue spaces can contribute to strengthening connections between Brazil and the United Kingdom and support integrated responses to topics of shared interest.

UK REFERENCE

In summary

- The convergence of AI and cybersecurity is systemic and requires integrated governance approaches.
- Brazil has a relevant framework in AI, cybersecurity and data protection.
- Brazil, United Kingdom cooperation creates opportunities for capacity building and the exchange of experiences.
- Information integrity establishes itself as a central topic for digital resilience.

References

References follow the APA style (7th edition). Official UK sources (NCSC, DSIT, Cabinet Office, AISI, Alan Turing Institute) are highlighted and available as open-source publications.

Akhtar, Z. B., et al. (2021). Artificial intelligence in cyber defence and offence: A capability-based assessment.

Alan Turing Institute. (2025). Defence and National Security: AI for Cyber Defence Research Centre (AICD).

Available at: <https://www.turing.ac.uk/aicd>

AI Security Institute (AISI). (2025). Our 2025 Year in Review.

Available at: <https://www.aisi.gov.uk/blog/our-2025-year-in-review>

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review.

DOI: <https://doi.org/10.17148/ijarcce.2022.11912>

Barakat, A. (2025). AI-driven threat intelligence: Strengthening cyber defence mechanisms in international cybersecurity frameworks.

Bioni, B., Garrote, M., & Guedes, P. (2023). Key themes in AI regulation: The local, regional, and global in the pursuit of regulatory interoperability. Data Privacy Brasil.

Bisht, R. K. (2024). Cybersecurity and artificial intelligence: How AI is being used in cybersecurity to improve detection and response to cyber threats.

Cabinet Office. (2025). The Mitigating "Hidden" AI Risks Toolkit. GOV.UK.

Available at: <https://www.gov.uk/government/publications/a-human-centred-approach-to-scaling-and-de-risking-ai-tools>

Cavalcante, P. (2024). Artificial intelligence and algorithm accountability: Potential risks and proposed governance measures. Blavatnik School of Government, University of Oxford.

Chinelo, E. C. E., Umeanozie, P., & Alozie, C. (2025). Enhancing threat intelligence for critical infrastructure protection through artificial intelligence: A proactive cyber defence approach.

Condrut, C. (2024). Validation and prioritization of knowledge, skills and abilities for cyberintelligence analysis in intelligence and national security.

Craglia, M. (Ed.), Annoni, A., Benczur, P., Bertoldi, P., Delipetrev, P., De Prato, G., & Feijóo, C. (2018). Artificial intelligence: A European perspective. European Commission, Joint Research Centre.

Department for Science, Innovation and Technology (DSIT). (2025a). AI Cyber Security Code of Practice and Implementation Guide. GOV.UK.

Available at: <https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice>

Department for Science, Innovation and Technology (DSIT). (2025b). Trusted Third-Party AI Assurance Roadmap. GOV.UK.

Available at: <https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap>

Department for Science, Innovation and Technology (DSIT). (2025c). Cyber Security and Resilience Bill: policy statement and explanatory documents. GOV.UK.

Available at: <https://www.gov.uk/government/collections/cyber-security-and-resilience-bill>

Fauziyyah, G., Maulana, I., Komarudin, K., & Selamat, R. (2025). Risk security cyber in system AI-based: Study evaluative on Indonesian government digital infrastructure.

- Gerlich, M. (2023). Perceptions and acceptance of artificial intelligence: A multi-dimensional study. *Social Sciences*, 12(9).
- DOI: <https://doi.org/10.3390/socsci12090502>
- Hamon, R., Junklewitz, H., Soler Garrido, J., & Sánchez, I. (2024). Three challenges to secure AI systems in the context of AI regulations.
- DOI: <https://doi.org/10.1109/access.2024.3391021>
- Hunnewell, B. (2024). National security concerns for artificial intelligence and civilian critical infrastructure.
- Hurzhii, S. (2023). The special features of using the artificial intelligence in the matters of cybersecurity.
- IBM. (2024). Cost of a Data Breach Report 2024.
- INCC, Instituto Nacional de Combate ao Cibercrime. (2025). Sectoral analyses of the Brazilian scenario of digital fraud and social engineering. INCC.
- ISC2. (2024). Cybersecurity Workforce Study. International Information System Security Certification Consortium.
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions.
- DOI: <https://doi.org/10.1016/j.inffus.2023.101804>
- Krasodomski, A., Gwagwa, A., Jackson, B., Jones, E., King, S., Lane, M., & Mantegna, M. (2024). Artificial intelligence and the challenge for global governance: Nine essays on achieving responsible AI.
- Kulothungan, V. (2024). Securing the AI frontier: Urgent ethical and regulatory imperatives for AI-driven cybersecurity.
- Kurniati, A. (2024). Study of the artificial intelligence role in achieving cybersecurity for critical information infrastructure.
- Lockey, S., Gillespie, N., Holm, D., & Someh, I. (2021). A review of trust in artificial intelligence: Challenges, vulnerabilities and future directions.
- DOI: <https://doi.org/10.24251/hicss.2021.664>
- Modupeola, T. O., Oluwasusi, V. A., Nobari Azar, N. A., & Ichull, A. P. (2025). Deepfake detection and cybersecurity index: The role of computer vision as a digital forensic tool.
- National Cyber Security Centre (NCSC). (2023). Guidelines for secure AI system development. GOV.UK / NCSC.
- Available at: <https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development>
- National Cyber Security Centre (NCSC). (2024). The near-term impact of AI on the cyber threat. NCSC.
- Available at: <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>
- National Cyber Security Centre (NCSC). (2025a). Impact of AI on cyber threat from now to 2027. NCSC.
- Available at: <https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027>
- National Cyber Security Centre (NCSC). (2025b). Preserving integrity in the age of generative AI. NCSC Blog.
- Available at: <https://www.ncsc.gov.uk/blog-post/preserving-integrity-in-age-generative-ai>
- National Cyber Security Centre (NCSC). (2025c). Defending Democracy collection. NCSC.
- Available at: <https://www.ncsc.gov.uk/collection/defending-democracy>
- National Cyber Security Centre (NCSC). (2025d). NCSC Annual Review 2025: CyberFirst and Resilience at Scale.
- Available at: <https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf>
- Nicolás, M. A., & Sampaio, R. C. (2024). Balancing efficiency and public interest: The impact of AI automation on social benefit provision in Brazil.

- Olanrewaju, B. A., & Onianwa, B. (2025). Regulating AI in cybersecurity: Balancing challenges, opportunities, and global frameworks.
- Pandey, A. (2025). AI's Dark Side: The Rise of Deepfakes and the Battle for Truth.
- Parihar, R. (2025). Investigating the impact of artificial intelligence on cybersecurity threat detection and response mechanisms.
- Qader, A., Ashfaq, K., & Sarwar, Z. (2025). Technological innovation and global governance: The role of AI, cyber, and space in international relations.
- Radanliev, P., et al. (2024). Frameworks for AI safety and security in the development of cybersecurity solutions.
- Rios-Campos, C., Venegas Paz, S. C., Orozco Vilema, G., Robles Díaz, L. M., Flores Zambrano, D. P., Mendoza Zambrano, G. M., & Luzuriaga Viteri, J. C. (2024). Cybersecurity and artificial intelligence (AI).
- Tao, F., Akhtar, M. S., & Zhang, J. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey.
DOI: <https://doi.org/10.4108/eai.7-7-2021.170285>
- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence.
- Urbanovics, A. (2022). Cybersecurity policy-related developments in Latin America.
- Velev, D., & Zlateva, P. (2024). Workforce challenges in cybersecurity and artificial intelligence: A multi-sector analysis.
- Verizon. (2024). Data Breach Investigations Report 2024.
- Widaningsih, Abdurrahman, S. S., & Busairi, H. (2025). Artificial intelligence and cybersecurity governance: Comparative insights into national defence strategies.
- World Economic Forum. (2025). Global Risks Report 2025: A world of growing divisions.
Available at: <https://www.weforum.org/publications/global-risks-report-2025/>
- Yu, C. (2024). AI as critical infrastructure: Safeguarding national security in the age of artificial intelligence.
DOI: <https://doi.org/10.31219/osf.io/u4kdq>



Credits

INITIATIVE AND REALISATION

UK Government

TECHNICAL COORDINATION AND SYSTEMATISATION OF THE DEBATES

Luana Tavares

REPORT ELABORATION

Instituto Nacional de Combate ao Cibercrime (INCC)

EVENT

Turing Club · Brazil Chapter

British Embassy in Brasília

12 March 2026

EDITION

1st edition

Brasília / São Paulo · March 2026

Free distribution · Institutional use

ABOUT THE TURING CLUB INITIATIVE

Inspired by Alan Turing and the United Kingdom tradition of computational intelligence, the Turing Club · Brazil Chapter is a bilateral space for strategic dialogue on emerging technologies, including AI, cybersecurity and digital governance, supported by the UK Government under the Brazil, United Kingdom cooperation agenda.

© 2026 · Turing Club · Brazil Chapter

A strategic dialogue initiative on artificial intelligence, cybersecurity and digital governance.