

Digital Democracy in a Divided Global Landscape

Steven Feldstein, editor

Arindrajit Basu | Luca Belli | McKenzie Carrier | Iginio Gagliardone | Dean Jackson | Lillian Nalwoga
Jonathan Corpus Ong | Irene Poetranto | 'Gbenga Sesan | Janjira Sombatpoonsiri | H. Akin Unver

04

When AI Meets Cybersecurity: Framing Brazil's Information Security and AI Challenges

Luca Belli

Artificial intelligence (AI) has transformed the cybersecurity landscape over the past decade, leading to an increase in the frequency, impact, and sophistication of cyber attacks. While organizations can leverage AI to enhance their cyber defenses, detect cyber threats, and improve decisions about how to react, cyber criminals can also exploit the technology to launch targeted attacks at an unprecedented speed and scale, bypassing traditional detection measures.

Indeed, the increasing use of AI systems in a wide range of processes in various critical sectors—such as health, justice,⁹³ and autonomous vehicle management—creates numerous new, and sometimes unpredictable, risks and can open new avenues in attack methods and techniques.⁹⁴ Such risks are maximized when AI is deployed for automated decisionmaking, leading legislators around the world, including in Brazil, to consider appropriate risk regulations aimed at AI systems.⁹⁵

This essay argues that considerable work is needed to support the implementation of existing and proposed cybersecurity and AI frameworks. Such effort is particularly necessary through the adoption of technical standards able to specify and give meaning to highly vague formulations that are typically adopted by AI regulatory frameworks to define cybersecurity risk management provisions. Notably, the essay focuses on the Brazilian context to explore how the country is dealing with the emerging threats and opportunities presented by the intersection of AI and cybersecurity, a set of issues that Brazil—and any other country—needs to consider seriously to be able to build its AI Sovereignty.⁹⁶

AI and Cybersecurity: A Complicated Relationship

The relationship between AI and cybersecurity is dynamic, affecting defensive, offensive, or adversarial capabilities.⁹⁷ While there is already a wide body of research on the technical aspects of AI and cybersecurity, remarkably scarce research exists on the interactions of AI and cybersecurity from a regulatory and governance angle. To start, it is important to distinguish between defensive AI and offensive AI. Defensive AI usually leverages machine learning and other AI techniques to enhance the cybersecurity and resilience of computer systems, networks, and databases, and to protect individuals by shielding them against cyber threats.⁹⁸ From this perspective, AI systems can increase the effectiveness of security controls aimed at protecting specific assets, for instance through automated malware analysis, active firewalls, and automated cyber threat intelligence operations.⁹⁹

In contrast, offensive AI, also known as AI-powered cyber attacks, involves the use of AI to launch malicious activities, enhancing attackers' ability to detect and exploit vulnerabilities, develop new cyber attack types and strategies, or automate the exploitation of existing vulnerabilities.

A Paradigm Shift

The integration of AI capabilities constitutes a watershed moment in the development of cyber threats, significantly augmenting the efficacy, scope, scale, and precision of malicious cyber operations. This evolution marks a paradigm shift in the cybersecurity landscape, fundamentally altering the nature of both offensive and defensive strategies.

First, the democratization and increased sophistication of AI tools enables cyber criminals to automate and refine their attacks, making them more effective, dynamic, and difficult to detect. Machine learning algorithms, for instance, can analyze vast amounts of data to identify vulnerabilities in systems and networks, enabling attackers to exploit these weaknesses with greater precision. Automated phishing campaigns can be tailored to individual targets based on data harvested from the target's social media accounts and other sources. This personalization increases the likelihood of the target falling for the phishing scam, as the messages appear more convincing and relevant. Critically, AI-enhanced malicious attacks now represent the top emerging risk, according to the latest version of the periodic Gartner study dedicated to risk monitoring, because "the relative ease of use and quality of AI-assisted tools, such as voice and image generation, increase the ability to carry out malicious attacks with wide-ranging consequences."¹⁰⁰

Second, AI is likely to expand the scope of cyber threats by allowing attackers to increase the scale of their operations with minimal human intervention. For example, attackers can use AI-powered botnets to implement massive distributed denial-of-service (DDoS) attacks, shutting down the targeted website, server, or network with a large volume of traffic. Ransomware attacks—when an attacker infects a targeted device with malware and

threatens to deny the victim access to their device or release sensitive data if the victim does not pay the demanded ransom (although the payment does not guarantee data recovery, as obviously there is no enforceable contract with cyber criminals and data decryption entirely relies on their "good faith") are also becoming more widespread because of AI, leading to the emergence of a thriving global industry of ransomware-as-a-service (RaaS).¹⁰¹ In this context, AI is lowering barriers to entry for attackers and increasing the ease and availability of ransomware, resulting in high costs associated with recovery and extended downtime.¹⁰²

Third, AI systems can substantially increase attackers' ability to analyze complex datasets and recognize patterns, thus allowing them to execute highly targeted and precise attacks. For example, AI can be used to identify high-value targets within organizations and tailor attacks to their specific roles and responsibilities. AI can also allow cyber criminals to create realistic audio and video impersonations known as deepfakes, which can be used in social engineering attacks to manipulate individuals into divulging sensitive information or authorizing fraudulent transactions.¹⁰³ In a memorable case of an elaborate deepfake scam, a finance worker at a multinational firm was duped into paying \$25 million to fraudsters who had lured him into a fake emergency call.¹⁰⁴

Fourth, the increasing sophistication of deepfakes can be used to orchestrate disinformation campaigns for both financial and political purposes. These technologies pose a novel cybersecurity threat to democratic processes by enabling malicious actors to undermine information integrity at an unprecedented scale. The current democratization of AI implies much greater and easier access to AI systems that, until just a few years ago, were only accessible to researchers and highly specialized companies or governmental actors.¹⁰⁵ This process leads to an enormous expansion of the attack surface, both in terms of potential perpetrators and potential vulnerabilities and attack strategies that can be used.

Importantly, AI-driven cyber attacks have acquired a dynamic nature; they can adapt to changing defensive measures, making detection and mitigation more challenging. By using machine learning capabilities, attackers can alter malicious software in real time to avoid detection by traditional antivirus systems. For instance, AI-enhanced polymorphic or metamorphic malware can mutate its features or automatically "re-code" itself when it propagates to evade pattern matching detection systems that are traditionally deployed as security solutions. Furthermore, AI systems can be used to quickly identify and exploit zero-day vulnerabilities before patches can be developed and deployed.¹⁰⁶

Crucially, defenders are also increasingly employing AI-based systems to detect cyber threats and vulnerabilities and rapidly respond, for instance by leveraging AI to identify software bugs and self-patch them. However, within a sort of cybersecurity arms race, attackers are also leveraging AI to outmaneuver these defenses. In a situation where both sides continuously refine their techniques, defensive AI systems must evolve rapidly to detect new attack patterns and anomalies, while policy and governance framework must be crafted to mitigate risks and facilitate communication, collaboration, and coordination among cybersecurity stakeholders.

Understanding the Brazilian Context

Despite relevant advancements in recent years, the regulation of AI and cybersecurity in Brazil is highly fragmented, limited, and poorly implemented. By adopting multiple cybersecurity-related sectoral regulations, Brazil has improved in several international rankings that assess cybersecurity readiness.¹⁰⁷ But regulatory oversight and cybersecurity implementation remain patchy because such processes are the responsibility of many different and uncoordinated entities, including sectoral regulators, private and public computer security incident response teams, and the military.¹⁰⁸

Critically, Brazil does not have a general cybersecurity law, nor a cybersecurity agency, which represents an unforgivable deficiency, in 2025. The top institution responsible for cybersecurity governance and policy proposal is the Institutional Security Cabinet (GSI in its Portuguese acronym) of the Brazilian presidency. However, the GSI's remit is limited to the federal administration, restricting the scope of its reach. Importantly, in December 2023, Brazil adopted a new National Cybersecurity Policy and established a new multistakeholder National Cybersecurity Committee,¹⁰⁹ known as “CNCiber,” of which the author of this essay has been appointed a member.¹¹⁰ Among the tasks of CNCiber is the elaboration of a proposal for a new national cybersecurity strategy and a new body for cybersecurity governance and regulation.

Indeed, one of the reasons for Brazil's fragmented cybersecurity regulatory landscape is the lack of a unique institution responsible for coordinating the various dimensions of cybersecurity. At this moment, Brazil does not have an actionable cybersecurity strategy allowing the country to organically tackle the multiple—and mounting—cyber threats it faces nor a cybersecurity agency able to assess the ways in which AI technologies are impacting such threats.

Furthermore, only limited AI regulation exists, primarily under the purview of the Brazilian National Data Protection Authority (ANPD). In this context, the Brazilian National Congress is currently considering dedicated legislation to regulate AI, which would include cybersecurity obligations related to AI systems. (At the time of publication, legislation was still pending and the rapporteur of a new Special Commission for AI, established by the Chamber of Deputies, had promised to alter the bill.)¹¹¹

Information Security?

Information security is an essential dimension to both AI and cybersecurity. In Brazil, the ANPD is tasked with enforcing the Brazilian General Data Protection Law (LGPD) and ensuring that organizations comply with data protection obligations.¹¹² Data security is a fundamental principle set by the LGPD, aimed at ensuring that personal information is protected against unauthorized access, loss, alteration, damage, or destruction. Importantly,

the LGPD explicitly establishes a security-by-design obligation for data controllers and processors, who need to implement security measures that the data subject “can expect” to demonstrate that personal data processing activities are regularly undertaken.

To comply with the LGPD, data processing agents—that is, the individuals or entities responsible for defining how personal data are processed in a given organization and implementing such decisions—are supposed to implement solid information security solutions, such as establishing an information security policy, raising awareness and capacity, and establishing technical measures to build data resilience. Without these, data processing should be considered irregular. In practice, however, data security compliance is poor at best. In the first four years after its inception, ANPD did not adopt the minimum data-security standards that it was empowered to enact in accordance with LGPD article 46.1, and its oversight is limited to receiving communications about data breaches without providing any solutions.

While the ANPD has a potentially enormous role to play in establishing data security regulations aimed at avoiding cybersecurity incidents, it has instead spent its energies on regulating the communication of such events to the public, providing guidance only on how the tragedy must be communicated instead of about how to avoid it. Indeed, Brazil ranks second globally for cyber attacks, which have exploded in number and sophistication because of the adoption of AI systems together with frequent data leakages and a “thriving” black market for personal data.¹¹³

A more proactive approach has been adopted by the Ministry of Management and Innovation, through its Ordinance SGD/MGI No. 852, which established the Privacy and Information Security Program (PPSI).¹¹⁴ PPSI is designed to enhance cybersecurity in the Brazilian public administration by providing guidance on data governance, encouraging projects and adaptation processes aimed at increasing cybersecurity maturity, resilience, effectiveness, collaboration, and intelligence. However, the Brazilian Court of Auditors has recently assessed that the implementation of PPSI is at an alarmingly low level, noting gross lack of compliance.¹¹⁵

While the LGPD and PPSI are essential information security pillars, they are not sufficient on their own. It is essential that a new cybersecurity strategy and a cybersecurity agency, to be proposed by the National Cybersecurity Council, provide guidance on how to specify information security criteria applicable to all entities, with particular regard to providers of essential services, critical infrastructures, and all entities managing categories of sensitive information that are not personal.¹¹⁶ Furthermore, a future Brazilian cybersecurity agency should establish cooperation agreements, and ideally an effective communication and coordination mechanism, with the ANPD and the other sectoral regulators to ensure a harmonized cybersecurity approach.

What Is an “Appropriate” Way of Regulating AI?

It is important to emphasize that both cybersecurity and AI are quintessentially multidimensional. Indeed, the effective regulation of AI risks and digital technology cybersecurity relies on the understanding that both AI and digital technologies are systems based on the interconnection of data, software, and hardware. Risks and vulnerabilities are inherent to both the elements that compose the systems and the ways such elements interact. The success of both cybersecurity and AI governance depends on having a good understanding of how the different components of digital and AI technologies interplay, how they are utilized, and what are the vulnerabilities in their use and deployment.¹¹⁷

Sound management of information and infrastructure, good stakeholder coordination, and solid capacity-building are therefore essential for both AI and cybersecurity regulation. However, in Brazil, each dimension or component of both AI and cybersecurity is currently regulated by multiple entities with limited or no coordination. While Brazil is in the process of developing a new AI framework, there are several concerns about the way in which the framework proposes to regulate cybersecurity aspects of AI and foster coordination among sectoral regulators.

For one, all versions of Brazil’s proposed AI framework—including the last one available at the time of this writing—have included a considerable amount of vaguely worded cybersecurity provisions, such as obligations to “perform tests to evaluate appropriate levels of security” of AI systems (see article 18.c).¹¹⁸ “Appropriate” and “adequate,” along with “reasonable,” are every lawyer’s favorite adjectives because they can mean virtually anything. While such language is essential to preserve normative flexibility, with no further guidance this can easily turn into legal uncertainty, which is the opposite of what new regulations should bring.

Clarifying and specifying these flexible provisions will require considerable technical knowledge. It is not a coincidence that the EU AI Act delegates this task to technical standardization bodies.¹¹⁹ However, this solution has raised concerns from human rights advocates who claim it constitutes a delegation of regulatory power to private and poorly accountable standardization bodies with scarce knowledge about fundamental rights’ risk posed by AI systems.¹²⁰

To address these challenges, the Brazilian AI bill proposes to establish an AI governance and regulation system, where all sectoral regulators would come together under the leadership of the ANPD “to regulate and classify high risk AI systems” considering, among other things, “the high potential for systemic harms, such as to cybersecurity, and violence against vulnerable groups” (see article 15.VII that associates these two rather different risks for unspecified reasons).

The idea of a coordination system is promising, but the bill fails to articulate how it would function in practice and, most worryingly, who would deal with the cybersecurity dimensions of AI. Additionally, it seems risky to entrust the leadership of the system to an overstretched organ that barely manages to cope with fulfilling its current mission. To think that the ANPD, under its current structure, can effectively lead a new system of such relevance and magnitude, and effectively guarantee AI cybersecurity seems overly optimistic.

Conclusion

The relationship between AI and cybersecurity presents significant and transformative developments. While it has empowered malicious actors to conduct more impactful, far-reaching, and precise attacks, it has also underscored the importance of proactive and adaptive cybersecurity strategies. Indeed, the integration of AI into offensive and defensive cyber capabilities demands a fundamental shift in cybersecurity strategies.

In this context, fostering collaboration between government entities, private sector organizations, and research institutions is essential for Brazil—and all other states—to address the challenges posed by AI in the cybersecurity domain. The adoption of a multistakeholder approach is critical to understand the cyber threats landscape and develop effective regulations, standards, governance, and capacity-building mechanisms. Indeed, these elements are key to implementing robust cybersecurity measures and promoting innovation in defensive AI technologies to cope with mounting AI-driven cyber attacks.

Unfortunately, despite some advancements, the current Brazilian approach does not seem capable of confronting effectively the mounting number and complexity of cyber threats. It is vital that considerable resources be allocated to support an effective multistakeholder cooperation that need to be enshrined in the future strategic and institutional framework adopted by Brazil. This will not only increase the quality of policymaking with evidence-based solutions but, more importantly, will enable inter-stakeholder coordination to implement cybersecurity measures in an agile and effective fashion.

In this perspective, the establishment of a robustly resourced Cybersecurity Agency must be seen as an imperative for Brazil, enabling the country to comprehensively assess how both existing and emerging technologies can either bolster or compromise cybersecurity. Considering the increasing reliance of our critical infrastructure, essential services, and societal functions on AI systems, neither Brazil nor any other country can afford to operate without considering the cybersecurity of AI systems an utmost priority.