AI: A GAME CHANGER IN MANAGING NATIONAL CYBER RISKS

DIGI AMERICAS ALLIANCE MEMBERS

*The views and/or opinions expressed in this document do not necessarily reflect the official policy or position of the Digi Americas Alliance members or its representatives.

On January 16, 2024, at the margins of the World Economic Forum (WEF) Annual Meeting in Davos, Switzerland, the Digi Americas Alliance - with the support of Mastercard - hosted a roundtable on 'AI: A Game Changer in Managing National Cyber Risks.' The first part of the discussion focused on 'Managing National Cyber Risks and Protecting Critical Infrastructure,' while the second part focused on 'Fostering Digital Trust: Strategies to Combat Cybercrime.' The following report summarizes the insights, strategies, and recommendations discussed at the event.

INSIGHTS

The first discussion focused on leveraging AI for cyber defense and protecting critical infrastructure. Participants noted the rapid digitization of the Latin America region, with AI functioning as a catalyst for further growth. As mobile penetration has dramatically increased across Latin America, phishing, ransomware, and trojan attacks have often targeted the region's financial and e-commerce sectors and government services. The uptick in regional ransomware attacks is correlated to target hardening - as other countries and regions build stronger cyber defenses and become less likely to pay the ransoms, attackers have turned their focus to Latin America. Despite this, 17 countries in the region do not have a national cybersecurity plan for critical infrastructure. Policy development, increased regulation, and capacity building are crucial when securing the Internet of Things (IoT) and industrial IoT devices. Technology risks are further exacerbated by people and process issues, including a lack of digital literacy in local populations and governments, a significant cybersecurity workforce shortage, and a technical skills deficit.

While panelists noted the numerous ways AI is already being used for cyber security defense - from automated detection systems network analysis to analyzing threats and anomalies despite linguistic barriers - they also emphasized that AI simultaneously exists as a powerful threat vector. In a global landscape of cyber threats, there were reminders that while cyber-attacks may target a particular region, they often originate from a completely different place. The geopolitical backdrop for the region was emphasized by participants; while Latin America is highly heterogeneous, nearly 80% of countries in the region have China as their number one trading partner, which helps illustrate the large influence China has across the continent.

The second discussion revolved around the proliferation of cybercrime and the role of AI as a tool both for and against cybercriminals. Participants noted that AI is democratizing the availability of cybercrime tools and often expanding the scale of their impact, with large language models readily available for sale online for malicious purposes. As cybercrime and fraud increase, it is crucial to continue to educate local populations, especially since AI enables more sophisticated and personalized cyber-attacks, particularly in social engineering. With social engineering in mind, especially from an institutional perspective, participants highlighted the value of zero-trust architecture, which requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside the network perimeter.

AI: A GAME CHANGER IN MANAGING NATIONAL CYBER RISKS

Participants emphasized the important role of law enforcement in prosecuting cyber criminals and the need to focus on individual-level attribution of the criminals behind the attacks rather than just identifying behavioral patterns associated with larger criminal groups. A silver lining is using AI to gather and aggregate more data about cyber criminals and their behaviors. These law enforcement efforts are supported by INTERPOL in partnership with national law enforcement agencies across Latin America and with cross-national initiatives such as the International Police Cooperation Centre (IPCC) in Rio de Janeiro and Ameripol (Police Community of the Americas), including through INTERPOL's regional bureaus in Buenos Aires and San Salvador. Participants note that regional and global cooperation around cybercrime law enforcement can be limited because countries have different legal systems and, sometimes, different incentives, as well as substantial discrepancies in national cybersecurity and cybercrime investigation capabilities. Despite this obstacle, participants highlighted the benefits of institutionalized threat information sharing - across different public stakeholders and between the public and private sectors- while noting potential challenges around sharing information in accordance with local privacy laws.

PARTICIPANTS SHARED THEIR VIEWS ON POTENTIAL CYBERSECURITY RECOMMENDATIONS FOR THE REGION, INCLUDING:

- Develop national cybersecurity strategies, guidance, and training - especially for critical infrastructure - but also focus on supporting local cyber workforce development and increased public education and awareness.
- Leverage automation to augment the cybersecurity workforce and ease the workforce gap.
- Navigating cross-border attacks and threats requires strong multilateral cooperation and leadership.
- Robust and institutionalized public-private partnerships, especially around threat intelligence sharing, will shape more positive outcomes regarding AI in cybersecurity.
- It is imperative to secure the data systems that underpin AI and be able to detect any interference or manipulation.
- Alongside software, hardware risks also need to be considered and prioritized (e.g. through the use of confidential computing, capabilities that enable the protection of data-in-use by performing computation in a hardware-based, attested Trusted Execution Environment).
- Continue to advance the technical work around AI being done in standard bodies such as the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU) while ensuring that the local contexts in different regions are considered as standards are being developed.
- The private sector should utilize and strengthen multilateral policing architecture around cybercrime with a particular focus on AI - in terms of existing bodies like INTERPOL and ongoing treaty negotiations like the United Nations Cybercrime Convention.

AI: A GAME CHANGER IN MANAGING NATIONAL CYBER RISKS

NEXT STEPS

- Digi Americas Alliance will host its **LATAM CISO Summit in Guanacaste, Costa Rica, on September 12-13, 2024**. The European Union has already confirmed the intention to invite Ministers and High-Level government authorities to the Summit. Representatives from All Alliance Members and high-level executives from the region are expected to participate.
- Brazil's assumption of the G20 Presidency represents a critical moment to advocate and advance the cybersecurity needs of the Global South. **The 2024 G20 in Rio de Janeiro, Brazil (November 18 - 19)** will serve as an important forum for continuing the dialogue in Davos and robust in-person engagement with the Latin American public and private sectors.

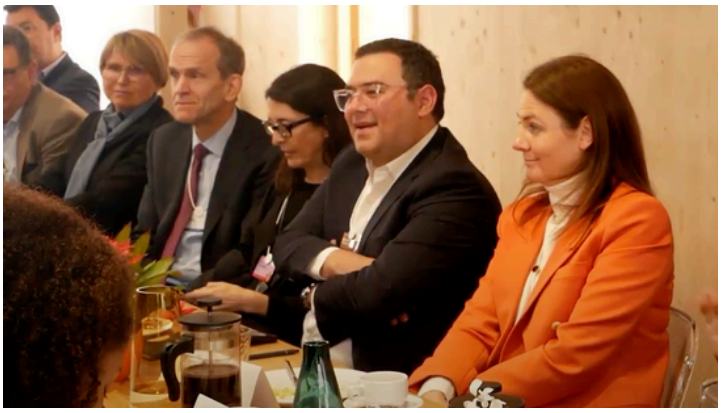
RELEVANT RESOURCES

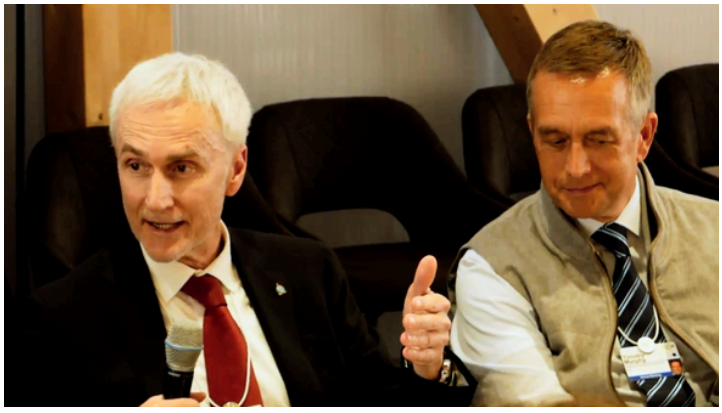
- Envisioning Cyber Futures with AI Report: A written report summarizing the work of the Aspen Institute's US and Global Cybersecurity Working Group on what the uses and misuses of artificial intelligence (AI) could mean for cybersecurity in terms of both risks and benefits.
- Cybercrime Atlas: Hosted by the World Economic Forum's Centre for Cybersecurity, the Cybercrime Atlas uses open-source research to create new insights into the cybercriminal ecosystem. The Cybercrime Atlas community comprises organizations with a key role in identifying and disrupting cybercriminal operations.
- Google's Secure AI Framework: A conceptual framework to secure AI systems.

PARTICIPANTS

- Michael Punke, Vice President of Global Public Policy, Amazon Web Services (AWS)
- Michelle Zatlyn, Co-Founder, President, and Chief Operating Officer, Cloudflare
- Michael Daniel, Chief Executive Officer, Cyber Threat Alliance
- John Kent "Kent" Walker, President of Global Affairs, Google
- Patricia Astudillo, Deputy Director, Grupo Radical
- Denise Anderson, President, Health-ISAC
- Robert Muggah, Co-Founder Igarapé Institute and Principal at SecDev
- Bruce Andrews, Corporate Vice President and Chief Government Affairs Officer, Intel
- Jürgen Stock, Secretary General, INTERPOL
- Timothy Murphy, Chief Administrative Officer, Mastercard
- Ilona Simpson, Chief Information Officer, Netskope
- Anna Makanju, Vice President of Global Affairs, OpenAi
- Helmut Reisinger, Chief Executive Officer EMEA & LATAM, Palo Alto Networks
- Claire Alexandre, Head of International Government Relations, PayPal
- Bryan Palma, Chief Executive Officer, Trellix
- Merry Walker, Senior Advisor, Office of the Special Envoy for Critical and Emerging Technology, U.S. Department of State
- Sir Jeremy Fleming, Former Director, UK GCHQ
- Belisario Contreras, Senior Director, Global Security & Technology Strategy, Venable LLP
- Ryan Gillis, Senior Vice President, Global Head of Government Partnerships, Zscaler

AI: A GAME CHANGER IN MANAGING NATIONAL CYBER RISKS





AI: A GAME CHANGER IN MANAGING NATIONAL CYBER RISKS