November 1, 2024

The Honorable Antony Blinken
Secretary of State
U.S. Department of State
2201 C Street NW
Washington, D.C. 20520

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

The Honorable Gina Raimondo
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, D.C. 20230

Jake Sullivan
Assistant to the President for
National Security Affairs
The White House
Washington, D.C. 20500

Re: UN Convention Against Cybercrime

Dear Secretary Blinken, Attorney General Garland, Secretary Raimondo, and Mr. Sullivan:

On behalf of the Software & Information Industry Association (SIIA) and the Computer & Communications Industry Association (CCIA), representing a wide array of technology, data, and digital content leaders, we are writing to share our concerns regarding the draft United Nations convention against cybercrime (the "Convention") ahead of the upcoming vote in the United Nations General Assembly. While we support its admirable goals, we have grave concerns that the Convention will erode critical safeguards for individuals and companies, expose companies to technology and data exfiltration, weaken cybersecurity and AI safety, and cede ground in the global values competition around technology.

These concerns are not unique to our organizations' members: civil society stakeholders and industry groups, as well as several U.S. Senators have all expressed concerns. We write separately to highlight a handful of issues from the perspective of the technology and information industries in the hope that these will assist you in your important deliberations on the Convention.

The Convention will Undermine AI Safety and Cybersecurity Resiliency

The technology industry has been instrumental in developing advanced cybercrime protections, often working directly with governments to deploy cutting-edge security technologies and processes that protect businesses, individuals, and national infrastructures. These efforts have transformed the cyber landscape, piloting innovations that detect and defend against increasingly sophisticated cyber threats. The industry's deep commitment to cybersecurity is not just to safeguard its own networks, but to contribute to a safe and secure global digital environment that supports economic growth and public trust. We believe that to sustain this momentum and make further strides, particularly with the growing adoption of AI technologies worldwide, it is crucial to adopt policies that support, rather than limit, the

capacity of researchers to innovate and identify vulnerabilities preemptively. We are concerned that the Convention will have the opposite effect.

The Convention calls for criminalizing conduct that could directly undermine AI safety and cybersecurity resiliency. This is reflected in Articles 7-10, which do not require criminal intent and lack a good-faith exception for security research. AI-driven solutions are already enhancing real-time threat detection, automating response actions, and making predictive analyses that identify potential threats before they materialize. However, to effectively safeguard these AI systems against malicious actors, they must undergo rigorous safety testing by researchers who simulate cyber-attacks and assess model vulnerabilities, a process known as "red-teaming."

Rigorous red-teaming and other third-party vulnerability testing is a key component of Executive Order 14110 and U.S. government cybersecurity policy. The Executive Order highlights the importance of this research, emphasizing the need for diverse and comprehensive testing to ensure AI systems are resilient against abuse and misuse. By failing to include a good-faith provision for such safety research, the Convention will discourage the very research necessary to foster AI safety and security across sectors. This is a vital issue for U.S. national security and economic interests, including continued U.S. leadership in the values competition that underlies continued leadership in AI. It could also limit the ability for the international AI research community and the International Network of AI Safety Institutes to carry out important work on AI and cybersecurity.

In the private technology sector, AI safety represents a significant area of investment and research. Companies across sectors rely on these efforts to preemptively address potential vulnerabilities before they can be exploited, helping protect millions of consumers and enterprises alike. If researchers are hindered from conducting tests that mimic real-world cyber threats, it weakens the foundational security measures of AI systems across industries, leading to a less secure global marketplace and an increased risk of large-scale cyber incidents.

Dissuading Security Research Will Exacerbate the Talent Deficit

The restrictions on security research also have negative implications for the ability of nations like the United States to address the still vast global talent shortage, which APNSA Sullivan highlighted in a speech just last week. As international adoption of AI increases, the need for open collaboration among researchers from diverse cultural and linguistic backgrounds becomes even more pressing. Without the ability to test models comprehensively, including in different languages and cultural contexts, AI technologies may remain vulnerable to localized threats that could later escalate. The Convention's potential criminalization of cybersecurity research will deter the best minds from entering the field, constrainthe global advancement of AI safety protocols and weaken collective defenses against AI-enabled cybercrime.

Governments May Use Convention to Justify Technology and Data Extraction from U.S. Companies

The technology and information industries are concerned that autocratic regimes could use the Convention to justify the expropriation of data and technology from SIIA and CCIA member firms without due process or other safeguards that are currently in place in the United States and like-minded nations. Competitors of the United States have long sought to extract technology and data from U.S. companies to advance their own technological development, support the growth of domestic champions, and, at times, to support influence operations. APNSA Sullivan touched on this last week in citing "theft and espionage" as a "playbook" that competitors are deploying in order "to depose our AI leadership." APNSA Sullivan spoke to how the new National Security Memorandum on AI "establishes addressing adversary threats against our AI sector as a top-tier intelligence priority."

Unfortunately, we believe the Convention would make it significantly easier for competitor nations and adversaries to extract technology and data from U.S. firms - and to do so in the name of complying with a UN mandate. As one example, Article 16 calls for criminalizing, among other things, the "transmitting, publishing, or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image." This requires no intent, and may well capture platforms and passive conduits used by bad actors. Nevertheless, that would be sufficient pretense for a state to justify invoking the bevy of search, seizure, collection, and interception authorities set out in Chapter III.

The Lack of Safeguards on Government Access will Legitimize Censorship and Privacy Intrusions and Undermine the Open Internet

We share the Senators' concerns about the negative impact of the Convention on privacy and surveillance. Articles 28-30 of the Convention illustrate these concerns. These Articles would require each State Party to adopt measures to enable the search and seizure of stored electronic data, real-time collection of traffic data (i.e., metadata), and interception of content data. Although Article 24 would place conditions and safeguards on state actors, in practice we are concerned this will have limited impact as many states have already indicated their intent not to agree to these provisions. The same is true of other safeguards embedded in the draft Convention regarding human rights. This approach is anathema to democratic principles and reflects an endorsement of the types of practices more commonly associated with autocratic regimes.

Our concerns are not limited to how foreign states may implement the convention through their domestic authorities. The Convention would require international cooperation to investigate alleged criminal activity that occurred in a foreign state. Its expansive data-sharing and cross-border access provisions open doors to potential surveillance abuses, particularly for nations with limited oversight or autocratic regimes. Without clear privacy safeguards, there is a risk of infringing on individual rights as governments pursue cross-jurisdictional cybercrime investigations.

In addition, encryption remains vital to secure communications, yet the Convention would disincentivize encryption technology if not lead to outright prohibitions in certain state parties. This could weaken the security that individuals, especially those in repressive regions, rely on to protect sensitive information.

In nations like the United States, it will lead to weakened privacy protections for individuals and increase security vulnerabilities.

Finally, we note that the approach taken by the Convention is completely at odds with the framework set out in the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, which the United States helped to negotiate over a two-year period. The Declaration, while not perfect, represents a different approach to government access that we would encourage the U.S. government to stand behind as a framework for broader cooperation with UN member states. Likewise, the Budapest Convention, which has been in effect for two decades and has 76 state parties, does not share the flaws of the draft Convention and represents an approach to addressing transnational cybercrime more in line with U.S. national and business interests.

Ambiguity in Definitions Raising Censorship and Human Rights Implications

The Convention's definitions of cybercrime remain overly broad, and this ambiguity risks curbing free expression and online freedoms as countries interpret "cybercrime" according to local laws and biases, potentially leading to the criminalization of what the United States may consider to be lawful online speech. Countries such as Russia, China and Iran will feel emboldened to impose further restrictions and enforcement against the press and others speaking openly online.

From an industry perspective, clear and narrow definitions are essential to avoid unintended consequences that may lead to further undermining basic rights and freedoms. Technology companies play a vital role in supporting global communication, expression, and access to information, yet overly broad definitions of cybercrime may create additional challenges for firms operating globally across jurisdictions that vary widely in terms of both their commitment to human rights and their regulatory approaches. Without clear protections, this also raises the risk that global technology providers may be caught in cross-border disputes that stifle their ability to innovate and serve international markets. This undermines not only the industry's capacity for growth but also its foundational role in empowering users worldwide and supporting the digital economy.

Conclusion

Given these concerns, we respectfully urge the United States and other member states to reconsider this Convention's current form before it is voted upon in the U.N. General Assembly. Thank you for taking the time to consider our views. We look forward to further engaging with the Administration on these issues. Please direct any questions on this matter to Paul Lekas, SIIA Senior Vice President for Global Public Policy, at plekas@siia.net.

Sincerely,

Software & Information Industry Association (SIIA)
Computer & Communications Industry Association (CCIA)