ITSCC - AI Policy Principles

Given the increasing attention to Artificial Intelligence, its benefits, and its potential harms, the ITSCC has developed a set of AI Policy Principles for U.S. policymakers, focusing specifically on cybersecurity and privacy. We have developed and/or adopted many of these principles based on *Global AI Policy Recommendations* published by the Information Technology Industry Council (an ITSCC member).[1]

1) **A risk-based, context-specific approach to AI regulation is essential.** Risks need to be identified and mitigated in the context of the specific AI use. This will help policymakers determine use cases or applications that are of particular concern, avoiding overly prescriptive approaches that may serve to stifle innovation. Context is also key, as not all AI applications negatively impact humans and thus inflict no harm that would warrant regulation. A risk-based, context-specific approach will be the most effective means of addressing concerns that may be associated with AI, while simultaneously allowing for innovation and agility in development of AI applications.
2) **Global, voluntary, industry-led standards should be supported and leveraged.** AI standards are essential to increasing interoperability, harmonization, and trust in AI systems. They can inform AI regulation, practical implementation, governance and technical requirements. Governments should work to support global, voluntary, industry-led standards, and safeguard the work and processes of international standards development bodies. Broad contributions to and adoption of international standards reduces market access barriers. Standards work for the net benefit of the international community and should be developed and applied without prejudice to cultural norms and without imposing the culture of any one nation. Standards work should also be technology neutral (avoiding preferential treatment for any specific technical approach). We especially encourage alignment with the work of ISO/IEC JTC 1/SC 42, which is developing a number of AI related standards, including on risk management, terminology, reference architecture, governance of AI, and trustworthiness.
3) **Polices should support the use of AI for cybersecurity purposes**. Cybersecurity tools and technologies should incorporate AI to keep pace with the evolving threat landscape, including attackers who are constantly improving their sophisticated and highly automated methods to penetrate organizations and evade detection.

[1] https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

Defensive cybersecurity technology can use machine learning and AI to more effectively address today's automated, complex, and constantly evolving cyberattacks. When combined with cloud, AI can help to scale cyber efforts through smart automation and continuous learning that drives self-healing systems. To support and enable the use of AI for cybersecurity purposes, policymakers must carefully shape (or reaffirm)[2] any policies related to privacy to affirmatively allow the use of personal information such as IP addresses to identify malicious activity.

4) **Public and private sector stakeholders should incorporate AI systems into threat modeling and security risk management.** This should include encouraging organizations to ensure that AI applications and related systems are in scope for organizational security program monitoring and testing and that the risk management implications of AI systems as a potential attack surface are considered.
5) **The use of strong, globally accepted and deployed cryptography and other security standards that enable trust and interoperability in AI systems should encouraged.** The tech sector incorporates strong security features into our products and services to advance trust, including AI systems. Policymakers should promote policies that support using published algorithms as the default cryptography approach as they have the greatest trust among global stakeholders, and limit access to encryption keys.
6) **Investment in security innovation to counter adversarial AI is critical.** It is important that businesses and governments also invest in cybersecurity directed at countering adversarial AI. For example, malicious actors can use adversarial AI to cause machine learning models to misinterpret inputs into the system and behave in a way that is favorable to the attacker. To produce the unexpected behavior, attackers create "adversarial examples" that often resemble normal inputs, but instead are meticulously optimized to break the model's performance. Adversarial AI represents an incremental threat compared to traditional cyber-attacks, so it important that governments ensure their policy instruments do not inadvertently stifle industry's efforts to counter adversarial AI.
7) **Frameworks and guidelines that protect privacy and promote the appropriate/ethical use of data that may be used in data sets underpinning AI should be supported and developed.** To protect personal information and support fundamental human rights, data in data sets used by AI systems may be required to be anonymized, aggregated, or otherwise de-identified such that the datasets exclude any personal information and cannot be re-identified. Doing so ensures the beneficial use of the data in training intelligent systems while protecting individual privacy and security consistent with protecting fundamental human rights.

[2] For example, the GDPR recognizes that ensuring network and information security is a "legitimate interest" of entities for processing personal data (Recital 49).