

INSIGHTS

AI, Cyberspace, and ICTs: Untangling the Digital Universe

Chhem Siriwat¹, Ph.D. Candidate in Leadership, Master of Digital Technology Management (MDTM), Master of Arts in Diplomacy

Dr. Hul Seingheng², Doctor of Environmental Engineering

Dr. Lim Putthi Cheat³, PhD in Economics

Ros Sayumphu⁴, MA in Security, Conflict and International Development, LLM in International Law

¹ ***Chhem Siriwat** is a President of AI Forum*

² ***Dr. Hul Seingheng** is a Chairman of AI Forum*

³ ***Dr. Lim Putthi Cheat** is a Independent Scholar*

⁴ ***Ros Sayumphu** is a Research Fellow at AI Forum*

Introduction

The digital revolution is sweeping the world, and sophisticated terms for these technologies and systems are emerging. These terms include cloud, blockchain, cryptocurrency, mining, AI, ICTs, IoT, and others. Although these terms are becoming popular and being adopted by humans in their daily lives, it is still being determined whether they have been correctly used or defined from one local context to another. When key term definitions are ambiguous and not similar, it can lead to misleading and confusing use, which is even more dangerous when the ambiguity is incorporated into laws or regulations. From a foreign affairs perspective, it is undeniable that these key terms were created and introduced by technologically advanced nations that created or adopted the technology early on, as opposed to user or imported nations. In other words, such sophisticated technology cannot be named by those who did not create it, just as a child is usually named by their parents or family and rarely by an outsider. That being said, if such a proposition is true, it implies that developing nations or countries adopting foreign technology must exercise caution and be aware of the potential meaning when defining technology, particularly the language for law. Seeing such an emerging issue, the article aims to define three terms: Artificial Intelligence (AI), Information Communication Technologies (ICTs), and Cyberspace, while also seeking to understand their differences and give policy recommendations. The purpose of this paper is to highlight the importance of precise definitions and the potential risks of ambiguity in legal and regulatory systems. Furthermore, the study aims to highlight the differences in interpretation can lead to policy gaps, particularly in poor countries that adopt these technologies.

AI, Cyberspace, and ICTs?

To begin with it is only natural that when hoping to have an understating of a new sophisticated term, it is essential to refer to source where discussion about this has taken place and where it tries to universally define the term even if symbolically. With this, the glossary provided by the UN, specifically the UN E-government knowledgebase will be examined. The UN-based platform has defined the three terms as follow:

“Artificial Intelligence (AI): Is the ability of a computer or a computer-enabled robotic system to process information and produce outcomes in a manner similar to

the thought process of human beings in learning, decision-making and problem-solving (United Nations, n.d.a).”

“**Cyberspace:** A virtual or notional environment of electronic communications. The online environment facilitated by the internet is the most popular type of cyberspace (United Nations, n.d.b).”

“**Information and Communications Technology (ICT):** ICT refers to technologies that provide access to information through telecommunications. This includes the Internet, wireless networks, cell phones, and other communication mediums (United Nations, n.d.c).”

Comparatively, this commentary will also hope to examine the key term identify by ASEAN. In the ASEAN Guide on AI Governance and Ethics, the document defined AI as the following:

“**Artificial Intelligence (AI):** is an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments (ASEAN, 2024).”

Though the terms "Cyberspace" and "ICTs" were not mentioned or found, the Joint Press Statement of the First ASEAN Telecommunications Ministers Meeting (First TELMIN) in 2001 tended to define ICTs as a digital tool for connectivity, as mentioned in paragraph 5, and access and spread of information in paragraph 7. 5 Emphasizing the need for communication in the information age, the paper also addresses the ASEAN Information Infrastructure (AII), ICTs, thus, can be defined as digital tools for connectivity and information. Still, ASEAN has not clearly defined cyberspace. The ASEAN Cybersecurity Cooperation Strategy (2021–2025) notes in paragraph 22 of the paper that the world is using digital as a norm, becoming the new normal, and it has evolved into a critical infrastructure and national security.⁶ Cyberspace is therefore mentioned as necessary. Furthermore, mentioned in paragraph 25 is cyberspace as the whole digital and cyberenvironment. In other words, ASEAN defines cyberspace as a global digital domain that includes the internet and virtual environments.

All in all, UN and ASEAN define AI as a system miming human cognition to make decisions and predictions. ICTs can be defined as digital tools that foster information and connectivity

via digital telecommunications, while Cyberspace is a global digital domain that includes the internet and virtual environments and can be critical to national security.

AI, Cyberspace, and ICTs: What Sets Them Apart?

AI differs from traditional digital technologies such as ICT, Cyberspace, the Internet, or the Web in that digital technology focuses on information transmission, storage, and management. In contrast, AI can "think", "act", "give advice", and "decide" wisely, imitating human. As previously stated, AI is an intelligent tool capable of producing and making nearly human-like decisions, which can help improve efficiency, quality, and productivity in all sectors and cross-sectoral sectors for human tasks. Its precision, data-driven decision-making, and prediction can have an impact in all fields, including economics, social sciences, security, and defence. Examples include:

- using AI to analyses stock trading to reduce risk,
- using AI in the health sector to help identify disease, and
- using AI as part of a national defense strategy to prevent potential cyber threats.

While that is the case, AI can also raise ethical concerns, challenge legal norms, and make monitoring and control more difficult than traditional digital technology, necessitating a different approach to AI and its governance. The unethical use of AI includes deepfakes, autonomous weapons capable of killing indiscriminately, or breaches of personal data privacy.

Legal Ambiguity

Cyberspace is the digital domain in which AI operates, and it also includes information communication technology. This interaction is critical for understanding policies governing data sharing, security, and AI deployment because these technologies do not operate in silos. However, due to AI and ICT's distinct yet interconnected nature, a clear-cut specific legal governance of the field is difficult to define. Other nations and international organizations, including the UN, ASEAN, and OECD, have been obliged to participate in a more extensive conversation of ICT and artificial intelligence to cover and apply these digital components in harmony. For instance, the OECD's 2019 AI Principles, which the UN supports and has been embraced by 42 countries, emphasize human-centric AI and trustworthy technology as guiding

concepts for harmonizing legal definitions and standards. The principle also underlines the risks and responsibilities of cross-border digital transactions, such as cybercrime and e-commerce, which face significant regulatory challenges requiring a coordinated worldwide endeavour. Practical models for including these elements in thorough policy frameworks are offered by the UN Internet Governance Forum (IGF). While ASEAN adopted a separate Guide on the ethical use of AI in 2024, the ASEAN e-commerce agreement (2019) is an early attempt to standardize legal definitions across borders for digital transactions. However, there are still gaps in how countries such as Myanmar, Cambodia and Laos address AI-driven cross-border cybercrime.

Domestically, ICT and artificial intelligence (AI) are starting to be handled separately; Singapore's AI Strategy gives ethical AI deployment, research, and talent development for essential sectors, including healthcare, top priority. Under the Smart Nation Initiative's ICT plan centres on digital connectivity, 5G rollout, and cybersecurity resilience. On the other hand, Malaysia's AI Strategy focuses on improving public services, fostering innovation, and ethical AI governance. Yet, the ICT strategy was outlined in MyDIGITAL aims to strengthen the digital economy through egovernment services, 5G deployment, and cybersecurity. In addition, Vietnam's AI Strategy focusses on AI-driven economic growth, talent development, and research collaborations. While its National Digital Transformation Programme focusses its ICT strategy on expanding digital infrastructure, providing e-government services, and ensuring cybersecurity.

Drawing on ASEAN's experience with its AI Governance and Ethics Framework, which stresses the need of a centralized entity to harmonize AI policies across member states and reflects how AI and ICT do not operate in silos and require integrated governance to manage the complexity of data sharing, cybersecurity, and cross-border digital challenges, a coordinating specific body is absolutely vital to effectively govern artificial intelligence.

Conclusion and Recommendation

For all fields and across sectors, the evolution of digital technologies, including artificial intelligence, cyberspace, and ICTs, will continue to be influential. Though they are sometimes used synonymously in the digital ecosystem, artificial intelligence, cyberspace, and ICTs represent different spheres. AI uniquely replicates human intelligence, supporting autonomous actions, datadriven predictions, and decision-making. While cyberspace is the virtual domain, including the internet and related digital environments, ICTs concentrate on the tools and systems that enable communication and information exchange. Nevertheless, the uncertainty of the term and the several interpretations can lead to ethical conundrums, legal gaps, and misinterpretation of terminology. It is advised that legal and policy frameworks clearly define AI, ICTs, and cyberspace to help lower uncertainty and improve term understanding. It is recommended that:

- Customise technology terms for particular local environments.
- Give ethical and responsible AI governance top priority, including rules for data privacy, bias avoidance, and moral use.
- Create public awareness, digital literacy, and policymaker, regulator, capacity to grasp artificial intelligence subtleties,
- Work with international organisations such as the UN and ASEAN to establish digital governance norms.

References:

- ASEAN. (2001). *Joint media statement of the first ASEAN Telecommunications & IT Ministers (TELMIN)*. <https://asean.org/wp-content/uploads/images/2012/Economic/TELMIN/presrelease/Joint%20Media%20Statement%20of%20the%20First%20ASEAN%20Telecommunications%20&%20IT%20Ministers.pdf>
- ASEAN. (2021). *ASEAN cybersecurity cooperation strategy (2021–2025)*. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-CooperationPaper-2021-2025_final-23-0122.pdf
- ASEAN. (2024). *ASEAN guide on AI governance and ethics*. https://asean.org/wpcontent/uploads/2024/02/ASEAN-Guide-on-AI-Governance-andEthics_beautified_201223_v2.pdf
- Kshetri, N. (2017). Potential roles of blockchain in fighting poverty and reducing financial exclusion in the global south. *Journal of Global Information Technology Management*, 20(4), 201–204. <https://doi.org/10.1080/1097198X.2017.1391370>
- Putra, B. A. (2024). Governing AI in Southeast Asia: ASEAN’s way forward. *Frontiers in Artificial Intelligence*, 7, 1411838. <https://doi.org/10.3389/frai.2024.1411838>
- Tan, E. E. G., & Ang, B. (2023). ASEAN ambiguity on international law and norms for cyberspace. In *Global Dialogue on Cyber Norms: Towards a Cyber Norms Architecture?* (pp. 134–150). Brill. https://doi.org/10.1163/22115897_02001_008
- United Nations. (n.d.a). *Glossary of terms: Artificial intelligence*. United Nations EGovernment Knowledgebase. <https://publicadministration.un.org/egovkb/enus/Resources/Glossary#i>
- United Nations. (n.d.b). *Glossary of terms: Cyberspace*. United Nations E-Government Knowledgebase. <https://publicadministration.un.org/egovkb/enus/Resources/Glossary#c>

United Nations. (n.d.c). *Glossary of terms: Information and communications technology (ICT)*. United Nations E-Government Knowledgebase.

<https://publicadministration.un.org/egovkb/en-us/Resources/Glossary>

** Edited with ChatGPT for clarity; all views expressed are solely those of the author.*

** The opinions expressed are the author's own and do not reflect the views of AI Forum.*