CSIS-ASPI Workshop on Persuasive Technologies

July 10th, 2024

Background

Persuasive technologies are becoming increasingly influential in shaping public opinion and behavior, raising significant concerns about their ethical implications and potential misuse. These technologies are designed to manipulate users' attitudes or actions, which can lead to widespread misinformation and the erosion of trust in digital platforms. As these technologies become more sophisticated, they pose a growing threat to individual autonomy and democratic processes.

In response to these concerns, the Centre for Strategic and International Studies (CSIS) and the Australian Strategic Policy Institute (ASPI) held a workshop in Jakarta on July 10th, 2024. The workshop focused on understanding persuasive technologies and formulating policy recommendations for governments. The objectives of the workshop were to raise awareness about the implications of persuasive technologies, consult on policy ideas for the Indonesian government, and prepare for future cognitive warfare challenges.

This closed event aimed to engage key Indonesian stakeholders, including Ministries, Government Agencies, the House of Representatives, Civil Society Organizations (CSOs), and Tech platforms. By addressing these critical issues, the workshop sought to foster a multi-stakeholder dialogue and develop actionable policy recommendations to safeguard against the misuse of persuasive technologies.

Keynote Speech

saferinternetlab.org
secretariat@saferinternetlab.org
Pakarti Centre Building
Jl. Tanah Abang III No. 23 - 27
Central Jakarta, DKI Jakarta 10160

Executive Director of CSIS, **Yose Rizal Damuri**, welcomed the participants and highlighted the importance of the event. Dr Yose pointed out that persuasive technologies exploit the behavioral shifts to influence attitudes and decision-making processes. He emphasized the collaborative effort between CSIS and ASPI, where ASPI provides insights into the functioning and evolution of these technologies, while CSIS focuses on the motivations, behaviors, and strategies of the actors involved. This holistic approach aims to develop more effective policies and interventions.

Following Dr Yose's keynote speech, **Beltsazar Krisetya**, principal researcher of Safer Internet Lab at CSIS, introduced the workshop's four thematic sessions:

1. What are persuasive technologies?
2. The role of commercial entities in online manipulation.
3. Open-source intelligence skills.
4. Preparing for the next generation of cognitive warfare.

Session 1

Albert Zhang, an analyst from Australian Strategic Policy Institute, opened the session with an overview of persuasive technologies, which are defined as information technologies designed to influence decision making, attitudes, or behavior. He highlighted the challenges of countering malign influence operations, which are increasingly driven by private actors and enterprises, alongside the rapid technological changes that complicate these efforts. Albert also provided specific examples of how private actors create urgency and influence user behavior. Key takeaways from his presentation included the profit-driven incentives behind persuasive technologies, the necessity of safeguarding users through data privacy and transparency, the importance of proactive strategies to counter malign influences, the social

cohesion challenges posed by emerging technologies, and the essential role of coordinated intelligence and policy efforts in regulating technology and data.

Albert's presentation prompted questions from government sectors, civil society organizations, and private actors. The discussion covered critical points about online manipulation and persuasive technologies, including the distinction between manipulation and online manipulation. It was noted that while persuasive efforts are typically transparent in their intentions, manipulation often lacks such clarity. Participants noted that malign actors can exploit data collected from users' reactions to promotions to further their negative intentions. The discussion also identified vulnerabilities, highlighting that the elderly and those unfamiliar with technology are particularly at risk. It was stressed that transparency can help avoid breaches. The discussion also explored algorithm confidentiality and transparency, focusing on large companies due to their significant power, and the pragmatic benefits of algorithm transparency for studies on consumers and political discourse. The privacy paradox was also discussed, revealing reluctance among several stakeholders to share data. To address these concerns, the importance of standards and transparency regarding data access was underscored.

Session 2

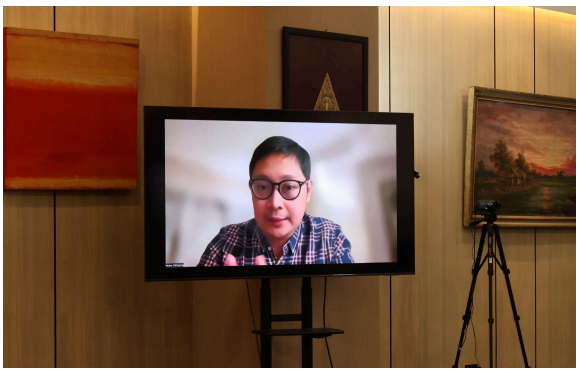
The second session began with a lecture by **Dr. Sih Yuliana Wahyuningtyas**, an associate professor at the Atma Jaya Catholic University of Indonesia, on the role of commercial entities, public relations firms, and marketing companies in online manipulation. She explored how private companies develop and offer persuasive technologies to influence people's behavior and decisions, examining the use of generative AI, immersive technologies, and wearables in online influence operations.

The presentation sparked a discussion among the participants, inviting government sectors, private sectors, and civil society organizations to share the governments' methods in creating data privacy regulations, the private sectors' mechanisms of data security and prevent public manipulation, and the role of civil society in gathering evidence related to the misuse of regulation or technology implementation.

From the private sector's perspective, they aim to help the customers and make their lives easier, while also considering ethics and regulations. Meanwhile, the government representatives highlighted gaps between the regulatory creation process and its implementation. Both the government and private sectors agreed that the regulation should not be one-size-fits-all but should be tailored to each sector or category.

Furthermore, Dr Sih Yuliana emphasized the ethical considerations and boundaries for creating market demand. Platforms should avoid manipulative practices and ensure transparency by informing consumers on the basis for product recommendations. Respecting mindful choices is crucial; consumers should not be misled in their decisions. Additionally, platforms should avoid spamming consumers with persuasive content to prevent consumer confusion. Regarding regulation, effective regulation of persuasive technology and cybersecurity requires thorough mapping to understand each business type and its target, ensuring precise and appropriate regulations.

Session 3



Shifting focus to the political aspects, the third session was opened with a pre-recorded presentation by **Noory Okthariza,** a researcher from the Department of Politics and Social Change at CSIS Indonesia. He discussed the importance of OSINT (Open Source Intelligence Technology) for understanding and countering the influence of political buzzers in elections, emphasizing the need for technical skills in OSINT and collaborative efforts between research institutions and the government to effectively counteract the influence operations and

effective policy-making.

Rifqi Rachman, a Safer Internet Lab researcher, continued with an explanation of the CSIS research, highlighting that the research mainly focused on the actors. He also mentioned that election actors use three key calculations when producing disinformation, employing various tools including OSINT. Firstly, they consider the timing, ensuring that disinformation can be produced quickly. Secondly, they focus on ease of access, making sure the generated content is easily shareable and editable to facilitate information disorder. Lastly, they calculate quantity, aiming to dominate the digital space with significant resources.

With their research experience, civil society organizations share their views and initiatives in combating information disorder using OSINT and AI technology. Both OSINT and AI technology are beneficial for their research, but they also pointed out limitations, such as understanding motives and methods of political actors.

The third session was closed by emphasizing that in data-sharing schemes with platforms, there are two types of data: (a) Open Source Intelligence (OSINT) and (b) publicly available data provided by private entities. In this context, OSINT should serve as a complement.

Session 4

The last session was held to delve deeper into the complexities of deepfakes technology and its regulatory challenges. **Alia Yofira Karunian**, a researcher of PurpleCode Collective discussed the definition of deepfakes, the technology behind it, its challenges and risks, and its potential role in disinformation and political manipulation. She also compared the regulations in Indonesia with the European Union's AI Act, Digital Services Act, and General Data Protection Regulation (GDPR) and pointed out the challenges in Indonesia regulations

such as, UU ITE and UU Data Protection. To spark discussion, she cited several studies that indicated that deepfakes increase the persuasiveness of disinformation.

Since it covered a lot about regulations, many government sectors responded by highlighting the current challenges they face. The Indonesian government currently lacks the capacity to develop comprehensive regulations for AI technology, including deepfakes, due to the complexity and rapid development of these technologies. Additionally, challenges exist in effectively implementing other existing regulations, such as the ITE Law and the Personal Data Protection Law. These challenges highlight the need to review and possibly revise current regulations to address new technological challenges. Furthermore, there is a need for a common understanding among all government agencies and stakeholders about the urgency of cybersecurity and the importance of AI regulation.

In closing the last session, Alia emphasized the need for robust policies and regulations in AI, content moderation, and personal data protection. She also highlighted the necessity for clear guidelines from authorities to address potential issues, and the importance of platform accountability in content moderation and transparency. Additionally, the relatively new AI Bill requires thorough analysis to identify regulatory gaps.

In concluding the discussion, Beltsazar Krisetya, as the facilitator, expressed hope this discussion would be followed up by formal discussions within each participants' institutions to collaboratively address issues related to persuasive technologies.

Please find the presentation materials for the event in this link:
https://on.csis.or.id/CSIS-ASPI