MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

NOTE FOR NATIONAL DEFENCE: Regulation and Need for Categorization of AI-Based Products

Authors: R. Bahrevar[1] and K. Khorasani[2]
[1] Graduate Student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- For accomplishing a coordinated investment in order to address ethical, privacy, and security aspects of AI systems and emerging and disruptive technologies, there exists a need for studying the public and defence policies for AI-based products, services, and systems that are based on categories that can represent their corresponding threats.

- Our goal is to discuss that categorization depends on a variety of parameters such as the user's age, type and nature of the application, the purpose of the AI application under consideration, to name a few.

- Furthermore, we also explain how the context matters and the higher intelligence level in an AI system does not necessarily lead or imply a greater level of AI threat.

CONTEXT

- In [1], it has been stated that AI technologies can be categorized through three dimensions, such as multi-functionality, intelligence, and user interaction. Each of these dimensions can be subjected to ethical, security, transparency, and privacy concerns. The purpose of this categorization is to help direct the efforts for tackling the AI issues.

- More interaction implies higher threats since the AI system needs higher level of features to be able to improve the user interaction [1]. For example, in infotainment applications of the smart vehicles recommendation system, besides the search history and user's preference, the location of the vehicle may be used as well [2].

- Multi-functionality also poses a great threat, since it implies that the AI device is collecting more sensory information. For example, smartphones or smartwatches, depending on the type of information they collect, such as voice, image, search history, and location [1], can be subjected to ethical, privacy, and security issues. In [1], AI intelligence is also introduced as another dimension in which a more intelligent AI system is presumed to be more threatening [1].

- However, a more intelligent AI system does not always mean more threats. Two AI products that have the same level of access to sensory devices such as cameras and microphones with internet accessibility can present the same level of security threats. The security threats depend on how much preventive and defensive mechanism an AI system offers.

- One can also define a more intelligent AI as a system that also considers the security measures.

- Here, our goal is to introduce a different way of categorization, and it is recommended that targeted regulation based on AI systems' special features, their user, or special application may lead to a better path for coordinated investment and tackling AI-related issues. One needs to make the path for policies clearer rather than obscure.

CONSIDERATIONS

- AI ethical policy concerns in cloud computing [3], facial recognition [4], and the medical domains [5].

- AI categorization based on three criteria of multi-functionality, interactivity, and intelligence, which is introduced in [1].

NEXT STEPS

- Considering the following types of regulations will help one to categorize the AI systems based on their ethical, security, or privacy concerns. Specifically:

- Regulation based on the type of information that the AI system uses. For example, consider evaluating the type of sensory devices that the AI system utilizes.

- Organizational specific policy. For example, one has to make sure private organizations do not utilize AI systems for employee behavior monitoring applications [6].

- One needs user-specific policies, where the AI system is regulated such that a more vulnerable user will be offered more protection. For a regular citizen, location information with regards to infotainment applications does not create a high-level of security concerns. However, for high-profile officials, one has to be concerned of adversaries.

- What age groups does the AI product targets? For example, the use of facial recognition systems in AI products designed for children should be of special concern.

- How much the AI system is internet dependent? What type of information is transferred and processed through the internet?

- Regulating the AI systems based on their purpose. For the AI system in the medical domain, transparency and ethical issues are of concerns. AI systems used in the vehicular ad-hoc network (VANET) can be a danger to safety of citizens.

- Regulation based on reachability of AI systems. Ones need policy specific for AI systems that can be manipulated and used as a national threat. For example, consider recommender systems in social media applications.

References

[1] Winstanley, D. and Woodall, J., 2000. The ethical dimension of human resource management. *Human resource management journal*, *10*(2), p.5.

[2] Al-Turjman, F., 2020. *Unmanned Aerial Vehicles in Smart Cities*. Springer Nature.

[3] Neto, L.D.S.B., Maike, V.R.M.L., Koch, F.L., Baranauskas, M.C.C., de Rezende Rocha, A. and Goldenstein, S.K., 2015, April. A Wearable Face Recognition System Built into a Smartwatch and the Visually Impaired User. In *ICEIS (3)* (pp. 5-12).

[4] Musaddiq, A., Ali, R., Bajracharya, R., Qadri, Y.A., Al-Turjman, F. and Kim, S.W., 2020. Trends, Issues, and Challenges in the Domain of IoT-Based Vehicular Cloud Network. In *Unmanned Aerial Vehicles in Smart Cities* (pp. 49-64). Springer, Cham.

[5] Schneeberger, D., Stöger, K. and Holzinger, A., 2020, August. The European legal framework for medical AI. In *International Cross-Domain Conference for Machine Learning and Knowledge Extraction* (pp. 209-226). Springer, Cham.

[6] Dattner, B., Chamorro-Premuzic, T., Buchband, R. and Schettler, L., 2019. The legal and ethical implications of using AI in hiring. *Harvard Business Review*, *25*.