Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

BN-53-The role of AI-May2021

REGULATION AND NEED FOR CATEGORIZATION OF AI-BASED SYSTEMS

Authors: Reza Bahrevar [1] and Kash 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 to address ethical, privacy, and security aspects of AI-based technologies, there is an urgent need to studying the policies for the AI-based product based on the categories that can represent their threat.
- Categorization issues that are discussed depend on a variety of parameters such as user's profile, type of application, and the purpose of the AI application.
- Our goal is to explain how context matters and higher intelligence levels in AI systems do not necessarily imply a greater AI threat.

CONTEXT

- In [1], it is stated that AI technologies can be categorized through three dimensions, namely 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 support and direct the efforts for tackling challenging AI issues.
- More interactions imply possibility of more threats since AI system needs a higher level of features to be able to improve the user interaction [1]. For example, in infotainment applications of smart vehicles recommendation system, besides the search history and user's preferences, the location of the vehicle may as well be used [2].
- Multi-functionality also poses a great threat, since it implies that an 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 imply 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 mechanisms an AI system offers.
- We can also define a more intelligent AI as a system that also considers and takes into account security measures.
- Our goal is to introduce a different way of categorization, and we recommend that targeted regulations based on AI systems' special features, their user, or special applications may lead to a better path for coordinated investment and tackling AI-related issues. We need to make the path for public policies clearer rather than obscure.

CONSIDERATIONS

- AI ethical policy concerns in cloud computing [3], facial recognition [4], and the medical domain [5] are of significant importance for public policy decision makers.
- AI categorization should be based on three criteria of multi-functionality, interactivity, and intelligence, as introduced in [1].

NEXT STEPS

- Considering the following types of regulations will help one to categorize AI systems based on their ethical, security, and privacy concerns:
  - Regulations based on the type of information that AI systems use are essential. For example, evaluating the type of sensory devices that AI system utilize should be considered.
  - Organizational specific policy where one would have to make sure private entities do not utilize AI systems for employee behavior monitoring applications [6].
  - User-specific policies are needed, where AI system are regulated such that a more vulnerable user will be offered more protection. For general and average citizens, location information with regards to infotainment applications do not create a high level of security concerns. However, for high-profile officials, one has to be warier of adversary malicious intentions.
  - What age groups does AI products target? 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 AI systems based on their purpose should be carefully considered. For AI systems in the medical domain, transparency and ethical issues are of outmost concern. AI systems used in the vehicular ad-hoc network (VANET) can pose serious dangers to safety of citizens.
  - Regulation based on reachability of AI systems should be carefully considered. One needs policy specific for AI systems that can be manipulated and used by malicious adversaries as a national threat. For example, recommender systems in social media applications is an area of particular concern.

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*.