Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

BN-62-Emerging technology and military application-May2021

VULNERABILITIES OF EMERGING TECHNOLOGIES: A SYSTEMATIC LITERATURE REVIEW

Authors: Saman Asvadi[1] and Mohsen Farhadloo[2]

[1] Graduate student, John Molson School of Business, Concordia University, Montreal, Canada

[2] Professor, John Molson School of Business, Concordia University, Montreal, Canada.

SUMMARY

- This note spots and categorises the vulnerabilities and problems caused by emerging technologies through a literature review and makes suggestions regarding resolving the issues.
  - The new technologies of which the vulnerabilities are being considered are:
  - Artificial Intelligence (AI), including but not limited to Machine Learning and Deep Learning
  - Internet of Things (IOT)
  - Smart Cities including Smart Homes and Self Driving Vehicles
  - Block Chains
  - Cloud Computing
  - Quantum Computing
  - Dark Web
- The vulnerabilities being investigated include:
  - Security
  - Privacy
  - Trust and confidence
  - Fairness, equality and human rights
  - Law and policy making
- Developers of these technologies need to consider such vulnerabilities, to solve the consequent problems. Policy and decision makers, on the other hand, are encouraged to be aware of these vulnerabilities to establish laws to protect human rights and safety.

CONTEXT

- In this briefing note, literature review is done to identify and categorize vulnerabilities of emerging technologies. Previous papers have considered only one technology and discussed vulnerabilities of that sole technology. To the best of our knowledge, no peer reviewed paper has been published that identify and categorize vulnerabilities of all emerging technologies, especially considering the effects on human life.
- Several papers have addressed the issue of cyber security and safety, concerning companies and organizations. Nevertheless, safety and security issues causing fear and problem for people should also be considered, as done in [1], [3] and [8].
- As new technologies emerge, new laws must be stablished to protect those who may be adversely affected.
- The issue of human rights needs much more attention by developers of new technologies. As discussed in [9], automated decision making by AI algorithms has increased discrepancies in employment, welfare and policing for immigrants and minority groups.

CONSIDERATIONS

- Artificial Intelligence
  - AI algorithms can learn very fast and automatically, even the developers cannot understand the results. As discussed in [10] computers can reset market equilibrium, by collecting data and monitoring price variations. They will retaliate against any deviation. They easily can substitute cartels, and the developers cannot understand what is happening.
  - Developing AI has led nations to get power in battlefields, and currently there is no law to stop or control such activities. Fear exists about the use of strong AI for malicious reasons [7].
  - Biases in AI algorithms had led to unintentional violations of human rights. According to [9], Facial recognition technology is now being used in criminal justice systems around the world. Instead of mitigating and controlling police work, the use of these algorithms enhances pre-existing discriminatory law enforcement practices.
- Dark Web
  - Research by Zack Brooke [14] shows that, the number of Tor hidden sites is between 7,000 to 30,000 which is 1.5 percent of the total web. However, this number is still high.
  - Marketers cannot collect data on their customers using dark web, since they don't leave any information on their identity, location or interests. Consequently, marketers have problems analysing customer preferences, and suggesting products.
- Internet of Things
  - There is a trust issue associated with IOT. It is not clear that how much data the user is willing to share. The reliability and availability of IOT services is another issue to consider. [2]
  - There are problems regarding designing protocols to guarantee safety and security measures.
- Smart Homes
  - The heterogeneous nature of smart home makes the security deployment hard. Devices work with different systems and coordinating them is hard. An Introder can easily cause problems by malicious codes.
  - There is also a fear about denial of service, from service providers.
- Quantum Computing
  - When quantum computers are built, they decipher standardised encryption in a few minutes, posing security risk to many systems working with encryption. Researchers should consider developing encryption algorithms that are secure against traditional and post quantum cryptography.

RECOMMENDATIONS AND FUTURE WORK

- Research can be done, and laws and protocols be issued to consider the person in charge of any mistake by an automatic decision-making algorithm. If an AI algorithm makes a wrong decision, who is culpable? The developer of the algorithm, the person who codes it or the one who uses the algorithm?
- Protocols should be developed to ensure security and safety of personal information as a new technology emerges, and to minimize fear of using it by public.
- Frameworks must be developed to measure the risks of using technologies, prioritize them, and plan to resolve them.

REFERENCES

[1] Alshehri, M. D., & Hussain, F. K. (2019). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing*, *101*(7), 791-818.

[2] Ng, C. K., Wu, C. H., Yung, K. L., Ip, W. H., & Cheung, T. (2018). A semantic similarity analysis of Internet of Things. *Enterprise Information Systems*, *12*(7), 820-855.

[3] Ul Rehman, S., & Manickam, S. (2016). A study of smart home environment and its security threats. *International Journal of Reliability, Quality and Safety Engineering*, *23*(03), 1640005.

[4] Figueroa-Lorenzo, S., Añorga, J., & Arrizabalaga, S. (2020). A survey of IIoT protocols: A measure of vulnerability risk analysis based on cvss. *ACM Computing Surveys (CSUR)*, *53*(2), 1-53.

[5] Ren, J., Zhang, D., He, S., Zhang, Y., & Li, T. (2019). A survey on end-edge-cloud orchestrated network computing paradigms: transparent computing, mobile edge computing, fog computing, and cloudlet. *ACM Computing Surveys (CSUR)*, *52*(6), 1-36.

[6] Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys (CSUR)*, *53*(3), 1-43.

[7] McGinnis, J. O. (2010). Accelerating Ai. *Nw. UL Rev.*, *104*, 1253.

[8] Grody, A. D. (2020). Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions*, *13*(2), 155-162.

[9] Humble, K. P., & Altun, D. (2020). Artificial Intelligence and the threat to human rights. *Journal of Internet Law*, *24*(3), 1-19.

[10] Noethlich, K. (2018). Artificially Intelligent and Free to Monopolize: A New Threat to Competitive Markets Around the World. *Am. U. Int'l L. Rev.*, *34*, 923.

[11] Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Management Review*, *13*(1), 37.

[12] Chen, C. M., Lei, D. Y., Cheng, J. H., & Huang, K. P. (2020). BLOCKCHAIN TECHNOLOGY AND BUSINESS TRANSACTION: FROM SECURITY AND PRIVACY PERSPECTIVES. *International Journal of Organizational Innovation*, *13*(2).

[13] Weber, R. M., & Horn, B. D. (2017). Breaking Bad Security Vulnerabilities. *Journal of Financial Service Professionals*, *71*(1).

[14] Brooke, Z. (2016). A marketer's guide to the Dark Web. *Marketing Research*, *28*(1), 22.