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

Security-Policy NET Nexus of Emerging Technologies

NOTE FOR NATIONAL DEFENCE: Cognitive Security Analyst and Why we Need It

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

- Our goal is to address the next-generation of emerging technologies for security operation centers that are referred to as cognitive AI.

- The cognitive AI is the next-generation technology that is introduced for improving the military decision making and for boosting cybersecurity defenses as compared to traditional IDSS (intelligent decision and support system) suffer from various shortcomings on trust and security due to the black-box nature of AI systems.

- As the nature of adversarial attacks is rapidly changing, there exists a need for an AI security defense solution and mechanism that is inherently aware of its own uncertainties and can optimally integrate with the next-generation of emerging technologies such as edge computing to enhance the performance and operations in various military applications.

CONTEXT

- Since Intelligent Decision and Support Systems (IDSS) are vulnerable to adversarial attacks, have bias and trustability problems, and cannot provide the needed flexibility of decision making in military applications, a new generation of AI security concepts is deemed to enhance the operational security against threats such as phishing, malicious data tampering, and DOS attacks [1].

- This idea is referred to as cognitive AI, where there is a mutual awareness between AI and humans. The main question is, based on an environment that the AI system is deployed, how can we achieve situational awareness [1,2]? This an important issue, specifically in military applications where there can be variables such as fatigue, needs, capabilities, and malicious intentions.

- In [2], three elements are stated as the foundation of such human-AI cooperation. Be mutual predictable, mutually directable, and have mutual common ground.

- In this Briefing Note, our goal and aim is to discuss cognitive AI, companies that are moving forward with this type of technology, what should be done to accomplish it, and what one can accomplish with this type of AI technology.

CONSIDERATIONS

- In view of the IBM QRadar Advisor with Watson cognitive AI can overcome the lack of talent and job fatigue in cybersecurity:

    - It can visualize how the attack is progressing, validate the threat, and suggest what are the possible threats that can still occur.
    - Possess cognitive reasoning for isolation of threat.
    - Provides a priority-based investigation list.

- CISCO also provides edge and fog processing, data analysis, feedback, and computation that can be a key concern in a connected battlefield:

    - Provides solutions such as joint node networks enabling soldiers to communicate via satellite.
    - Considers the technology of mobile edge computing, which can provide the networking and interconnection between the AI devices.

NEXT STEPS

- One of the main challenges of mobile edge computing is the security and trustability of exchanged information. Developing cognitive AI can provide this by bringing observability, explainability, awareness, and constant reconfiguration and learning for AI systems against AI threats.

- We need a combination of mobile edge computing and cognitive AI to bring situational and environmental awareness, as well as being able to establish a human-AI interconnection.

- For example, consider a group of scattered UAVs that are controlled by military operators and communicate with each other through military vehicles and devices that are installed/on the move in an area of operation such that together will form a mobile edge computing server. One of the cognitive AI technology's roles is to help operators to remain responsive to potential threats and assess the integrity of exchanged information between UAVs or their input/output commands.

- In terms of training the military personnel, one can collaborate with companies such as CISCO.

- One needs to establish cognitive strategies that aim to resolve cognitive challenges such as massive data, fusion of complex data, building site-specific knowledge, and maintaining multiple mental models [3].

- One needs collaboration with universities in areas that one can train edge AI and cognitive AI experts so that in the long term one can keep up with the technological advances that are mobile as well as secure against adversarial attacks, are explainable, and are aware of their environment, and human operators.

References

[1] Maymir, F, cognitive and automatic cyber defense, NATO online: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-143/MP-MSG-143-24.pdf

[2] Karel van den Bosch and Adelbert Bronkhorst, human-ai cooperation to benefit military decision making, NATO online: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S3-1.pdf

[3] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B. and Roth, E., 2005, September. Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 49, No. 3, pp. 229-233). Sage CA: Los Angeles, CA: SAGE Publications.

[4] Allen, G. and Chan, T., 2017. *Artificial intelligence and national security*. Cambridge, MA: Belfer Center for Science and International Affairs.