NOTE FOR NATIONAL DEFENCE: How to Apply AI in the Battlefield Arena?

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

- How can we achieve reliable and secure connection of AI-of-Things (AIoT) devices in military applications?
- The next-generation approach to AI systems such as cognitive AI have capabilities and functionalities that can constantly adjust and adapt to situational events. Adapting to situational events is a prominent feature of military applications and can be used for both domains of AI cyber defense and offense.
- The adversary may use advanced technologies such as cognitive AI for manipulating, disrupting, or targeting ally resources and AIoT devices. Our objective is to address the zero-trust architecture as a possible approach and solution for countering advanced AI-based adversaries in the battlegrounds.

CONTEXT

- According to [2], integration of advanced identity management, software-defined networking, and hybrid multi-cloud capabilities are deemed to provide fast and reliable cyber platforms that are needed for implementing military strategies in a zero-trust network architecture.
- In [2], it is stated that futuristic military-based cyber platforms need novel data-science algorithms, while one must also make sure the current ones operate with maximum security. In other words, one has to adapt to the notion of "verifying and never trust."
- In a zero-trust security architecture, the users are connected directly to their respective devices [3].

- There is a trade-off between connectivity and security when it comes to zero trust network architecture. In this Briefing Note, we state some of the features of this strategy and try to recommend policies that can be helpful for improving the network security in rapidly changing environments such as the battlefields.

CONSIDERATIONS

- In [2], it is stated that a zero-trust cyber platform must have certain characteristics such as the following:
    - Software-Defined Networking and ICAM (identity credential, access, and management) must be ensured to be of a zero-trust nature. For example, every device in the network must be identifiable.
    - All networks must be assumed to be vulnerable to adversarial manipulations.
    - Users should only have access to their respective needed resources.
    - One needs to provide real-time detection and protection capabilities.
    - Maintain situational awareness and must be standardized and certified.
    - Ready for fast response to emerging ISR.
    - Support multi-cloud and edge computing.
    - Have a modern and programmable software-defined networking such that they can enforce new policies.
    - Operational agility and have flexible network maneuver options.
- Organizational theories as concerned with zero-trust policies [4].

NEXT STEPS

- A zero-trust policy should follow a hierarchy starting from the received input from top commanders to shared info between the army units and the integrity of communication between the operational AI-based military equipment. The aforementioned point is mainly necessary to avoid the risk of impersonation and manipulation of IoT-based exchanges of information.
- In a zero-trust policy, no asset is trusted. Therefore, policies for the development of human-aware AI (cognitive AI) and trained professionals that are aware of their controlled AI devices should be established.
- The potential for capturing assets and reverse engineering them should be considered in the design stage [4].
- Developing new deep learning algorithms that have better observability and threat verification capability than the current ones should be considered. Current black box

models may not be observable across all their entry data such that with knowledge of output, one can obtain information on the entry data to their models.

- Policies that encourage applying, converting, and integrating organizational theories concerned with zero-trust into the battlefield framework while also reinforcing and improving the already existing policies [5] should be considered.

- Risk assessment in finding how hybrid-trust in civil applications can negatively affect national security should be investigated. Here, the hybrid trust implies that in some applications the zero-trust policies are considered, and in less critical applications such policies are relaxed to ensure IoT services are fast and less disrupted.

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] Stewart, A., 2020. Three Emerging Innovative Technologies Required for Cyber Operations to Execute Commander's Intent at Machine Speed. *Military Cyber Affairs*, *4*(2), p.3.

[3] Phillips, D., 2021. The Shape of Cloud Security in The WFH ERA. *ITNOW*, *63*(1), pp.42-43.

[4] Collier, Z.A. and Sarkis, J., 2021. The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, pp.1-16.

[5] Minu, B., McMiller, E., Kyser, J., Zenone, F., Walker, G., Cilenti, S., Sturzinger, E. and Duncan, K., 2020, March. Establishing and Maintaining Multivariate Trust in a Hierarchical SDN. In *2020 SoutheastCon* (pp. 1-7). IEEE.