MOBILIZING INSIGHTS IN DEFENCE AND SECURITY
MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy
NET Nexus of Emerging Technologies

BRIFING NOTE FOR Department of National Defence
Cyber Security in the Industry 4.0 Era

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

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

SUMMARY

- The forth industrial revolution, also known as industry 4.0, is the continuous automation of manufacturing processes, which were traditionally not automated, using merging technologies such as artificial intelligence and robotics. [4]
- Although industry 4.0 has been very beneficial in many aspects, there are various security issues inherent in it, that can cause huge problems for connected industries. [2]
- A Cyber attack may have such vast consequences, that would shut down the value chain processes for several days. Not every organization is always prepared to retain its normal states after a cyber attack. [3]
- In this era after industry 4.0, organizations highly depend on data. Therefor, security breach not only can damage thee reputation of organizations, but also can stop the work of an organization for several days, causing huge financial losses. [1]

CONTEXT

- One main reason of cyber security risks is human maliciousness. In order to quantify cyber security risk, it is essential to understand insider threat, expertise and financial motives of a hacker. [5]

- Wireless network community has searched for new routing protocols which remain sustainable in various situations and conditions. Most of these protocols rely on high energy and quality of service. As a result, a huge effort is needed to maintain network life time, quality of service, and battery autonomy. [1]

- One example of malicious behaviour is about robots which has an implanted controller which contains data. A person or group with malicious reasons can change the controller, with another one being programed by himself. This way not only can the robot sabotage the environment, but also can obtain secure data from the environment. The data can later be used by the hacker for other purposes. [6]
- As most equipment are connected to the internet, there is a high risk of cyber attacks in connected network of equipment. Such attacks can cause working down time, loss of information, and in the worst-case loss of human life.

RECOMMENDATIONS:

- Malicious thoughts and behaviours have to be considered when establishing security measures. People with malicious reasons can find vulnerabilities in systems, and write malicious codes to attack the system. [1]
- It is highly important that environments with connected intelligent equipment establish basic security rules to protect data, equipment and human lives. It is also vital to have action plans to react to any possible risk. [1]

REFERENCES:

[1] Clim, Antonio. "Cyber security beyond the Industry 4.0 era. A short review on a few technological promises." *Informatica Economica* 23.2 (2019): 34-44.

[2] Sanmartin, Paul, et al. "Sigma routing metric for RPL protocol." *Sensors* 18.4 (2018): 1277.

[3] Waslo, René, et al. "Industry 4.0 and cybersecurity: Managing risk in an age of connected production." Erişim tarihi 15 (2017).

[4] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolu

[5] Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." *Journal of advanced research* 5.4 (2014): 491-497.

[6] Fernandez-Anez, Victoria, et al. "Smart City projects assessment matrix: Connecting challenges and actions in the mediterranean region." *Journal of Urban Technology* 27.4 (2020): 79-103.