BRIEFING NOTES

#BN-42-The role of AI-Feb2021

DUAL-USE IN IT DEVELOPMENT

Authors: Bita Afshar[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

- Undoubtedly, Information Technology (IT) is a fundamental development that has affected human life during the past few decades. IT benefits educational systems, businesses, industries, transportation systems, and military services.
- Information Technology has a dual-use aspect where through its wide range of applications the important concern for the policy makers has been how to avoid, monitor or control potential threats of destructive IT applications in the society as well as the military. These issues do indeed deserve careful analysis and considerations that we are currently investigating.

CONTEXT

- The notion of dual use has drawn increasing attention from the policy community over the past years. The dilemma of dual use refers to goods, knowledge and technologies that can be used for civilian (peaceful) and military purposes [1].
- In today's world, computers and networks do not only have a crucial role in an individual's life or business processes, but also have significant impact on the nation's critical and security infrastructures [2].
- Computers have wide usage in different areas such as food delivery, transportation systems, financial organizations, and many essential critical infrastructures such as nuclear and power grids, water dams and oil and gas installations [2].
- The employment of IT is not limited to only the above commercial and civilian applications. IT has an important role in the modern military critical infrastructures such as smart weapons that are computer controlled. Moreover, military forces rely on the shared battleground information that have been facilitated through advanced IT technologies [2].
- IT industry is categorized as dual-use technology because it can be considered as a double-edge sword when deployed for harmful purposes [2].
- The importance of IT and cyberspace security is an internationally hot topic for both civilian and military projects because of the potential adverse consequences of cyber attacks [2].
- Criminals and terrorists are also utilizing cyberspace infrastructure for illegal, inhuman and immoral purposes such as committing fraud, stealing intellectual property and proceeding destructive acts [2].
- Nations utilize the wide application of cyberspace to achieve superiority not only to take measures for their defences, but also to plan strategic tactics for their offensive purposes and actions [3].
- Cyber attacks have become a new technique for interstate actors. This threat leads to new concerns for national security agencies and governments [3].

- This is where the conversion of civilian IT applications for military functions has taken place. However, it was not fully predicted and fully thought through in the initial steps of the IT development [3].

CONSIDERATIONS

- It is a sheer fact that IT has become the key contributing factor to the economical, educational, industrial, and military developments. Therefore, many organizations and institutes such as military forces have employed IT to enhance their defensive and offensive capabilities [2,5].
- The use of IT ("good" or "bad" users) could employ this technology for both beneficial or harmful targets. The policy and legal frameworks are crucial for IT applications in various domains including military aspects of the cyberspace security [2,5].
- The development of IT makes it vulnerable to cyber-attack and should be carefully monitored because of the potential dangers to nations and citizens [6-8].
- The attacker may target the IT infrastructure itself as the main target or utilize this base as a weapon to target other safety critical infrastructure of a nation [6-8].
- These attacks are initiated and facilitated based on using IT-based and networked communication data streams and have different purposes such as to gain access to a network and collect, transfer, and modify data. Finally, a significant manipulation in controlling a process can occurr through this cyber attack [9-10].
- Three pillars of network security may be aimed for network attacks that are listed as Confidentiality, Integrity and Availability (CIA). The CIA triad is a common model for developing cybersecurity and these concepts can guide policies for accomplishing information security [6-8].
- Confidentiality guarantees that information and data are not made available to unauthorized users. Integrity ensures that data or computer operations are not suffering from modifications and availability confirms that the user can access the services, applications and data [6-8].
- Cyber operations can be categorized into three different groups of cyber crime, cyber attacks, and cyber warfare [9-10].
- The notion of cyber warfare has drawn world leader's attention and it refers to actions that impact another country's network system with the aim of damage and interruption of vital infrastructures [9-10].
- To address the seriousness of this issue many state and non-state organizations are getting involved and military organizations are in charge of this situation [9-10].
- The security dilemma refers to states and their actions for the country's security and combating the enemy's threat. Nations attempt to observe each other's measures and employ state of the art technologies for defensive and offensive actions. Dual-use technologies should be monitored to decrease military conflicts among countries although dual-use legislation remain a challenging task [9-10].

RECOMMENDATIONS

- Governments can utilize special operating systems for critical infrastructure that are not known to other countries and organizations.
- Critical and security organizations can utilize clouds to improve communication and transformation of information in their safety critical infrastructure systems. It should be noted that it is not feasible for individuals to attack clouds with conventional and standard software programs.
- Quantum cryptography is another approach which can be employed to ensure and provide secure and safe data communication associated with vital critical security organizations.

REFERENCES

1-Reuter, C. (Ed.). (2019). Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. Springer.

2- https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice/section/6

3-Reuter, C., Altmann, J., Göttsche, M., & Himmel, M. (2019). SCIENCE PEACE SECURITY '19: Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research.

4- https://www.cgai.ca/canada_and_cyber

5- https://www.nap.edu/read/10415/chapter/7#136

6- Islam, M. S. (2017). Cyber Warfare and International Humanitarian.

7- https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice/section/6

8- https://www.omnisecu.com/ccna-security/types-of-network-attacks.php

9- Harris, E. D., Rosner, R., Acton, J. M., & Lin, H. (2016). Governance of Dual-Use Technologies: Theory and Practice. American Academy of Arts and Sciences.

10- Miller, S. (2018). Dual use science and technology, ethics and weapons of mass destruction. Springer.