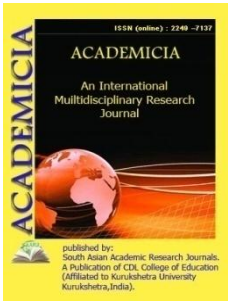
ACADEMICIA

ISSN: 2249-7137 Vol. 11, Issue 10, October 2021 Impact Factor: SJIF 2021 = 7.492

ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)



DOI: 10.5958/2249-7137.2021.02086.3

CYBER SECURITY LESSONS FROM NUCLEAR WEAPONS

Dr. Ajay Rana*; Rohit Vats**

*Shobhit Institute of Engineering and Technology,
(Deemed to be University), Meerut, INDIA
Email id: ajay.rana@shobhituniversity.ac.in,

**School of Computer Science and Engineering,
Faculty of Engineering and Technology,
Shobhit Institute of Engineering and Technology,
(Deemed to be University), Meerut, INDIA
Email id: rohit.vats@shobhituniversity.ac.in

ABSTRACT

The term "revolutions in military affairs" is arbitrary, but some inflection points in technological change are larger than others: for example, the gunpowder revolution in early modern Europe, the nineteenth-century industrial revolution, the early twentieth-century second industrial revolution, and the nuclear revolution in the middle of the last century. We may also include the information revolution in this century, which has resulted in today's very fast development of cyberspace. Earlier information technology revolutions, such as Gutenberg's printing press, had significant political consequences, but the present revolution can be traced back to Moore's law and the thousand-fold reduction in computing power prices that happened in the final part of the twentieth century. Political leaders and experts are just now starting to understand the implications of this game-changing technology. Cyber security has mainly been the province of computer professionals and specialists until recently. This tiny group was like a virtual village of individuals who knew each other when the Internet was established 40 years ago, and they built an open system with no regard for security. While the Internet is not new, the commercial Web is just a few decades old, with a user base that has grown from a few million in the early 1990s to more than two billion now. This growing interconnectedness has generated both tremendous possibilities and significant weaknesses, which strategists are now grappling.

KEYWORDS: *Cyber War, Cyber Crime, Nuclear Reactor, Nuclear War, Space Technology.*

REFERENCES

1. T. Rid, "Cyber War Will Not Take Place," *J. Strateg. Stud.*, 2012, doi: 10.1080/01402390.2011.608939.

2. T. J. Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *J. Strateg. Stud.*, 2013, doi: 10.1080/01402390.2012.739561.

3. M. Sleat, "Just cyber war?: Casus belli, information ethics, and the human perspective," *Rev. Int. Stud.*, 2018, doi: 10.1017/S026021051700047X.

4. M. Durante, "Violence, Just Cyber War and Information," *Philos. Technol.*, 2015, doi: 10.1007/s13347-014-0176-5.

5. M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, 2015, doi: 10.1016/j.cose.2014.11.007.

6. N. Kshetri, "Pattern of global cyber war and crime: A conceptual framework," *J. Int. Manag.*, 2005, doi: 10.1016/j.intman.2005.09.009.

7. P. Dombrowski and C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Nav. War Coll. Rev.*, 2014.

8. B. K. Mishra and A. Prajapati, "Modelling and Simulation: Cyber War," *Procedia Technol.*, 2013, doi: 10.1016/j.protcy.2013.12.447.

9. J. Andress and S. Winterfeld, "Chapter 16 - The Future of Cyber War," *Cyber Warf. (Second Ed.*, 2014.

10. A. Sharma, "Cyber wars: A paradigm shift from means to ends," 2009, doi: 10.3233/978-1-60750-060-5-3.