Opinion
Volume 11:6, 2022

Journal of Telecommunication System and Management

ISSN: 2167-0919 Open Access

Cyber War Defined as the Disrupting a Country's Infrastructure and Communications Systems

Stancy Ency*
Department of Telecommunications, University School of Technology, NewYork, USA

Abstract

Numerous nations have taken action to reduce the potential harm that cyber-attacks could cause. For instance, the Control System Security Program (CSSP), which includes a specialist Industrial Control Systems Cyber Emergency Response Team, is run by the U.S. Department of Homeland Security National Cyber Security Division (NCSD). Cyber war and cyber-attacks present a number of conceptual issues for geographers who are interested in peace and justice. Like everything else, war now primarily focuses on relationships.

Keywords: Satellites • Cyber-attacks

Introduction

The next year, from servers situated in Brooklyn, botnet attacks were launched against the Republic of Georgia, becoming known as "Web War I." Chinese hackers stole terabytes of data in 2009 from US Department of Defence computers related to the development and operation of the F-35 fighter jet. North Korea runs a specific cyber-attack unit called Lab 101 that has launched attacks against European and American systems and shut down South Korean institutions. Previously dismissed as a post-apocalyptic science fiction dream, cyber warfare has grown in significance as a site of political conflict.

Literature Review

Although there haven't been any fatalities from cyber-attacks to yet, their potential is huge. They have the power to bring down satellites, computer networks, electricity grids, natural gas pipelines, air traffic control systems, and any other device connected to the internet. When they devastate airport controls, banks, electrical grids, or pipelines, cyber-attacks can constitute real acts of war that may lead to retaliation in cyberspace or on the ground [1]. The potential for serious physical damage to occur through the wires is very real. These instances show how the internet has become into a battlefield for armed combat. Once dismissed as a post-apocalyptic science fiction dream, cyber warfare is now an increasingly serious issue. Significant political battleground current cyber-attacks have been small-scale, causing no casualties, but they have immense potential, including the ability to undermine air traffic management. systems, financial transactions, computer networks, electrical power grids, natural gas pipelines, satellites, and any other technological advancement linked via the internet. [2].

When they wreck airport security, whether targeting banks, electrical networks, or pipelines, cyber-attacks can genuine acts of war that could result in reprisals online or elsewhere the surface. A country's infrastructure and communications networks, especially its financial markets, can be disrupted through hacking and a variety of tools that focus on harmful code as part of cyber warfare. Similar to how governments that deny any connection to cyber-attacks frequently conceal cyber terrorism. Criminal organisations including the Russian Business Network. While there are many attacks carried out by individual hacking groups, there are also instances of well-planned attacks carried out by state military organisations, such as China's famed Unit 61398, based in Shanghai. Governments rarely publicly accuse one another of such behaviour since it is challenging to identify the perpetrators, which prevents formal declarations of war. [3-4].

Cyber War Generates New Geographies of Conflict

It is challenging to distinguish between cyber warfare, cyber terrorism, and cybercrime since, in contrast to conventional warfare, it is frequently hard to trace the origins of attacks. Typically, for cyber-attacks to be classified as terrorism, they must be the product of political, religious, or ideological motive. Cyber-attacks can take a variety of forms, including defacing websites, distributed denial-of-service attacks, and the introduction of botnets that turn computers into “zombies,” malware, trapdoors that allow unauthorized entry into ostensibly secure systems, and logic bombs, which cause a network to shut down and erase data. Most cyber assaults involve distributed denial of-service attacks or overloading targeted websites until they are no longer functional.

Cyber warfare also increases the risk that created viruses could evade containment safeguards and cause havoc with computer systems across numerous nations. As evidenced by North Korean attacks on South Korea, Syrian government airstrikes on rebel troops, and Russian strikes on Georgia, Estonia, and Ukraine, these operations also affect crucial financial and banking systems. Some initiatives have gone beyond denial-of-access to target the energy infrastructure. There are several significant ways that cyberwar differs from traditional conflict. [5].

Conclusion

Cyber-attacks, which make it more difficult for a state to protect its infrastructure, are one of the phenomena that best exemplify the increasingly permeable borders between the actual and virtual worlds that exist today. Scientists argues in Terror and Territory that several aspects of conventional warfare—such as the involvement of non-state actors and the lack of difference between combatants and non-combatants—are defied by terrorism and the so-called battle against it. Such events cast doubt on the established bond between the state and the area that it governs. Similarly, cyber war gives non-state actors the chance to wreak widespread havoc and connects perpetrators and victims across the internet..

***Address for Correspondence:** Stancy Ency, Department of Telecommunications, University School of Technology, NewYork, USA, E-mail: stency@emline.org*

Date of Submission: 06 June, 2022, Manuscript No. jtsm-22-77273; **Editor assigned:** 07 June, 2022, PreQC No. P-77273; **Reviewed:** 17 June, 2022, QC No. Q-77273; **Revised:** 22 June, 2022, Manuscript No. R-77273; **Published:** 29 June, 2022, DOI: 10.37421-2167-0919.2022.11.332

References

1. Siljak, Harui, Irene Macaluso, and Nicola Marchetti. “Artificial Intelligence for Dynamical Systems in Wireless Communications: Modeling for the Future.” *J Telecommun Syst Manage* 7 (2021): 13-33.
2. Ji, Shaoxiong, Shirui Pan, Erik Cambria and Pekka Marttinen, et al. “A Survey on Knowledge Graphs: Representation, Acquisition, and Applications.” *J Telecommun Syst Manage* 33 (2021): 494-514.
3. Feijóo, Claudio, José Luis Gómez-Barroso, and Sergio Ramos. “Techno-economic implications of the mass-market uptake of mobile data services: Requirements for next generation mobile networks." *J Telecommun Syst Manage* 33 (2016): 600-612.
4. Panwar, Nisha, Shantanu Sharma and Awadhesh Kumar Singh. “A survey on 5G: The next generation of mobile communication." *J Telecommun Syst Manage* 18 (2016): 64-84.
5. J. S. Metcalfe. "Technology systems and technology policy in an evolutionary framework." *Cambridge J Econ* 19 (1995): 25–46.

How to cite this article: Ency, Stancy. “Cyber War Defined as the Disrupting a Country's Infrastructure and Communications Systems”. J Telecommun Syst Manage 11 (2022): 332.