

# Cyber Security and Cyber Attacks

Rebecca Smith\*

Editorial Office, International Journal of Advancements in Technology, Spain

## ABSTRACT

The majority of economic, commercial, cultural, social, and governmental activities and contacts of countries are now conducted in cyberspace at all levels, including individuals, non-governmental groups, and government and governmental institutions. Many private firms and government agencies throughout the world are currently dealing with cyber-attacks and the dangers of wireless communication technologies. Protecting data against cyber-attacks is a difficult task in today's environment, which is heavily reliant on electronic technology. Cyber-attacks are designed to cause financial harm to businesses. Cyber-attacks can also be used for military or political reasons in some situations. PC viruses, knowledge breaks, Data Distribution Service (DDS), and other assault vectors are examples of these harms. To this goal, numerous businesses employ a variety of strategies to mitigate the effects of cyber-attacks. Cyber security is based on real-time data on the most recent IT data. Until now, academics from all over the world have offered a variety of ways for preventing cyber-attacks or reducing the damage they do. Some of the methods are in use, while others are still being researched. The goal of this research is to examine and review the usual advances in the field of cyber security, as well as to look into the obstacles, flaws, and strengths of the offered approaches. The many sorts of new descendant attacks are discussed in depth. The history of early-generation cyber-security methods is described together with standard security frameworks. The goal of this research is to examine and review the usual advances in the field of cyber security, as well as to look into the obstacles, flaws, and strengths of the offered approaches. The many sorts of new descendant attacks are discussed in depth. The history of early-generation cyber-security methods is described together with standard security frameworks.

## INTRODUCTION

The Internet has played a vital role in global communication for more than two decades and is becoming increasingly interwoven into the lives of people all over the world. Because of innovations and cheap costs in this field, the Internet's availability, use, and performance have considerably increased, and the Internet now has around 3 billion users globally. The Internet has played a vital role in global communication for more than two decades and is becoming increasingly interwoven into the lives of people all over the world. Because of innovations and cheap costs in this field, the Internet's availability, use, and performance have considerably increased, and the Internet now has around 3 billion users globally. The Internet has established a massive global network that contributes billions of dollars to the global economy each year. The majority of economic, commercial, cultural, social, and governmental activities and contacts of countries are now conducted in cyberspace at all levels, including individuals, non-governmental groups, and government and governmental institutions. Most critical and sensitive information is transported to this space or has been produced in this space, and vital and sensitive infrastructures and systems are either a part of cyberspace themselves or are controlled, managed, and exploited through this space. The existence of a

complete definition of a cyber-attack will surely have a direct impact on the legal environment, making it more difficult to continue and identify the consequences of this type of attack. Without a doubt, the lack of a clear and comprehensive definition not only obscures the main legal road, but also leads to differences in interpretation and practice, and, finally, too often contradicting legal conclusions.

## CONCLUSION

In the third millennium, cyberspace and related technologies constitute one of the most important sources of power. The characteristics of cyberspace, such as low entry prices, anonymity, vulnerability, and asymmetry, have resulted in the phenomenon of power dissipation, which means that if governments have so far divided the game of power among themselves, other actors, such as private companies, organized terrorist and criminal groups, and individuals, must now play a role, though governments continue to play an important role. Naturally, governments will not be deprived of their national security as a result of this phenomenon. This effect can be measured in a variety of ways. The first is the idea of safety. National security is no longer defined solely in terms of military challenges and internal and external boundaries; rather, the threat of citizens' diminishing quality of life is now a national security

**Correspondence to:** Rebecca Smith, Editorial Office, International Journal of Advancements in Technology, Spain; E-mail: [reaserch@scholarcentral.org](mailto:reaserch@scholarcentral.org)

**Received:** November 02, 2021; **Accepted:** November 13, 2021; **Published:** November 26, 2021

**Citation:** Smith R. (2021) Cyber Security and Cyber Attacks. Int J Adv Technol. 12: 124.

**Copyright:** © 2021 Smith R. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

concern. The second is the removal of cyber threats' geographical dimension. Military threats had a defined geographical location in the past. As a result, dealing with it was not difficult, at least in terms of identification. The next point to consider is the scope of cyber-threat vulnerabilities. These threats are intermittent,

multifaceted, and extremely damaging due to their association with important networks and infrastructure. Because security in the digital age is not solely a political issue, the many theoretical approaches in international relations that are primarily based on government are easily neglected or misunderstood.