

Chapter 1

The Role and Place of Cyber Warfare and Cyber Security in the World: Past, Present, Future

Nika Chitadze

International Black Sea University, Georgia

ABSTRACT

Computer security, cyber security, or information security is the protection of computer systems and control points of networks from intrusion, unauthorized use, or damage to hardware, software, and electronic data, as well as from destruction and disruption of the services they provide to users. This area is becoming more and more important as a result of increasing dependence on computer systems, the internet, and wireless networks such as Bluetooth and Wi-Fi. Because of its complexity, in terms of politics and technology, cyber security is also one of the main challenges in modern life.

INTRODUCTION

The development of digital technologies has covered all areas of human life. The technological revolution, which has brought great benefits to humanity, has increased cyber risks in virtual space. Currently, the geographical borders of the state do not represent a barrier to cyber attacks. Malicious cyber activities can be carried out covertly from anywhere in the world, by a person or groups of people from home, through a computer, without requiring special, expensive resources. It can have the same devastating effect as conventional warfare.

The speed of technology development has completely changed the international security landscape. The world is faced with massive cyber challenges. Cyber security is a global challenge that transcends state borders and requires collective international cooperation. Even though the world's leading countries, members of the European Union, and the alliance are trying to deal with cyber threats independently,

DOI: 10.4018/978-1-6684-8846-1.ch001

none of the states has been able to effectively fight against cyber challenges. The fight against cybercrime at the international level is possible only with the collaboration of countries, with a collective approach.

At a time when many countries are constant targets of cyberattacks, information-psychological operations of the aggressor Russia, and a strong disinformation campaign by the Kremlin and its allies, the role of cyber security and the development of cyber capabilities in the national security policy of various countries is vital. The country's sovereignty, territorial integrity, and stability are achieved through integration into the democratic world. Although significant research has been conducted in the field of cyber security, because cyberspace is a new challenge of an unpredictable nature, which is becoming increasingly complex and large-scale with the rapid development of digital technologies, it can be said that the underlying causes of Countries cannot unite to fight cybercrime with all their might. What prevents them from cooperating on a global level? What methods can different countries deal with modern cyber challenges, which will become even more complex and unmanageable in the era of smart technologies, artificial intelligence, and quantum computers (Svanadze, 2015)?

Cyber Security: Taking Social Media and National Security as an Example

Mass media could always play a certain positive or negative role in any country's national security issues and have a certain impact on it, the main thing was just in which direction? who and where and how it would use traditional media. In the last decade of the beginning of the XXI century, the use of social media became very popular and useful. The means have changed, while the goals and objectives, as well as the questions above, have remained the same. Media means still have the same influence on national security as traditional media, only all this has accelerated in time, events are developing and spreading faster. Social media began its existence in the 21st century in the USA, and it is developing here with geometric progression. As of 2010, there were approximately two billion social media users, nearly a third of the planet's total population. In the first stage of development, between 2000 and 2005, social media was widespread in countries with high technologies, where the indicator of the index of democracy is quite high. Since 2005, social media has started to spread in relatively underdeveloped countries, where the index of democracy is relatively low, and in some places, it does not exist at all. This fact greatly affects not only the national security of the country but also regional and in many cases international security. Traditionally, social media refers to such well-known social networks as Facebook, LinkedIn, MySpace, Twitter, YouTube, Flickr, WordPress, Blogger, Typepad, LiveJournal, Wikipedia, Wetpaint, Wikidot, Second Life, Del.icio.us, Digg, Reddit, Lulu (Lindsay, 2011).

The number of users of social networks is increasing day by day. Its rapid global spread is facilitated by the features of social media, important for the user, such as operability, rapid transfer of information and the possibility of two-way communication, cheapness, etc. Sh. Constant growth of users. However, social media has both positive and negative sides. Its misuse can adversely affect the national security of the country. However, at the same time, social media can bring a positive effect on the country, it can be used to achieve strategic or tactical goals, work on threats and prevent them in time. Social media is developing very quickly, and it is necessary to constantly monitor geo-political, geo-economic, or other types of processes by the state. As a whole, this complex process will allow us to avoid external threats and their impact on domestic events. It can be said that social media is used quite successfully by international criminal groups, including terrorist organizations. Potentially adversarial countries and alliances do not hesitate to use social media in their interests to achieve their goals. It is necessary to know how and to what extent social media can help the state prevent threats and protect strategic interests. It is

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/the-role-and-place-of-cyber-warfare-and-cyber-security-in-the-world/332278

Related Content

A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications

Ioana Lasc, Reiner Dojenand Tom Coffey (2011). *International Journal of Information Security and Privacy* (pp. 33-49).

www.irma-international.org/article/mutual-authentication-protocol-resynchronisation-capability/53014

Subjective Attack Trees: Security Risk Modeling Under Second-Order Uncertainty

Nasser Al-Hadhrami (2023). *International Journal of Blockchain Applications and Secure Computing* (pp. 1-27).

www.irma-international.org/article/subjective-attack-trees/320498

IoT and Wearable Devices: Security Challenges and Solutions

Hira Akhtar Butt, Ishal Imran, Abdul Ahad, Jamila Faridand Filipe Madeira (2025). *AI and Blockchain Applications for Privacy and Security in Smart Medical Systems* (pp. 243-278).

www.irma-international.org/chapter/iot-and-wearable-devices/378071

Information Security by Words Alone: The Case for Strong Security Policies

Kirk P. Arnett, Gary F. Templetonand David A. Vance (2009). *International Journal of Information Security and Privacy* (pp. 84-89).

www.irma-international.org/article/information-security-words-alone/34060

Enhanced Security for Electronic Health Care Information Using Obfuscation and RSA Algorithm in Cloud Computing

Pratiksha Gautam, Mohd. Dilshad Ansariand Surender Kumar Sharma (2019). *International Journal of Information Security and Privacy* (pp. 59-69).

www.irma-international.org/article/enhanced-security-for-electronic-health-care-information-using-obfuscation-and-rsa-algorithm-in-cloud-computing/218846