Chapter 9
Cyber Security Strategies:
International Experience

Liza Partsvania
International Black Sea University, Georgia

ABSTRACT

In this chapter, the main concept of cyber security strategy and policy of several states in the field of cyber defense policy are discussed and analyzed. This factor allows the authors to make a comparative analysis of the cyber security strategies of such states and organizations as NATO, the European Union, the USA, Estonia, Lithuania, and Georgia. Particularly, there are analyzed appropriate documents in the field of cyber security and cyber defense taking into account the current realities in world politics.

INTRODUCTION

In the era of technological development, every sphere of life became more dependent on the Internet, software, artificial intelligence, and online systems than ever. Revolutionary changes during the previous decades promoted business, science, education, energy, transportation, communication, healthcare, and a variety of other sectors to adjust to reality and become more digital. In a progressively internet-centered world, the importance of protecting data, assets, and other electronic information has significantly increased. Since the contemporary world is highly interconnected cyber security breaches in a particular state affect other neighboring states and not only. According to the International Telecommunication Union, “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organizations’ and users’ assets” (ITU, 2009). Cyberattacks can also cause significant damage to businesses and individuals, including data breaches, identity theft, and reputational harm.

Furthermore, cyberspace could become the theater of warfare in the 21st century when cyberattacks are targeted against a particular state. The use of cyber operations as a means of warfare in armed conflicts poses a real risk of harm to civilians. Since Russia’s illegal annexation of Crimea in 2014, there have been ongoing cyberattacks by Russia against Ukraine, which escalated right before the 2022 invasion.

DOI: 10.4018/978-1-6684-8846-1.ch009

The public, energy, media, financial, commercial, and nonprofit sectors in Ukraine have been mostly damaged during this time. Their effects have included data theft and disinformation, the use of deep fake technology, and restricting access to fundamental services. Initiatives supported by the EU, US, and NATO have been implemented to defend critical infrastructure and avoid cyber threats to strengthen Ukraine's cyber defense. The case of Ukraine proves the significance of developing a National Cyber Security Strategy to understand the enemy's tactics, techniques, and procedures and respond effectively to any cyberattack during the war.

To address the global challenge of cybersecurity that significantly influences all institutions on national and international levels, the international community has been working to collectively develop plans for defense of the cyberspace. The Enhanced Cyber Defense Policy of NATO recognized cyberspace as a vital element of NATO's collective defense in 2016. It is outlined that "a decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."[1] NATO, EU, and other partner states have developed the National Cyber Security Strategy - the conceptual document that encompasses the existing cyber threats and challenges and provides essential strategical information, the tools, and approaches to defend critical infrastructure and guides states to strengthen their cyber resilience. This chapter analyzes the international cyber experience in the example of the United States and the European Union. It provides a detailed discussion of national cyber security policy and the recommendations that the international community should adopt to improve cyber resilience.

The Experience of the Different Countries in the Field of Cyber Security Strategies

The main conceptual document for ensuring cyber security is the national cyber security strategy, which includes the challenges and threats facing the country, and an action plan to overcome these challenges. Every state needs to have a strong cyberspace. Cyber security is a global challenge that transcends national borders and requires increased cooperation at the international level. At the 2014 Wales Summit, NATO member states declared cyber defense a key component of collective defense and stated that a cyber attack could trigger Article 5 of NATO's collective defense (Global Affairs Press, 2022). NATO member countries have begun to develop joint defense mechanisms. NATO, EU, and US partner countries have developed cyber security strategies to collectively address global cyber challenges.

The cyber security strategy is an important document that ensures the cyber resilience of the country. This chapter presents international experience, which includes an overview of cyber security strategies of the European Union, America, Estonia, and Lithuania and a detailed, comparative analysis of cyber security strategies of Georgia. On December 16, 2020, the European Union adopted a new strategy for combating cyberattacks, which involves joint actions with EU members and partner countries to combat cybercrime. In July 2021, the European Union, for the first time in its history, imposed sanctions in response to cyber attacks on the EU (European Commission, 2022).

According to the strategy:

- EU countries should ensure the security and stability of cyberspace through joint efforts;
- to strengthen the collective capabilities of combating cyber threats, to help member countries to protect the national security of the country, to counter cyber-attacks jointly;