Chapter 12
EU's Cyber Security Strategy Before and During the War in Ukraine

Tamari Bitsadze
International Black Sea University, Georgia

ABSTRACT

This chapter first examines the European Union's cyber security strategy and then analyzes the common principles of the member states in this regard. The authors discuss the European Union's role in the advancement of cyber security. In addition, the chapter reviews the EU Convention on Cybercrime. Most importantly, they discuss the impact of the most important and relevant issue, the Russia-Ukraine war, on the EU's cyber security strategy and investigate what changes and challenges the ongoing conflict in Ukraine has brought to the EU's cyber security strategy.

INTRODUCTION

In the modern world, informational war has become a bigger weapon than the physical one, since the beginning, the victory of the informational war in many cases meant the victory of physical war as well, a clear example of this is World War II, where, although the concentration camps were created by the Soviet Union before Germany, it did not trust the Jews either, that to this day, when we mention the concentration camp, it is associated with Germany, because it correctly calculated the methods and ways of spreading information.

The twenty-first century is the century of information technology; technologies have advanced to the point that any interested person can obtain real-time information from any location on the planet. As a result, information manipulation plays a critical role in the shaping of public opinion, and hence in the execution of effective policies.

Due to accessibility, so-called social media has become popular. Spread of fake news disinformation, various services, groups, and organizations purposefully spread disinformation against opponents, social

DOI: 10.4018/978-1-6684-8846-1.ch012

media has become an alternative arena of war, where weapons are words and materials, it can potentially lead to real war, and not only that, industrialization and the rapid spread of information have increased people's feelings of nationalism, and thus the materials spread here can cause a feeling of protest that will bring the community together and take it to the streets (Barry M., Vinton G., David D., Robert E., Kleinrock L. 1997).

If until now TV, radio, and written media were used for information warfare, now information technologies, cyber-attacks, and especially social media are the main sources. Cyber-attacks are used for various purposes, such as obtaining secret information, as well as creating an information vacuum, hindering the obtaining of information, suppressing, damaging the opponent's networks, etc. Social media and social networks such as Facebook, Instagram, and Twitter are used as a means of information warfare on a larger scale.

Information warfare can include (Reisman & Antoniou, 1994): Obtaining tactical information; Distributing propaganda and disinformation to misrepresent and manipulate the opponent; Confirming the accuracy of information; Preventing the opponent from gathering information; Distorting and misrepresenting the opponent's information. It follows from the name of information war that the war takes place through information, and the main source of information dissemination is information technology, this is where cyber security is involved, which should provide defense against various constituent parts of information war.

The European Union is the leading entity in the world in terms of activity, developed strategies and projects in terms of cyber security, cyber security is often the main topic at various conferences and meetings of the European Union, moreover, cyber-attack is considered the most urgent problem in the European Union. This topic is overseen by special agencies: "European Union Network and Information Security Agency" - ENISA, European Cybercrime Center - EUROPOL/EC3, European Defense Agency - EDA. There are also non-profit (Non-profit) self-financing organizations in the field of cyber security. The fact that so much attention is paid to the topic of cyber security makes it clear how seriously the European Union takes this issue.

Apart from various terrorist organizations, the biggest threat to the European Union is the Russian Federation, especially in cyberspace, where Russian propaganda is particularly active. Fighting through propaganda is nothing new for Russia; during the Soviet Union, a separate direction called "special propaganda" was taught. However, in Putin's Russia, these approaches have become particularly active; Russia actively leverages the advancement of information technology to disseminate disinformation and propaganda.

Anti-Western propaganda is a part of Russia's information war, they present the European Union and the West in general as countries against traditions, Europe is a nest of depravity. In doing so, they present their own superiority and pretend that it is their duty to protect the conservative values of the state.

In Russia, the presence of non-governmental organizations is strictly controlled, and similar organizations financed from Europe are practically minimized. The EU is always one step behind when it comes to Russian propaganda and disinformation, not because Russia is strong or Europe is weak, but because of the difference in political views and political cultures between the two sides. In Russia, fighting with similar methods is accepted, and blocking the opponent's opinion with different methods is part of their policy. Unlike Russia, one of the main values in Europe is freedom of speech, therefore it is not possible to control disinformation. Due to Russia's active information warfare, there is no other way for the EU countries to take some steps, one of the first was the UK law, which involves putting internet trolls who are clearly harmful in a penitentiary for 6 months. Corresponding legislation is also being developed in various EU countries (Čižik T., 2017).