# Chapter 11
# The EU's Cyber Security Strategy:
## The Question of Cyber Crime Management and Challenges in Europe

**Mukesh Shankar Bharti**
https://orcid.org/0000-0002-3693-7247
*Jawaharlal Nehru University, India*

## ABSTRACT

*This chapter aims to discuss the EU's cyber security strategy and how its policy is capable of restricting cybercrime in Europe. The study explains the role of EU Member States in dealing with cybercrime in this region. This research draws on qualitative comparative analysis to examine various EU initiatives to tackle cybercrime issues in Europe. Furthermore, this chapter discusses the core literature of primary and secondary resources through an empirical approach. Since globalisation reached its highest level across the world, the question of cyber security has emerged as a key area of multiple cooperation between the global actors. Cybercrime is now a complex issue among the global actors to restrict its expansion. The EU also started cooperation with Asian, American, and African countries on cybercrime issues. Finally, this chapter suggests that cybercrime is the central area of cooperation between the global actors to restrict it which is dangerous for humanity.*

## INTRODUCTION

The European Union (EU) is the largest political and economic platform of the regional organisation in Europe. Since 1951, it has been shaping multiple cooperation and public diplomacy in the EU and non–EU countries in Europe and have been establishing bilateral cooperation at the continental level. Through strategic partnerships, the EU is committed to working with other countries around the world

DOI: 10.4018/978-1-6684-8846-1.ch011

on cybercrime issues. It is an emerging question of how to tackle cybercrime between major economic blocks at the global level. The EU's policy is to provide security from cyber threats and strengthen trustworthy digital technologies to build resilience to cyber threats and provide a safe and secure digital world to protect their citizens and businesses. The EU faces descriptive and normative challenges in Europe and its policy is binding against internal and external security threats to limit these types of cybercrime. Thus, the EU policies are intensely working to protect of potential security issues in Europe. The EU's very keen to target the most urgent security threats, such as terrorism, organised crime, cybercrime, and cross-border issues. The EU's policies and management seem to secure its external borders and protect against civil disasters. The first EU "Cybersecurity Strategy" came into force in 2013 as a formal setting out of a new policy as security armor to protect against the possibilities of potential danger in Europe (European Commission and High Representative, 2013).

This chapter provides an extensive overview of cybercrime management and policies regarding sought out the major challenges in the EU. The chapter also aims to delve into the current state of the cybersecurity landscape in Europe. It has deeply analysed the EU's key agenda and legislative initiatives in an attempt to operate cybersecurity. Through the EU policy area, the EU seriously identifies the main challenges and conceptualizes the main areas of use of the legislation. Furthermore, the EU is focusing on and triggers to shape cybersecurity regulation between the member states. The EU's first priority and commitment are to provide security to its people in Europe and restrict any possibility of danger outside the border. In recent years, the EU's focus on pragmatic work on digital dependency always seems to unify the legal framework of constitutions. According to Ramses Wessel, cybersecurity forms "an excellent example of an area in which the different policy fields need to be combined (a requirement for horizontal consistency), and where measures need to be taken at the level of both the EU and Member States (calling for vertical consistency)" (Wessel, 2015). The EU's common understanding is that cybersecurity entails a combination of cybercrime, resilience, cyber defence, cyberspace and several concurrent concerning issues. EU diplomacy must work on these issues, which is a priority to ensure a secure Europe. The 2013 Strategy aimed to work on the abolition of prior cyber-attacks and want to achieve "to make the EU's online environment the safest in the world" (Fuster & Jasmontaite, 2020).

The EU and non-EU economies are also affected by cybercrime activities against citizens and the private sector. Cybercriminals are using increasingly sophisticated methods to interfere in the theft of critical data and information systems. They are also involved in ransoming businesses. The increase in economic espionage and state-sponsored activities in cyberspace constitutes a new category of threats for EU governments and businesses. Thus, cybercriminals cheat even the biggest entrepreneurs and sometimes the public sector is also cheated by online fraud. Although, the EU had decided to take strong action through legislation and common consensus among the member states (European Commission, 2013). The EU is also aware of the misuse of cyberspace for surveillance and control of its own citizens by governments.

## Framing Cybersecurity as a Policy Area

The European Union's activities came to light in the field of cybersecurity and combating cybercrime in the 1990s. At that time, the EU adopted the first non-binding legal acts to regulate and deal with cybercrime issues in Europe. The European Union Agency for Cybersecurity (ENISA) was set up as The European Network and Information Security Agency on the 15th of March 2004 by way of Regulation (EC) No 460/2004 of the European Parliament and of the Council of the 10th of March 2004 establishing