Cybercrime in Europe and Beyond: The Budapest Convention

# I. Introduction

Present day, cybercrime is a category of crimes that is widespread because technology has become a part of life, as almost all daily human activities use technology. Cybercriminals take advantage of such technologies to commit various cybercrimes, leading to huge losses on the part of victims. Cybercrime is an activity that uses computer technology as the main component.  
  
Cybercrime refers to any criminal activity in which computers or networks are a central component. This includes:  
- Fraud and identity theft (e.g., phishing or hacking),  
- Cyberbullying and online harassment,  
- Data breaches and system sabotage,  
- Intellectual property theft,  
- Child sexual exploitation online.  
  
In broad terms, computer fraud , in particular, is a prominent threat. It typically involves manipulating data, inserting false information, or giving deceptive instructions. Unlike technical attacks, such crimes often exploit human error and are emotionally damaging, making legal prosecution more challenging.  
  
These offenses have existed in analog form long before digital technology, but now criminals have faster, broader-reaching, and harder-to-trace tools. As a result, governments and international bodies have been forced to reconsider how crime is defined and combated in the digital age.

# II. Historical Context and the Emergence of the Budapest Convention

By the late 1990s and early 2000s, cybercrime had escalated significantly, exposing the global vulnerability of digital systems. Two major incidents highlighted this urgency:  
  
The Melissa Virus (1999) and The ILOVEYOU Worm (2000) : Viruses were two early and highly disruptive email-based cyberattacks that underscored the increasing threat of computer viruses. Melissa emerged in March 1999, created by David L. Smith, who disguised a malicious Word document as a harmless file. Once opened, the virus used Microsoft Outlook to automatically send itself to 50 contacts in the victim’s address book. The rapid spread overwhelmed email systems, forcing companies like Microsoft, Intel, and even the U.S. Marine Corps to shut down communications. Over a million email accounts were affected, causing damages in the hundreds of millions of dollars. Smith was arrested soon after and sentenced to 20 months in prison.

Just a year later, in May 2000, the ILOVEYOU worm appeared, originating in the Philippines. It arrived via email with the subject “ILOVEYOU” and an attachment that seemed like a love letter. Opening it triggered a Visual Basic script that replicated itself to all contacts and began overwriting various files, leading to severe data loss. Tens of millions of computers were infected within days, causing an estimated $10 billion in damages globally. Although the perpetrators were identified, they faced no legal consequences due to the lack of relevant laws in the Philippines at the time.

In response to these rising threats, the Council of Europe adopted the Budapest Convention on Cybercrime — the first and only binding international treaty on this issue. Though initiated in Europe, it is open to countries globally.  
  
The 2001 Budapest Convention on Cybercrimes regulates the formulation of criminal policy in order to protect the public from cybercrime and to increase cooperation between countries in dealing with such crime. Even though the convention was organized by the Council of Europe, this international agreement is also open to non-European countries. The Convention has rules that help countries agree on what cyber activities should be considered crimes.

These rules cover four main areas.

The first area relates to crimes against the security of computer data and systems. This includes things like hacking, interfering with data, damaging systems, and misusing devices. These are the most common types of cybercrime and are important to protect all digital systems.

The second area focuses on common crimes that can happen online, such as fake documents and online fraud. Even though many countries already had laws against these crimes, the Convention helps them work together and follow the same rules.

The third part deals with crimes involving child pornography. This is a serious issue because technology makes it easier for predators to reach children and share illegal material. The Convention aims to fight online child abuse and protect children from exploitation.

The fourth area covers crimes related to copyright and intellectual property. As more creative works are shared online, this part helps protect rights holders and prevent illegal sharing of protected content.

Examples of National Implementation

* France

Modified its digital economy law to comply with the Convention.

Uses it in investigating online drug and counterfeit product networks.

* Finland

Updated the Criminal Code and adopted the Coercive Measures Act to include Budapest Convention provisions.

Uses the treaty for remote searches and evidence collection in cyberattacks.

* Spain

Refers to the Convention in judicial rulings and training materials.

Amended laws to cover expedited preservation, production orders, and search/seizure of digital evidence.

* Hungary

Uses Article 32 to access publicly available or consented cross-border data.

Provided examples of successful prosecutions using treaty mechanisms, including child abuse and hacking cases.

# III. Ongoing Relevance and the Need for Global Cooperation

Regardless of how comprehensive a country's domestic laws may be, the international scope of cybercrime makes global cooperation essential. This cooperation may be necessary to gather evidence of illegal activities or to apprehend the perpetrators. A recent illustration involves law enforcement agencies from 13 nations jointly targeting a network of suspected child sex offenders operating the online forum 'boylover.net,' which is believed to have up to 70,000 members worldwide.

Chapter III of the Convention emphasizes international collaboration, especially regarding extradition and mutual assistance. It establishes the principle that parties will cooperate "to the widest extent possible" in cybercrime investigations and the collection of electronic evidence (article 23). This includes sharing information without prior requests if it aids another country's investigation (article 26). Additionally, parties are required to set up a 24/7 contact point to facilitate assistance in cybercrime investigations (article 35). Provisions are also established for mutual assistance, reflecting the procedural powers outlined earlier. Specifically, since evidence may be deleted before conventional legal processes are initiated, measures are in place for the rapid preservation of stored computer data and the swift disclosure of traffic data (articles 29 and 30). This ensures that evidence can be preserved or communication pathways identified while awaiting further requests. Regarding real-time collection of traffic data and interception of content data, parties are expected to provide such assistance as allowed by their national laws and applicable treaties (articles 33 and 34).

More recently, this commitment to international cooperation took a big step forward with the adoption of the United Nations Convention against Cybercrime in December 2024. After five years of negotiations, and with input from governments, civil society, tech experts, and the private sector, the United Nations General Assembly approved this landmark treaty. The new Convention creates a global platform for collaboration—not only to improve the exchange of evidence and protect victims but also to uphold human rights in the digital world. As UN Secretary-General António Guterres said, it’s a true victory for multilateralism and a powerful tool for building safer digital societies. Importantly, this Convention doesn’t just address traditional cyber threats. It also tackles emerging crimes like online child exploitation, digital financial fraud, and cyber-enabled human trafficking—while pushing for capacity building and support in less digitally advanced countries. The Convention will officially open for signatures in 2025 at a ceremony in Hanoi, Viet Nam. Once ratified by at least 40 countries, it will enter into force—marking the beginning of a new era of global cybercrime enforcement.