Politecnico di Torino

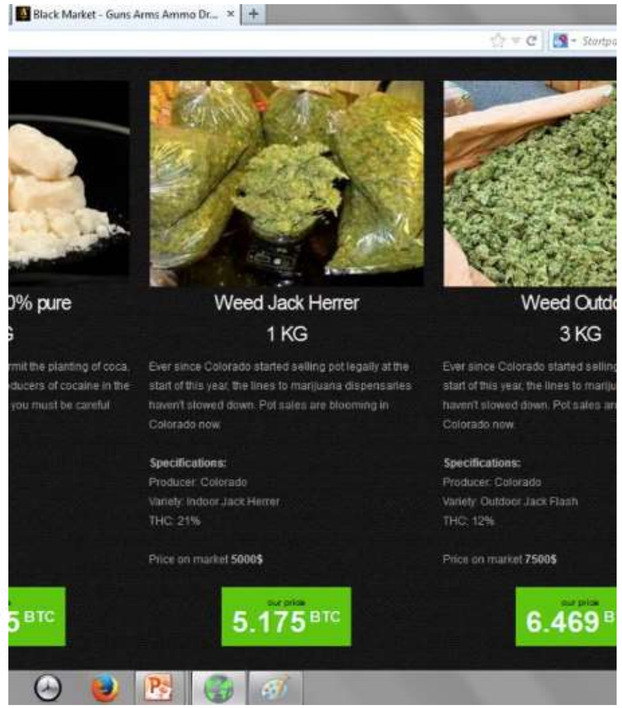
Computer Forensics
Class 2024/2025

Chapter 3: Cybercrime Convention

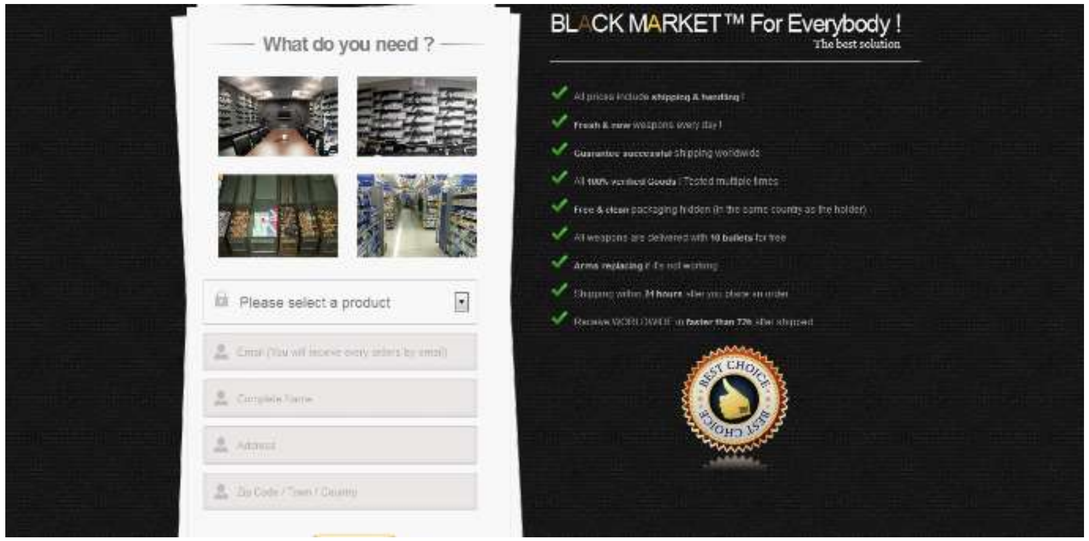
E-commerce on the Dark Web

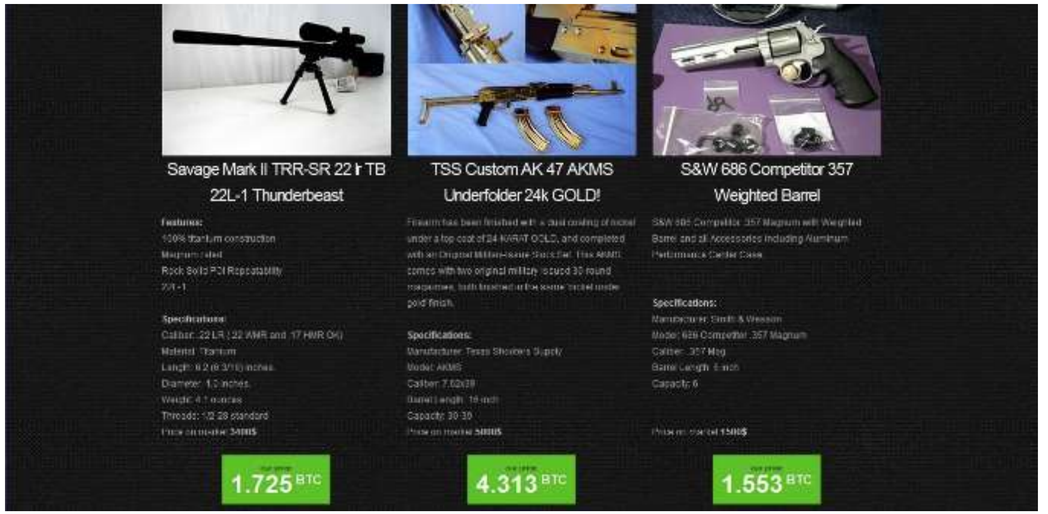
The Dark Web provides a platform for buyers and sellers to engage in e-commerce transactions, often involving illicit goods and services. This anonymous marketplace operates with the same principles as traditional e-commerce, but with heightened security and privacy measures to conceal identities.

Vendors on the Dark Web offer a wide range of products, from drugs and weapons to stolen data and hacking services. Buyers can browse listings, read reviews, and complete purchases using cryptocurrencies, all while maintaining a high degree of anonymity.



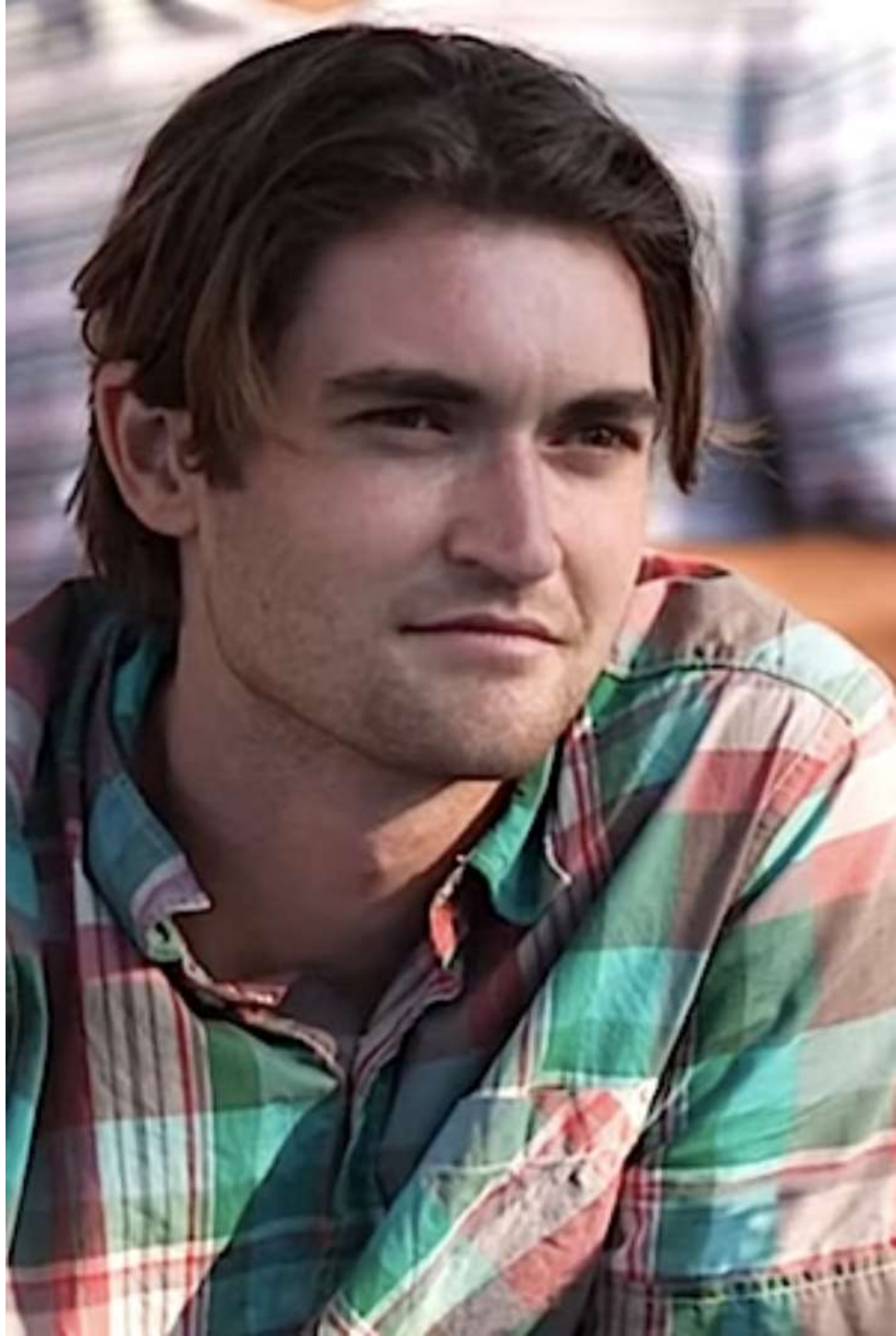

When will I get my order?
You will get your order info instantly and the physical order within 72 hours after Your payment. You can use your tracking number to contact us if you have any problem with our service.
How can I pay ?
For payment we prefer Bitcoins. You must use a Bitcoin Wallet to make the payment for our service. Other payment methods are not currently available.
How can I order ?
Select product, enter valid email and shipping address, click buy and send the CORRECT amount of bitcoins to the deposit address. After 4 confirmations (approximately 15 minutes) the product details and walkthrough guide will be sent to your email. If you have any further questions, don't hesitate to ask us.
TOP QUALITY
PREMIUM QUALITY GUARANTEED
BEST CHOICE
How can can we guarantee the successful shipping?
We guarantee the successful shipping because we have a good contact in the major Customs and Border institute and we have more than hundred type of packaging to make sure it arrives without any problems. If you have any problems, contact us via
Will I get a replace, if the account isn't valid/working/defect?
Yes, there's a replace time of 1 week. That means, You will get a new one, if you proof its invalidness by photo or by webcam within 1 week after delivery.
We are verified sellers on TCF and HB forum with good reviews.
If you want to see our reviews or leave us a feedback click here. The easiest way to really get started with us is to check out the full list of product and try to buy one


What do you need ?
Please select a product
BLACK MARKET™ For Everybody !
The best solution
All prices include shipping & handling !
Fresh & new weapons every day !
Guarantee successful shipping worldwide
All 100% verified Goods ! Tested multiple times
Free & clean packaging hidden (in the same country as the holder)
All weapons are delivered with 10 bullets for free
Arms replacing if its not working
Shipping within 24 hours after you place an order
Receive WORLDWIDE in faster than 72h after shipped
BEST CHOICE


Savage Mark II TRR-SR 22 lr TB 22L-1 Thunderbeast
Features:
100% titanium construction
Magnum rated
Rock Solid POI Repeatability
2Oz+1
Specifications:
Caliber: .22 LR (.22 WMR and .17 HMR OK)
Material: Titanium
Length: 8.2 (8 3/16) inches
Diameter: 1.5 inches
Weight: 4.1 ounces
Threads: 1/2-28 standard
Price on order: 340$
1.725 BTC
TSS Custom AK 47 AKMS Underfolder 24k GOLD!
Firearm has been finished with a dual coating of nickel under a top coat of 24 KARAT GOLD, and completed with an Original Military-Issue Stock Set. This AKMS comes with two original military issued 30 round magazines, both finished in the same nickel inside gold finish.
Specifications:
Manufacturer: Texas Shooters Supply
Model: AKMS
Caliber: 7.62x39
Barrel Length: 16 inch
Capacity: 30-30
Price on order: 5000$
4.313 BTC
S&W 686 Competitor 357 Weighted Barrel
S&W 686 Competitor .357 Magnum with Weighted Barrel and all Accessories including Aluminum Performance Carrier Case.
Specifications:
Manufacturer: Smith & Wesson
Model: 686 Competitor .357 Magnum
Caliber: .357 Mag
Barrel Length: 6 inch
Capacity: 6
Price on order: 1500$
1.553 BTC

Silk Road

Silk Road, often referred to as the "eBay of drugs," was an online marketplace that facilitated the sale of a wide range of illegal substances, including narcotics and controlled substances. At its peak in 2013, Silk Road had a reported annual revenue of $89.7 million.



Silk Road

1 **Combining Tor, PGP, and Bitcoin**

Ross Ulbricht leveraged the anonymity of Tor, the encryption of PGP, and the decentralized nature of Bitcoin to create the Silk Road marketplace.

2 **Bitcoin-only Payments**

Silk Road required all transactions to be conducted using Bitcoin, providing an added layer of anonymity and making it harder to trace purchases.

3 **User-friendly Interface**

Silk Road featured a well-designed interface that allowed users to easily navigate the site and leave feedback on their transactions.

4 **Intermediary Role**

Silk Road acted as an intermediary, handling the payment processing and logistics of shipping items purchased on the marketplace.

Silk Road Investigations

Operation "Marco Polo"

Undercover agents from the DEA and Secret Service were involved in extorting money from Ulbricht and attempting to threaten him.

Silk Road's Scope

At its peak, Silk Road had over 950,000 registered accounts, 1.2 million transactions, and nearly $79 million in commissions.

Incriminating Errors

Ulbricht made critical mistakes, like using his personal email and having counterfeit documents delivered to his home address.

Charges Against Ross Ulbricht

Summary of Charges

Ulbricht faced 7 key charges, including drug trafficking, money laundering, and computer hacking, which were consolidated into 3 main counts against him.

Legal Process

The trial lasted just 13 days and resulted in Ulbricht's conviction and life sentence, plus $180 million in damages.

History and objectives of the Convention on Cybercrime (Budapest Convention)

Budapest Convention on Cybercrime - Overview

- Purpose:
  - Harmonizing national laws on cybercrime
  - Improving investigative techniques
  - Increasing international cooperation

Involved Entities

- Albania
- Andorra
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Belgium
- Benin
- Bosnia and Herzegovina
- Brazil
- Bulgaria
- Cabo Verde
- Canada
- Cameroon
- Chile
- Colombia
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cyprus
- Czechia
- Denmark
- Dominican Republic
- Estonia
- Finland
- Fiji
- France
- Georgia
- Germany
- Ghana
- Greece
- Grenada
- Hungary
- Iceland
- Israel
- Italy
- Japan
- Kiribati
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Mauritius
- Monaco
- Montenegro
- Morocco
- Netherlands
- Nigeria
- North Macedonia
- Norway
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Moldova (Republic of)
- Romania
- San Marino
- Senegal
- Serbia
- Sierra Leone
- Slovakia
- Slovenia
- Spain
- Sri Lanka
- Sweden
- Switzerland
- Tonga
- Tunisia
- Türkiye (Republic of)
- Ukraine
- United Kingdom
- United States of America

Timeline and Ratifications

- Full Adoption: Committee of Ministers of the Council of Europe, November 8, 2001
- Signature: Budapest, November 23, 2001
- Entry into Force: July 1, 2004
- Participating States (as of April 2023):
  - 68 States have ratified
  - 2 States signed but not ratified (Ireland, South Africa)

Criticism and Opposition

- India: Initially refused to adopt due to non-participation in drafting
- Reconsideration (since 2018): Surge in cybercrime, but concerns about data sharing with foreign agencies remain
- Russia: Rejected due to concerns about sovereignty, limited cooperation in international investigations

New Global Cybercrime Treaty (UN, August 8, 2024)

 Content:

- Criminalization of unauthorized access to information systems
- Crimes related to online child exploitation and non-consensual explicit content distribution

 Criticism

- Concerns over human rights and press freedom
- Issues with data privacy and overly broad definitions of cybercrime

The Aim of The Convention

- The convention aims to help in the fight against crimes that can only be committed through the use of technology, where the devices are both the tool for committing the crime and the target of the crime, and crimes where technology has been used to enhance another crime, such as fraud. It provides guidelines for any country developing domestic laws on cybercrime and serves as a basis for international cooperation between parties to the convention.
- The first additional protocol aims to criminalize the dissemination of racist and xenophobic material through computer systems, along with racist and xenophobic-motivated threats and insults.
- The second additional protocol aims to provide common rules at international level to enhance cooperation on cybercrime and the collection of evidence in electronic form for criminal investigations or proceedings.

Key points of the Convention (1 July 2004)

- The convention covers:

  - the criminalisation of conduct – ranging from illegal access, data and systems interference to computer-related fraud and dissemination of child abuse material;
  - procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime;
  - efficient international cooperation between parties.

- Parties are members of the Cybercrime Convention Committee and share information and experience, assess implementation of the convention or interpret the convention through guidance notes.

- Of the 27 Member States, 26 have ratified the convention – Ireland has signed but not yet ratified it.

Key points of the Additional Protocol 1 (1 March 2006)

- This protocol extends the scope of the convention to cover xenophobic and racist propaganda disseminated through computer systems, providing more protection for victims. It furthermore:

  - reinforces the legal framework through a set of guidelines for criminalising xenophobia and racist propaganda in cyberspace;

  - enhances the ways and means for international cooperation in the investigation and prosecution of racist and xenophobic crimes online.

Key points of the Additional Protocol 2 (8 August 2024)

- This protocol aims to further enhance international cooperation.

- It addresses the particular challenge of electronic evidence relating to cybercrime and other offences being held by service providers in foreign jurisdictions, but with law enforcement powers limited to national boundaries.

- Its main features are:
  - a new legal basis permitting a direct request to registrars in other jurisdictions to obtain domain name registration information;
  - a new legal base permitting direct orders to service providers in other jurisdictions to obtain subscriber information;
  - enhanced means for obtaining subscriber information and traffic data through government-to-government cooperation;
  - expedited cooperation in emergency situations including the use of joint investigation teams and joint investigations.

Harmonization of national laws and international cooperation

International Cooperation Provisions

- Cooperation Principle:
  - Parties are to cooperate "to the widest extent possible" in investigating electronic evidence.

- Expedited Mutual Assistance
  - Issue with Current Mechanisms: Mutual assistance requests are often slow and take months.

- Convention solution:
  - Allows for expedited requests using "expedited means of communication"
  - Expedited means must provide adequate levels of security and authentication.

- Voluntary Information Sharing:
  - Parties may share information without a formal request if it would assist in investigations or help the receiving party with any related offences.

Mutual Assistance Provisions

- Procedural Powers for Assistance:
  - Expedited Preservation of stored computer data.
  - Expedited Disclosure of traffic data.
  - Real-time Collection of traffic data and interception of content data: parties provide assistance according to domestic laws and applicable treaties, subject to any reservations.

- Art 23 - General Cooperation Principle:
  - Mutual assistance "to the widest extent possible" for:
    - Cyber-related offences.
    - Collection of electronic evidence for any criminal offence.

- Restrictions:
  - Cooperation may be restricted in cases of:
    - Extradition.
    - Mutual assistance regarding real-time collection of traffic data.
    - Interception of content data.

24/7 Network for Immediate Assistance

- Provision for Constant Availability:
- Each party must designate a contact point available 24/7

- Purpose: Provide immediate assistance for cybercrime investigations, proceedings, or the collection of electronic evidence

- Based on the G8 network of contact points model

- Significance: aims to expedite the processing of urgent mutual assistance requests, overcoming current delays in traditional bureaucratic channels.

3.3 Legal measures against computer-related fraud and forgery

Criminalization of Fraud and Computer-related Forgery

- The Convention requires State Parties to criminalize specific conducts, including fraud and forgery carried out through computer systems. This includes, for instance, digital document forgery and fraud involving the use of electronic data to deceive or gain financial benefits.

- Computer-related fraud involves using computers to gain economic benefits through deceit, while forgery includes altering or creating digital documents with the intent to mislead.

Procedural Law Tools

- To effectively address these crimes, the Convention introduces procedural law tools that allow for quicker and more effective investigations. For example, expedited preservation of volatile data and seizure of information are crucial tools for gathering evidence in investigations against digital fraud and forgery.

- The Convention mandates that criminal justice authorities must be able to use effective means, such as search and seizure, and access stored data in computer systems, regardless of the type of crime involved.

Computer-Related Forgery

- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, **alteration, deletion, or suppression of computer data**, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Computer-Related Fraud

- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

  a) **any input, alteration, deletion or suppression of computer data**,
  b) **any interference with the functioning of a computer system**

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. .

3.4 Procedural powers for law enforcement (e.g., search and seizure of stored computer data)

Synopticon and Omnipticon

"Synopticon": The many watch the few

"Omnipticon": The many watch the many

What is the main concern?

Fighting cyber crime and protecting privacy in the cloud

European Parliament's Committee on Civil Liberties, Justice and Home Affairs - 2012

The main concern arising for private citizens, companies and public administration using cloud technologies is not so much the possible increase in "cyber" fraud or crime than the loss of control over one's data

This concern is not only for **privacy** reason, but for **digital investigation** purposes

Scope of Procedural Provisions (Article 14)

- Each Party must adopt legislative measures to define the powers and procedures for specific criminal investigations or proceedings.
- The provisions apply to offenses covered by the Convention, all other offenses committed through computer systems, and all electronic evidence related to any crime.

Conditions and Safeguards (Article 15)

- The application of powers and procedures must ensure adequate protection of human rights, following national law and international conventions (e.g., European Convention on Human Rights).
- Conditions and safeguards include judicial or independent supervision, considering proportionality and the rights of third parties.

Expedited Preservation of Stored Data (Article 16)

- Authorities must be able to order or obtain the rapid preservation of specific computer data, particularly if there is reason to believe that the data is vulnerable to deletion or modification.
- This order may require the data's custodian to preserve the data for up to 90 days, extendable as needed.

Expedited Preservation and Disclosure of Traffic Data (Article 17)

- To ensure data preservation, authorities can demand rapid disclosure of traffic data to identify service providers and communication pathways, even if multiple providers are involved in the transmission.

Production Order (Article 18)

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Subscriber Information (Article 18)

- For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

  a) the type of communication service used, the technical provisions taken thereto and the period of service;
  b) the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
  c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Search and Seizure of Stored Computer Data (Article 19)

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

  a) a computer system or part of it and computer data stored therein; and

  b) a computer-data storage medium in which computer data may be stored in its territory

Real-time Collection of Traffic Data (Article 20)

- Authorities can collect or record traffic data in real time, either directly or by requiring service providers to assist in the collection

Interception of Content Data (Article 21)

- For serious offenses, authorities may intercept or record the content of specific communications in real time, either directly or through the cooperation of service providers.

Mutual Assistance (Article 25)

The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Mutual Assistance (Article 25)

The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Expedited preservation of stored computer data (Article 29)

A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

Expedited disclosure of preserved traffic data (Article 30)

Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

What is the solution ?

Article 32 of the Cybercrime Convention (Budapest 2001)

A Party may, without the authorisation of another Party:

a) *access publicly available (open source) stored computer data, regardless of where the data is located geographically; or*

b) *access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.*

What are the consequences of article 32 b ?

LEAs routinely request-and are provided with-data from foreign service providers, without formal inter-State process such as mutual legal assistance (MLA). Ebay and Facebook have dedicated portals for facilitating such exchanges
(Micheál O' Floinn, *It wasn't all white light before Prism*, 2013)

5 Council of Europe's proposal to implement article 32b (Transborder Group of Cybercrime Convention Commitee)

1. "Transborder access with consent without the limitation to data stored 'in another Party'"
2. "Transborder access without consent but with lawfully obtained credentials."
3. "Transborder access without consent in good faith or in exigent or other circumstances."
4. "When the data is lawfully accessible or available from the initial system"
5. If the location of the data is not known, but the person having the power of disposal of the data is physically on the territory of, or a national of the searching Party, the LEA of this Party may be able [to] search or otherwise access the data

Additional Legal Framework

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32023L1544

In order to apply the rules in a consistent manner and to provide time for implementation and compliance, the **Regulation applies from 18 August 2026**. The **Directive must be transposed into the national laws of the EU Member States by 18 February 2026**.