

LEGAL ASPECTS OF COMPUTER SCIENCE

Law • Technology • Data • Cybersecurity • Digital Governance

Section 2

Jurisdiction, cybercrime and cybersecurity

- Principles of jurisdiction
- Jurisdiction in practice
- Budapest Convention and its offences
- Hanoi Convention and international cooperation
- NIS 2 Directive
- Polish national cybersecurity system
- Active cyberdefence
- Surveillance, encryption and the dark web



Legal Aspects of Computer Science

Section 2: Jurisdiction, cybercrime and cybersecurity

Joanna Kulesza, Ph.D., Lodz Cyber Hub, University of Lodz

Contents

Course scope for Section 2	3
Aims and learning outcomes	3
Lecture scope: meetings 4 to 9	3
Resources	4
Jurisdiction and sovereignty	5
State sovereignty	5
Recap of Section 1	5
International jurisdiction	6
Principles of jurisdiction	7
Cybercrime	9
What is cybercrime?	9
The Budapest Convention in brief	9
Jurisdiction and cybercrime	10
Cybersecurity and cybercrime: why the law matters	12
The Budapest Convention	14
The Budapest Convention and Polish law side by side	16
The Protocols to the Budapest Convention	19
Cybercrime against persons: children, stalking and impersonation	22
European Union law on cybercrime	25
The Hanoi Convention	26
Summary of the law of cybercrime	28
Cybersecurity	29
Active cyberdefence	29
International law and cybersecurity: responsibility and norms	31
Cybersecurity law: the NIS 2 Directive	32
The Polish national cybersecurity system	36
Further topics: data, surveillance and encryption	37
Selected case law of European courts	44
Case studies	45
Case study 1: A ransomware attack with many links	45
Case study 2: Extradition of a national	45
Case study 3: A hospital and the NIS 2 Directive	45
Case study 4: Hack back by a software company	46
Case study 5: Spyware on the phone of a journalist	46
Quiz	47
Summary	51

A note for students

These are study materials for students, prepared with AI assistance on the basis of course notes by Joanna Kulesza. Relevant copyright applies. Check against delivery: these materials are a written aid, and the oral presentation and discussion in class prevail.

Course scope for Section 2

Aims and learning outcomes

Section 2 moves from the sources of law, which were the subject of Section 1, to the question of who may apply the law and in which situations. It then applies this knowledge to cybercrime and cybersecurity. After this section students will be able to:

- explain the principles on which a state may exercise jurisdiction beyond its territory, and distinguish prescriptive, adjudicative and enforcement jurisdiction;
- identify the offences defined in the Budapest Convention and explain how states cooperate to investigate them;
- compare the Budapest Convention with the United Nations Convention against Cybercrime (Hanoi Convention);
- describe the main obligations of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (the NIS 2 Directive, where NIS means Network and Information Security) and of the Polish act on the national cybersecurity system;
- assess, with legal arguments, practices such as active cyberdefence, state surveillance and the use of encryption.

These aims correspond to learning outcomes E1, E3, E4, E6 and E7 of the course.

Lecture scope: meetings 4 to 9

Meeting 4. Trias politica and principles of jurisdiction

Meeting 5. Jurisdiction in practice: exercises

Meeting 6. Cybercrime: the Budapest Convention and its offences

Meeting 7. Cybercrime: the Hanoi Convention and international cooperation

Meeting 8. Cybersecurity: the NIS 2 Directive

Meeting 9. Cybersecurity: the Polish act on the national cybersecurity system

The schedule will be adjusted to the needs of the group. We will focus on the topics in which the students show particular interest. The notes also contain further topics (active cyberdefence, jurisdiction over data, surveillance, encryption and anonymity), which can be used in meetings 5 to 9 depending on the interest of the group.

Resources

Author	Year	Title
Legal instruments		
Council of Europe	2001	Convention on Cybercrime (Budapest Convention)
Council of Europe	2022	Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence
United Nations	2024	United Nations Convention against Cybercrime (Hanoi Convention)
European Union	2022	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)
Republic of Poland	2018	Act of 5 July 2018 on the national cybersecurity system (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa), Journal of Laws 2018 item 1560, as amended
United States	2018	Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Division V of the Consolidated Appropriations Act, 2018, Pub. L. 115-141
Selected publications		
Roy Balleste, Joanna Kulesza	2013	Signs and Portents in Cyberspace: The Rise of Jus Internet as New Order in International Law. Fordham Intellectual Property, Media and Entertainment Law Journal 23(4): 1311
Joanna Kulesza, Roy Balleste (eds)	2015	Cybersecurity and Human Rights in the Age of Cyberveillance. Rowman & Littlefield
Roy Balleste	2022	The Law of Space Cyber Operations: Gripping Mysteries, Entangled Frontiers, and Security Challenges. Journal of Law, Technology & the Internet 13(1): 146
Lee A. Bygrave	2025	The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. Computer Law & Security Review 56: 106071
European Parliament, Policy Department C	2012	Fighting cyber crime and protecting privacy in the cloud (study)
Supplementary reading		
Joanna Kulesza, François Delerue, Patryk Pawlak	2019	The application of international law in cyberspace: is there a European way? Research paper, EU Cyber Direct
Joanna Kulesza	2025	Cyber Diplomacy in Action: EU and Partners Deliver a UN Permanent Mechanism for Responsible State Behaviour and International Law in Cyberspace. Casimir Pulaski Foundation

Recap of Section 1

Section 1 explained where legal rules come from. In Poland, the sources of universally binding law are ranked: the Constitution, statutes, ratified international agreements and regulations. A ratified agreement that was approved by statute has precedence over a conflicting statute. Section 2 asks a different question: which state may apply its rules to a given event, person or data, and how do states cooperate when an event crosses their borders?

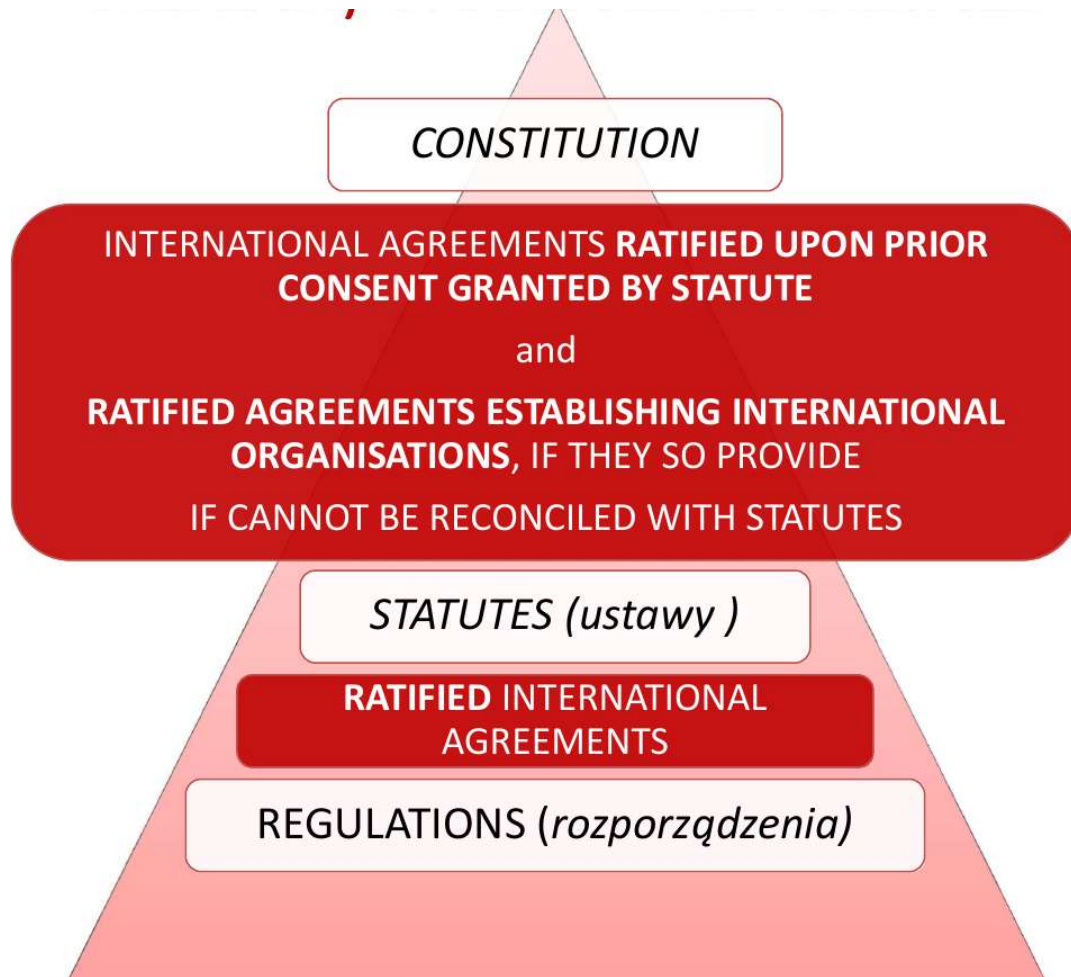


Figure 1. Recap: hierarchy of sources in Polish law.

Jurisdiction and sovereignty

State sovereignty

Sovereignty is the foundation of the law of jurisdiction. In international law it means that a state has supreme authority over its territory and population and is not subject to the authority of another state. In the Island of Palmas case (1928), the arbitrator Max Huber described sovereignty in relations between states as independence, that is, the right to exercise the functions of a state in a given territory, to the exclusion of any other state.

Sovereignty has an internal and an external dimension. Internally, the state is the highest authority and makes, applies and enforces the law. Externally, states are equal and free from outside interference, as the United Nations Charter confirms in the principle of sovereign equality and the prohibition of intervention in domestic matters. Sovereignty also creates duties, such as respecting the sovereignty of others.

Cyberspace challenges this model, because data and services cross borders without regard to territory. States nevertheless exercise sovereignty over the infrastructure, persons and activities on their territory. Whether sovereignty is a binding rule or only a principle, when applied to cyber operations, is debated among states.

State sovereignty and the Westphalian concept

Modern international law is built on the Westphalian concept of state sovereignty, which is associated with the peace treaties of 1648. A sovereign state has:

- exclusive authority over its territory and residents;
- the power to conduct foreign policy, to decide on war and peace, and to recognise states and governments;
- the power to establish diplomatic relations, to enter into military alliances and to join international organisations.



Figure 2. The Westphalian concept of state sovereignty. Gerard ter Borch, *The Swearing of the Oath of Ratification of the Treaty of Münster, (1648)*.

How is state authority exercised?

State authority is exercised in two respects:

- **in the material respect**, the state is authorised to organise social activities by exercising its authority over persons, property and events;
- **in the formal respect**, the state creates the laws that are necessary to organise those activities and provides for their execution.

The state does so by exercising **jurisdiction**. Jurisdiction is the legal power of a state to regulate conduct, to decide disputes and to enforce its decisions.

A case study

Imagine a waterfall that lies on the border between two states. An event begins on one side of the border and produces its effects on the other side. Which state may apply its law? Which state's courts may decide the case? Which state's police may act? These are questions of jurisdiction, and in cyberspace they arise every day, because an offender, a victim, a server and a service provider are rarely in the same state.

The classic form of the problem is a shot fired across a border. The shooter stands in State A, and the victim is hit in State B. The act begins in one state and its effect occurs in the other. Under the subjective territorial principle, State A may exercise jurisdiction. Under the objective territorial principle, State B may do so. Both claims are accepted in international law.

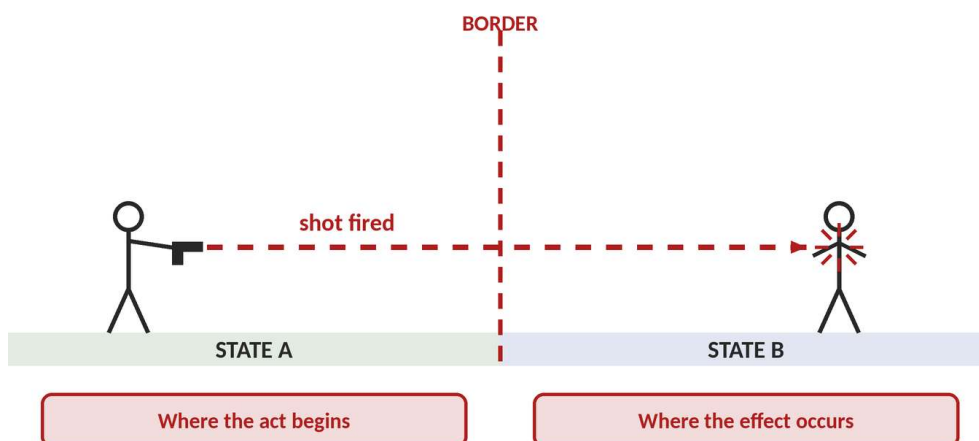


Figure 3. A shot fired across a border: the act begins in State A and its effect occurs in State B. Diagram prepared by the author.

Territorial and extraterritorial jurisdiction

Jurisdiction is exercised above all territorially. Within its own territory, the competence of a state is complete and exclusive. Outside its own territory, a state may exercise jurisdiction in two situations:

- in the territories of other states, and
- in shared territories, the so-called international spaces: the open sea, Antarctica and outer space.

In both situations a state acts under the authority of international law. Exercising state jurisdiction outside the state's territory may lead to a **conflict of jurisdiction**, when two or more states claim the right to regulate the same event. Principles for eliminating such conflicts are therefore needed.

Remember this

- **Sovereignty** is the supreme authority of a state within its territory and its independence from other states. Jurisdiction is the way in which that authority is exercised.
- Jurisdiction has three forms: to **prescribe** (make law), to **adjudicate** (decide cases) and to **enforce** (act on the ground). Enforcement is the most strictly limited by territory.

Principles of jurisdiction

International law recognises a basic set of jurisdictional principles. They answer the question of which link between a state and an event justifies the application of the law of that state.

1. **Territoriality principle (territorial jurisdiction).** A state may regulate conduct that takes place on its territory. In the subjective version, the state has jurisdiction because the act began on its territory. In the objective version, the state has jurisdiction because the act was completed, or produced its elements, on its territory.
2. **Effects principle (effective jurisdiction).** A state may regulate conduct abroad that has substantial effects on its territory. This principle is closely related to objective territoriality and is the most important basis of jurisdiction in cyberspace, because a website or an attack can be accessed or can cause harm in many states at the same time.
3. **Personality principle (personal jurisdiction).** A state may regulate the conduct of its nationals abroad (active personality) and, in some cases, conduct that harms its nationals abroad (passive personality).
4. **Protective principle (protective jurisdiction).** A state may regulate conduct abroad that threatens its security or other essential interests, for example the forgery of its currency or acts against its government.
5. **Universality principle (universal jurisdiction).** Every state may prosecute certain crimes that offend the international community as a whole, wherever and by whomever they were committed. Piracy is the classic example. Other examples are genocide, war crimes and crimes against humanity.

The jurisdictional toolbox

A state may exercise three kinds of jurisdiction, which correspond to the three powers of government: **prescriptive** jurisdiction (the power to make law, which belongs to the legislature), **adjudicative** jurisdiction (the power of courts to decide cases) and **enforcement** jurisdiction (the power of the executive to enforce the law, for example by arrest, search or seizure). This is a link between jurisdiction and the doctrine of trias politica, or the separation of powers, which was introduced in Section 1.

Type of jurisdiction	Exercised by	Example
Prescriptive	Legislature	A statute that criminalises unauthorised access to computer systems
Adjudicative	Courts	A court that decides whether a defendant committed that offence
Enforcement	Executive (police, prosecutors, administration)	Arrest of the suspect, search of a server, seizure of data

The three kinds of jurisdiction do not extend equally far. As a rule, a state may be allowed to legislate and to adjudicate with respect to conduct abroad if there is a sufficient link, but it may **enforce** only on its own territory, unless another state consents. This distinction was developed in the S.S. "Lotus" case (France v. Turkey, Permanent Court of International Justice, 1927), which also stands for the proposition that a state may extend its jurisdiction unless a prohibitive rule of international law forbids it. Today most lawyers read the Lotus case together with the requirement of a genuine link.

Remember this

- Five principles justify jurisdiction: **territoriality, effects, personality, protection and universality**.
- In cyberspace the **effects principle** is the most important basis, because a website or an attack can be accessed or felt in many states at once.

Exercise: the jurisdictional toolbox

	Territorial (subjective)	Territorial (objective, effective)	Personal (active)	Personal (passive)	Protective (preventive)	Universal
Prescriptive						
Adjudicative						
Enforcement						

The facts below are fictional. For each case, name the principle or principles on which each state may claim jurisdiction, and identify any conflict of jurisdiction.

1. A student in State A writes a program that encrypts the files of a company in State B. The command server is located in State C, and the ransom is paid to a wallet administered by a national of State D.
2. A national of State A, who is living in State B, publishes online a database of personal data of citizens of State C. Under the law of State B, publication is not an offence.
3. Pirates attack a ship flying the flag of State A in the open sea. The crew detains them, and they are brought to State B, which has no link with the ship, the crew or the pirates.
4. Hackers break into the network of the ministry of defence of State A from internet cafés in State B. Their goal is to obtain information on the location of military units.
5. Police of State A, with a valid warrant from a court of State A, connect remotely to a server in State B and copy data stored there.

Cybercrime

What is cybercrime?

The discussion now moves from the general law of jurisdiction to the law of cybercrime. A first and important observation is that international law contains no legal definition of cybercrime. The term is used in politics, in scholarship and in the titles of treaties, but no binding instrument says what cybercrime is. The Budapest Convention, which is the most important treaty in this field, does not define it either. Its title refers to the "Convention on Cybercrime", but its text defines only particular offences, and the term "cybercrime" appears only in its title and preamble, not in any operative definition. The United Nations Convention against Cybercrime follows the same approach.

This situation is not unusual in international law. There is also no comprehensive treaty definition of terrorism, and states have instead agreed on specific offences in sectoral treaties. By contrast, piracy is defined in the United Nations Convention on the Law of the Sea (Articles 101 to 103). The law of cybercrime resembles the first model: it lists conduct that states must criminalise, and it does not rely on an abstract concept.

For study purposes, scholars and practitioners often distinguish two groups. These categories come from doctrine and from practice. They are not legal categories and they do not produce legal consequences by themselves.

1. **Cyber-dependent crime:** offences that can be committed only with the use of information technology and that are directed against it, for example illegal access to a system, interference with data or the spreading of ransomware.
2. **Cyber-enabled crime:** traditional offences whose commission is changed in scale or in method by the use of information technology, for example fraud, the distribution of child sexual abuse material or the infringement of copyright online.

The Budapest Convention in brief

The Convention on Cybercrime of the Council of Europe (European Treaty Series No. 185) was opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004. It is a binding multilateral treaty, and it is open to states that are not members of the Council of Europe. It is supplemented by two additional protocols, which are described later in this section. Its work is supported by the Cybercrime Convention Committee (T-CY), which adopts guidance notes. These notes are not binding, and they belong to soft law: they present a shared interpretation of the parties, but they do not create obligations.

You are here: Treaty Office > Full list

Chart of signatures and ratifications of Treaty 185

> Convention on Cybercrime (ETS No. 185)

> Status as of 13/10/2026

Title	Convention on Cybercrime (ETS No. 185)
Reference	ETS No. 185
Opening of the treaty	Budapest 23/11/2001 - Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
Entry in force	01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe

☒ State who signed
 ☒ State who ratified
 ☒ State who neither signed nor ratified
 ☒ State who suspended
 ☒ State who denounced

State or International Organisation	Signature	Ratification	Entry into Force	Notes	R _r	D _r	A _r	T _r	C _r	O _r
Members of Council of Europe										

Total number of signatures not followed by ratifications	2
Total number of ratifications/accessions	83

The Convention consists of four main groups of provisions:

- **substantive criminal law (Articles 2 to 13),**
- procedural law (Articles 14 to 21),
- jurisdiction (Article 22) and
- international cooperation (Articles 23 to 35).

It is therefore a hybrid instrument, which combines harmonisation of national criminal law with rules on cooperation between states.

Technological neutrality

The drafters deliberately avoided names of specific technologies. The offences are described by reference to the function of the conduct and to a few general terms defined in Article 1: "computer system", "computer data", "service provider" and "traffic data". A **"computer system" is any device or group of interconnected devices which performs automatic processing of data**. This wording covers a personal computer, a smartphone, a server and an industrial control system, and it is wide enough to cover devices that did not exist in 2001.

The reason is practical and also legal. Technology changes faster than treaties can be amended, and a treaty tied to the technology of 2001 would soon be obsolete. Technologically neutral drafting allows the parties to apply the same provisions to new situations, for example to ransomware, botnets or attacks on cloud services, without a formal amendment. Interpretation by the parties and by the T-CY

performs the task which in other fields is performed by amendment. A similar technique is found in environmental law, where framework treaties use general standards, such as "significant harm", and leave their application to later practice.

Technological neutrality has a price. General wording gives the parties wide discretion when they implement the Convention, and national definitions can differ. It also leaves open the question whether a new phenomenon, such as the use of artificial intelligence in an attack, falls within an existing offence. Courts and legislators answer such questions case by case. The result is a degree of fragmentation in national law, which the Convention tries to limit through the common minimum standard of the offences and through the consultation mechanism of Article 22, paragraph 5.

Remember this

- There is **no legal definition of cybercrime** in international law, not even in the Budapest Convention. The treaties list offences and do not define the concept.
- The Budapest Convention is a **binding treaty**. The guidance notes of the Cybercrime Convention Committee (T-CY) are **soft law**.
- The Convention is **technologically neutral**: it describes conduct by function, so that it can apply to new technologies.

Jurisdiction and cybercrime

Cybercrime shows why the principles of jurisdiction matter. The Budapest Convention of the Council of Europe, which is discussed in more detail below, obliges the parties to establish jurisdiction over the offences it defines on the basis of several of the principles described above. The provision is Article 22:

Article 22 Budapest Convention, Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
 - a. in its territory; or
 - b. on board a ship flying the flag of that Party; or
 - c. on board an aircraft registered under the laws of that Party; or
 - d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

The provision combines the territorial principle (paragraph 1, letters a to c) with the active personality principle (letter d). Paragraph 3 expresses the idea of *aut dedere aut judicare*: a state that refuses to extradite its national must be able to prosecute him or her. Paragraph 4 leaves the parties free to apply other grounds of jurisdiction under their own law, for example the effects principle. Paragraph 5 does not solve conflicts of jurisdiction, but it requires the states involved to consult each other.

International cooperation in practice

Jurisdiction to prescribe and to adjudicate is of little use without the possibility to enforce. Since the servers, the data and the suspects are often abroad, investigators depend on cooperation with foreign authorities. Law enforcement agencies and their partners coordinate large operations through Europol, Eurojust and similar channels. One example is the operation against the infrastructure used to distribute malware, which, according to Europol, shut down the loaders IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee, led to four arrests and took down more than 100 servers worldwide.

At the level of treaties, two instruments are at the centre of this course. The first is the Budapest Convention of the Council of Europe. The second is the United Nations Convention against Cybercrime, which was negotiated by an ad hoc committee of the United Nations General Assembly. Both are described below.

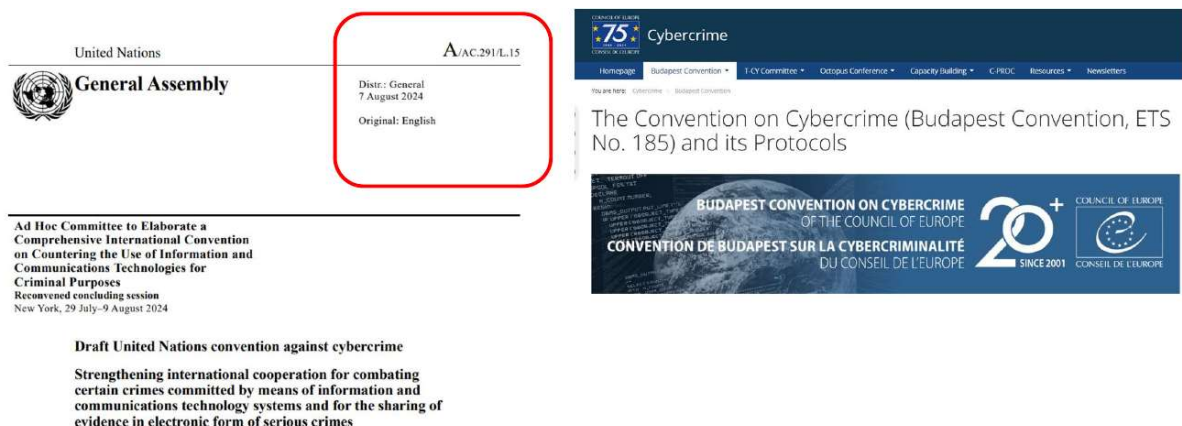


Figure 4. Draft United Nations convention against cybercrime and the Budapest Convention. Sources: United Nations; Council of Europe.

Remember this

- Article 22 of the Budapest Convention requires jurisdiction on the grounds of territory, flag, registration and nationality. Paragraph 3 expresses *aut dedere aut judicare*, and paragraph 5 requires consultation when several states claim jurisdiction.
- Jurisdiction without cooperation is of little use, because evidence, servers and suspects are often abroad.

Cybersecurity and cybercrime: why the law matters

Cybersecurity is the protection of networks, systems and data against threats. Cybercrime is the commission of criminal offences with the use of, or against, information systems. The two are connected: the law of cybercrime punishes attacks after the fact, and the law of cybersecurity requires organisations to prevent them and to report them. The examples below are discussed in the lecture. Each of them shows a different legal problem.

Example	What happened	Legal issue
WannaCry ransomware (2017)	Ransomware encrypted data in many countries. According to a press report shown in the lecture, the attack on the British National Health Service cost 92 million pounds and led to the cancellation of 19,000 appointments.	Cybercrime, critical infrastructure, duties of operators to protect systems
Mirai botnet (2016)	Hacked home devices were used to cause a massive internet outage, as reported by the press in October 2016.	Security of consumer devices, responsibility of manufacturers, cross-border investigation
Cable cut in Armenia (2011)	An elderly woman looking for scrap copper damaged a cable and cut off internet access in Armenia for several hours, as reported by a newspaper in 2011.	Cyber threats are not always attacks; resilience of infrastructure
Stuxnet (2010)	A computer worm was designed to infect industrial control systems and to damage centrifuges, as the diagram shows.	Use of force and sovereignty in international law; attribution
Request to extradite a hacker (2012)	A British citizen, accused of hacking US military computers, was not extradited to the United States after the Home Secretary decided that he was not fit to stand trial.	Jurisdiction, extradition, human rights
Attacks combined with physical harm (2022 -)	Press reports describe drones used against military targets, which has been common in the war in Ukraine since 2022, and explosives planted in communication devices, as in Lebanon in 2024.	Technology as a means of warfare; international humanitarian law
Cyber-attacks against Estonia (2007)	Over several weeks in April and May 2007, denial-of-service attacks disrupted the websites of the Estonian government, parliament, banks and media. They followed a dispute about the removal of a Soviet war monument in Tallinn. Estonia pointed to Russia, but no state was held responsible in a legal proceeding.	Attribution and state responsibility; whether such operations amount to a use of force or an armed attack; sovereignty; collective defence in NATO. The attacks led to the Tallinn Manual and the Budapest Convention's wider use



By Liilia Moroz - Own work, CC0, <https://commons.wikimedia.org/w/index.php?curid=99451390>



Figure 5. Ransom message displayed by the WannaCry ransomware.



Figure 6. Press report on the internet outage caused by hacked home devices. Source: USA Today.

HOW STUXNET WORKED

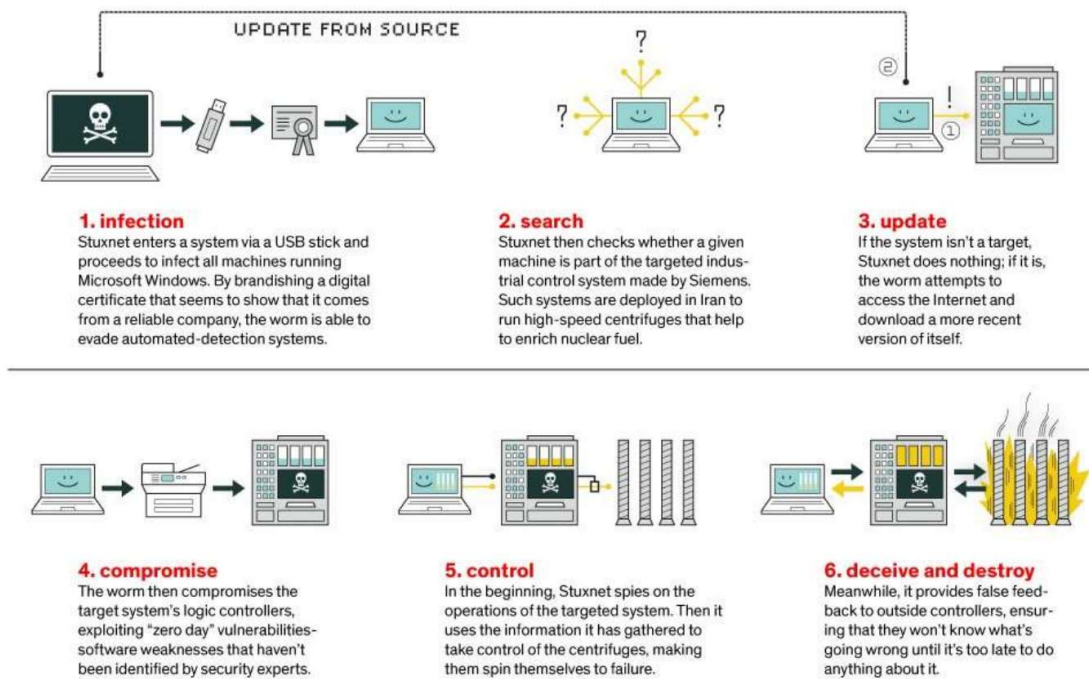


Figure 7. How Stuxnet worked. Source: Institute of Electrical and Electronics Engineers (IEEE) Spectrum illustration.

The Budapest Convention

The Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, was opened for signature in 2001. It is the first and, for many years, the only binding international treaty on cybercrime. It is open to states that are not members of the Council of Europe, and it has been ratified by states from all continents. Poland is a party to it. It is a binding treaty in the sense of Section 1: a state is bound only after ratification, and a ratified treaty is part of the domestic legal order.

The Convention pursues three aims:

1. to harmonise the definitions of cybercrime offences in national criminal law;
2. to give national authorities the procedural powers needed to investigate cybercrime and to collect electronic evidence;
3. to establish a fast and effective system of international cooperation.

Offences defined in the Budapest Convention

The Convention requires the parties to criminalise the following conduct, when committed intentionally and without right. The table below is a summary written for study purposes. It is not a quotation of the Convention.

Group	Offence	What it covers
Offences against the confidentiality, integrity and availability of computer data and systems		
	Illegal access	Access to the whole or a part of a computer system without right. A party may require that security measures were circumvented, or that there was an intent to obtain data or another dishonest intent.
	Illegal interception	Interception, by technical means, of non-public transmissions of computer data to, from or within a computer system.
	Data interference	Damaging, deleting, deteriorating, altering or suppressing computer data.
	System interference	Serious hindering of the functioning of a computer system by entering, transmitting, damaging, deleting, altering or suppressing data. A denial of service attack is an example.
	Misuse of devices	Producing, selling, obtaining for use, importing or distributing devices or programs designed to commit the offences above, and computer passwords or access codes, with the intent to use them. The Convention excludes authorised testing or protection of a computer system, which is important for security researchers.
Computer-related offences		
	Computer-related forgery	Input, alteration, deletion or suppression of data that results in inauthentic data being treated as authentic, with intent to deceive.
	Computer-related fraud	Causing a loss of property to another person by manipulating data or the functioning of a system, with a fraudulent or dishonest intent of obtaining an economic benefit.
Content-related offences		
	Offences related to child sexual abuse material	Producing, offering, distributing, procuring and possessing such material through computer systems.
Offences related to copyright		
	Infringements of copyright and related rights	Infringements committed wilfully, on a commercial scale and by means of a computer system.

The Convention also requires the parties to criminalise attempt, aiding and abetting of these offences, to provide for the liability of legal persons and to provide for effective, proportionate and dissuasive

sanctions. A First Additional Protocol deals with racist and xenophobic acts committed through computer systems.

In Polish criminal law, comparable conduct is punished by provisions of the Criminal Code, for example unlawful access to information, interception of communications, interference with data and computer fraud.

Procedural powers and international cooperation

- **Preservation.** Authorities may order the expedited preservation of stored computer data, including traffic data, which is volatile.
- **Production and search.** Authorities may order a person or a service provider to submit specified data, and may search and seize stored data.
- **Real-time collection.** Authorities may collect traffic data and, for serious offences, content data in real time.
- **International cooperation.** The parties cooperate on extradition and mutual legal assistance, and each party must designate a contact point that is available twenty-four hours a day, seven days a week.

Safeguards apply to all these powers. The Convention requires the parties to respect human rights and the principle of proportionality. A Second Additional Protocol, adopted in 2022, provides additional tools for enhanced cooperation and for the disclosure of electronic evidence, for example direct requests to service providers in other states.

Questions for discussion

1. Why does the Convention exclude authorised testing from the offence of misuse of devices?
2. Which jurisdictional principles are used in the Convention, and what does the obligation to consult add?
3. Why is expedited preservation important in cybercrime investigations?

Remember this

- The Budapest Convention has three aims: **harmonised offences, procedural powers for electronic evidence, and international cooperation.**
- The offences must be committed **intentionally and without right.** This phrase protects, for example, authorised security testing.
- The Polish Penal Code implements these offences, but not word for word. Compare the texts carefully.

The Budapest Convention and Polish law side by side

This section places the text of the offences in the Budapest Convention next to the Polish provisions that implement them. The left column quotes the Convention. The right column gives the Polish Penal Code (Kodeks karny, KK) in an unofficial working translation prepared for teaching. The Polish text of the Code is authoritative, and students should always check the current wording, because the Code is amended frequently. The translation follows the consolidated text of the Penal Code published in the Journal of Laws of 2025 and amended since. Where a provision is summarised and not quoted, this is stated. Article 10 refers to treaties of the World Intellectual Property Organization (WIPO). The Convention is not self-executing, so Poland implements it through its own offences, which follow a different structure and different terminology.

Budapest Convention	Polish counterpart (working translation)
Article 2: Illegal access Article 267 §1 and §2 KK	
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, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	Art. 267 §1. Whoever, without authorisation, obtains access to information not intended for him by opening a sealed letter, connecting to a telecommunications network, or breaking or bypassing electronic, magnetic, IT or other special protection of it, is subject to a fine, restriction of liberty or imprisonment for up to 2 years. §2. The same penalty applies to whoever, without authorisation, obtains access to the whole or a part of an IT system. §5. Prosecution of the offence in §1 to §4 takes place upon the request of the injured party.
Article 3: Illegal interception Article 267 §3 KK	
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, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	Art. 267 §3. The same penalty applies to whoever, in order to obtain information to which he is not entitled, installs or uses an eavesdropping device, a visual device or another device or software. §4. The same penalty applies to whoever discloses to another person information obtained in the manner described in §1 to §3.
Article 4: Data interference Articles 268a and 268 KK	
1. 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, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	Art. 268a §1. Whoever, without being entitled to do so, destroys, damages, deletes, alters or hinders access to IT data, or significantly disrupts or prevents the automatic processing, collection or transmission of such data, is subject to imprisonment for up to 3 years. §2. Whoever, committing the act described in §1, causes significant property damage, is subject to imprisonment from 3 months to 5 years. Art. 268 §1. Whoever, without being entitled to do so, destroys, damages, deletes or alters the record of significant information, or otherwise frustrates or significantly hinders the entitled person's access to it, is subject to a fine, restriction of liberty or imprisonment for up to 2 years. §2. If the act described in §1 concerns a record on an IT data carrier, the perpetrator is subject to imprisonment for up to 3 years. §3. Whoever, committing the act described in §1 or §2, causes significant property damage, is subject to imprisonment from 3 months to 5 years.
Article 5: System interference Articles 269a and 269 KK	
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, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating,	Art. 269a. Whoever, without being entitled to do so, through the transmission, destruction, deletion, damaging, hindering of access to or alteration of IT data, significantly disrupts the operation of an IT system, an ICT system or an ICT network, is subject to imprisonment from 3 months to 5 years.

altering or suppressing computer data.	Art. 269 §1. Whoever destroys, damages, deletes or alters IT data of special importance for the defence of the country, transport safety, or the functioning of the government administration, another state body or state institution, or local government, or disrupts or prevents the automatic processing, collection or transmission of such data, is subject to imprisonment from 6 months to 8 years. §2. The same penalty applies to whoever commits the act described in §1 by destroying or replacing an IT data carrier, or by destroying or damaging a device used for the automatic processing, collection or transmission of IT data.
Article 6: Misuse of devices Articles 269b and 269c KK	
1 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: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a. ii of this article.	Art. 269b §1. Whoever produces, acquires, sells or makes available to other persons devices or computer programs adapted to commit an offence described in Art. 165 §1 point 4, Art. 267 §1 to 3, Art. 268a §1 or §2 in connection with §1, Art. 269 §1 or 2, Art. 269a, Art. 270 §1 or Art. 270a §1, as well as computer passwords, access codes or other data enabling unauthorised access to information stored in an IT system, an ICT system or an ICT network, is subject to imprisonment from 3 months to 5 years. §1a. A person does not commit the offence described in §1 who acts solely in order to protect an IT system, an ICT system or an ICT network against the commission of an offence listed in that provision, or to develop a method of such protection. §2. In the event of a conviction for the offence described in §1, the court orders the forfeiture of the objects described in it, and may order their forfeiture if they were not the property of the perpetrator. Art. 269c. A person is not punishable for an offence described in Art. 267 §2 or Art. 269a who acts solely in order to protect an IT system, an ICT system or an ICT network, or to develop a method of such protection, and who promptly notified the administrator of that system or network of the threats discovered, provided that his action did not violate a public or private interest and did not cause damage.
Article 7: Computer-related forgery Article 270 KK	
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.	Art. 270 §1. Whoever, in order to use it as authentic, forges or alters a document, or uses such a document as authentic, is subject to imprisonment from 3 months to 5 years. §2. The same penalty applies to whoever fills in a form bearing another person's signature contrary to the will of the signatory and to his detriment, or uses such a document. Art. 115 §14. A document is any object or other recorded carrier of information to which a particular right is attached, or which, because of its content, constitutes evidence of a right, a legal relationship or a circumstance of legal significance.
Article 8: Computer-related fraud Articles 287 and 286 KK	
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:	Art. 287 §1. Whoever, in order to obtain a material benefit or to cause damage to another person, without authorisation influences the automatic processing, collection or transmission of IT data, or alters, deletes or enters a new record of IT data, is subject to imprisonment from 3 months to 5 years. Art. 286 §1. Whoever, in order to obtain a material benefit, causes another person to dispose of his own or another person's property to his detriment by misleading him or by exploiting his mistake or inability to understand properly the action he undertakes, is subject to imprisonment from 6 months to 8 years.
Article 9: Offences related to child pornography Article 202 KK	
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its	Art. 202 §3. Whoever, for the purpose of dissemination, produces, records or imports, stores or possesses, or

domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct. 3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d and e, and 2, sub-paragraphs b and c.	disseminates or presents pornographic content involving a minor, or pornographic content related to the presentation of violence or the use of an animal, is subject to imprisonment from 2 to 15 years. §4. Whoever records pornographic content involving a minor is subject to imprisonment from 1 year to 10 years. §4a. Whoever stores, possesses or obtains access to pornographic content involving a minor is subject to imprisonment from 3 months to 5 years. §4b. Whoever produces, disseminates, presents, stores or possesses pornographic content showing a created or processed image of a minor participating in a sexual activity is subject to imprisonment for up to 3 years. §4c. The penalty provided for in §4b applies to whoever, for the purpose of sexual satisfaction, participates in a presentation of pornographic content involving a minor.
Article 10: Offences related to infringements of copyright and related rights Copyright Act	
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party’s international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	Discussed separately
Article 22: Jurisdiction Articles 5, 6, 109 to 112a KK	
Quoted in full in the section on jurisdiction and cybercrime. Paragraph 1 requires jurisdiction over offences committed in the territory of a Party, on board a ship flying its flag, on board an aircraft registered under its laws, and by its nationals if the offence is punishable under criminal law where it was committed or outside the territorial jurisdiction of any state.	Art. 5. Polish criminal law applies to a perpetrator who committed a prohibited act on the territory of the Republic of Poland, as well as on a Polish vessel or aircraft, unless an international agreement to which the Republic of Poland is a party provides otherwise. Art. 6 §2. A prohibited act is deemed to have been committed at the place where the perpetrator acted or failed to act in breach of a duty to act, or where the effect constituting an element of the prohibited act occurred or, according to the perpetrator’s intention, was to occur.

	Art. 109. Polish criminal law applies to a Polish citizen who committed an offence abroad. Art. 110 §1. Polish criminal law applies to a foreigner who committed abroad a prohibited act directed against the interests of the Republic of Poland, a Polish citizen, a Polish legal person or a Polish organisational unit without legal personality, and to a foreigner who committed abroad an offence of a terrorist nature. Art. 111 §1. A condition of liability for an act committed abroad is that the act is also recognised as an offence by the law in force at the place where it was committed. Art. 112a. Irrespective of the provisions in force at the place where the prohibited act was committed, Polish criminal law applies to a Polish citizen and a foreigner who commit an offence using an IT system, an ICT system or an ICT network, if the act caused or could have caused on the territory of the Republic of Poland an effect violating the interest of the state in the protection of independence, territorial integrity, external and internal security, defence, foreign policy, international position, or scientific or economic potential.
--	--

Four observations arise from the comparison. First, the Convention is technology specific, while the Polish Code often uses general terms such as “IT data” and “IT system” and combines several Convention offences in one article. Second, Article 6(2) of the Convention protects authorised security testing. Polish law does so in two ways: Article 269b §1a excludes liability for acting solely to protect a system, and Article 269c exempts a person who acts to protect a system and promptly notifies its administrator, but only for the offences in Article 267 §2 and Article 269a, and only if no interest is violated and no damage is caused. This is narrower than a general exemption, which matters for penetration testers. Third, Article 6 §2 of the Code, which locates an act also where its effect occurred, applies the effects principle to offences committed from abroad. Fourth, Article 112a of the Code goes beyond Article 22 of the Convention: it extends Polish jurisdiction to offences committed with the use of IT systems whose effects violate certain interests of the state, whatever the place of the act and the nationality of the perpetrator.

Questions for discussion

1. Which Polish provision corresponds to each of the offences in Articles 2 to 5 of the Convention, and where do the Polish provisions differ in scope?
2. Compare Article 6(2) of the Convention with Articles 269b §1a and 269c of the Polish Penal Code. Does the Polish exemption protect a researcher who finds a vulnerability and reports it?
3. How do Articles 6 §2 and 112a of the Polish Penal Code help to establish jurisdiction in a case of an attack launched from another state?

The Protocols to the Budapest Convention

The Convention has been supplemented by two protocols. Both are separate treaties. A state becomes bound by them only if it ratifies them, and a state may be a party to the Convention without being a party to either protocol.

The First Additional Protocol: racist and xenophobic acts

The First Additional Protocol concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). It was opened for signature in 2003. Article 2 defines the central term:

Protocol, Article 2(1)

“racist and xenophobic material” means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

The Protocol requires the parties to criminalise the following offences, when committed intentionally and without right:

- **Dissemination of racist and xenophobic material** through a computer system (Article 3).
- **Racist and xenophobic motivated threat**, that is, threatening through a computer system to commit a serious criminal offence against persons or groups for these reasons (Article 4).
- **Racist and xenophobic motivated insult**, that is, publicly insulting persons or groups through a computer system for these reasons (Article 5).
- **Denial, gross minimisation, approval or justification of genocide or crimes against humanity**, as defined by international law and recognised by final and binding decisions of international courts (Article 6).
- **Aiding and abetting** the commission of any of these offences (Article 7).

The text of Articles 3 and 4 is quoted below.

Protocol, Article 3, Dissemination of racist and xenophobic material through computer systems

1. 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 following conduct:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Protocol, Article 4, Racist and xenophobic motivated threat

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 following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law,

- (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or
- (ii) a group of persons which is distinguished by any of these characteristics.

The Protocol shows a typical tension in the law of cybercrime between the protection of dignity and the freedom of expression. It allows parties to make reservations on several provisions, and concerns for free speech have limited participation by some states. The Polish counterparts of these offences are found in the Penal Code, for example in provisions on public incitement to hatred and on the public insulting of a group because of national, ethnic, racial or religious affiliation (Articles 256 and 257 KK). Poland also penalises denial of certain international crimes in a separate statute.

The Second Additional Protocol: enhanced cooperation and disclosure of electronic evidence

The Second Additional Protocol (CETS No. 224) was opened for signature on 12 May 2022. It addresses the problem that most electronic evidence is held by service providers located in other states, so that the traditional system of mutual legal assistance is too slow. It enters into force after the required number of ratifications and binds only the states that ratify it. Its main tools are the following:

- **Domain name registration information.** A competent authority may request registration data directly from entities providing domain name services in another party (Article 6).
- **Disclosure of subscriber information.** A competent authority may issue an order directly to a service provider in the territory of another party (Article 7).
- **Orders given effect by the requested party.** A party can give effect to an order of another party for the expedited production of subscriber information and traffic data (Article 8).
- **Emergencies.** Expedited disclosure of stored data (Article 9) and emergency mutual assistance (Article 10) in cases of a significant and imminent risk to the life or safety of a person.
- **Cooperation tools.** Video conferencing (Article 11) and joint investigation teams and joint investigations (Article 12).
- **Safeguards.** Conditions and safeguards (Article 13) and the protection of personal data (Article 14).

The Protocol is an example of the shift from cooperation between states to direct cooperation between authorities and private actors, a change with consequences for the sovereignty and jurisdiction discussed earlier in this section. In the European Union it is linked to the e-Evidence package, in particular Regulation (EU) 2023/1543 on European production orders and European preservation orders for electronic evidence in criminal proceedings and Directive (EU) 2023/1544, which require service providers to designate a representative in the Union. Both instruments are Union law, while the Protocol is a treaty, and the two sets of rules must be coordinated.

Questions for discussion

1. Why is the direct cooperation with service providers a challenge for the principle of territorial enforcement jurisdiction?
2. Which safeguards are necessary when an authority in one state orders a provider in another state to disclose subscriber information?
3. Should the criminalisation of denial of genocide be part of a treaty on cybercrime? Consider the freedom of expression.

Remember this

- The **First Additional Protocol** (2003) concerns racist and xenophobic acts committed through computer systems.
- The **Second Additional Protocol** (2022) concerns enhanced cooperation and the disclosure of electronic evidence, including direct cooperation with service providers in other states.

Cybercrime against persons: children, stalking and impersonation

The Budapest Convention concentrates on offences against computer systems and data. Many harmful online acts are directed against persons, and they are regulated in other treaties and in national criminal law. This part discusses three groups of such acts: the sexual abuse and grooming of children, stalking, and the abuse of another person's identity. In each of them the Polish Penal Code is compared with the international and European standard.

The Lanzarote Convention and grooming

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, CETS No. 201) was opened for signature in Lanzarote on 25 October 2007 and entered into force on 1 July 2010. Poland is a party. Like the Budapest Convention, it is a binding treaty of the Council of Europe, which is open to states that are not members of the organisation. It is the first treaty that treats the sexual abuse of children as a subject of its own, and its definition of the offences covers acts committed with the use of information technology. The table below summarises the offences. It is a summary written for study purposes and it is not a quotation of the Convention. Students should consult the official text.

Lanzarote Convention	Subject matter (summary)	Polish counterpart
Article 18	Sexual abuse of a child: sexual activity with a child who has not reached the legal age for sexual activity, or with a child where force, coercion, threats, abuse of a recognised position of trust or authority, or abuse of a particularly vulnerable situation are used	Articles 199 and 200 Penal Code
Article 20	Offences concerning child pornography: producing, offering or making available, distributing or transmitting, procuring, possessing, and knowingly obtaining access to child pornography by means of information and communication technologies	Article 202 §§ 3 to 4c Penal Code
Article 21	Offences concerning the participation of a child in pornographic performances	Article 202 §§ 3 and 4c Penal Code, and the provisions on sexual abuse
Article 22	Corruption of children: causing a child who has not reached the legal age to witness sexual abuse or sexual activities	Article 200 §§ 3 and 4 Penal Code
Article 23	Solicitation of children for sexual purposes (grooming): a proposal by an adult, through information and communication technologies, to meet a child, for the purpose of committing sexual offences against the child, followed by material acts leading to the meeting	Article 200a Penal Code

Grooming is a process in which an adult builds a relationship of trust with a child, usually by electronic means, in order to abuse the child. The Convention does not criminalise the whole process. It requires the parties to criminalise a defined conduct: a proposal to meet, made for a sexual purpose and followed by material acts leading to the meeting. Polish law sets the threshold earlier. The two paragraphs of Article 200a of the Penal Code are quoted below in an English translation.

Article 200a Penal Code (Poland), English translation

§ 1. Whoever, for the purpose of committing an offence specified in Article 197 § 4 or Article 200, as well as of producing or recording pornographic content, by means of an ICT system or a telecommunications network establishes contact with a minor under 15 years of age, aiming, by misleading him or her, by exploiting a mistake or an inability to understand the situation properly,

or by the use of an unlawful threat, to meet with him or her, shall be subject to imprisonment for up to 3 years.

§ 2. Whoever, by means of an ICT system or a telecommunications network, makes to a minor under 15 years of age a proposal of sexual intercourse, of submitting to or performing another sexual act, or of participation in producing or recording pornographic content, and aims at its realisation, shall be subject to a fine, restriction of liberty or imprisonment for up to 2 years.

Three observations are useful for discussion. First, paragraph 1 criminalises establishing contact with a specific aim, and it does not require that a meeting takes place. In this respect it goes further than the minimum standard of the Convention. Second, the protection is limited to children under 15 years, which is the age of consent in Polish law. Third, the offence is committed by means of an ICT system, which shows the technological neutrality of the drafting that was discussed above: the Polish text refers to any ICT system or telecommunications network, and not to a particular service or platform. At the level of the European Union, the same subject is regulated in Article 6 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography.

Stalking and impersonation: Article 190a of the Penal Code

The Budapest Convention does not contain an offence of stalking, and international law does not contain a general treaty on it. Stalking is, however, addressed in Article 34 of the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention), which requires the parties to criminalise intentional conduct that repeatedly threatens another person and causes that person to fear for her or his safety. At the level of the European Union, Directive (EU) 2024/1385 on combating violence against women and domestic violence requires the Member States to criminalise cyber stalking, cyber harassment, the non-consensual sharing of intimate or manipulated material and cyber incitement to violence or hatred. The Directive entered into force on 13 June 2024 and the Member States must transpose it by 14 June 2027.

Poland introduced the offence of stalking in 2011, in Article 190a of the Penal Code. The provision is notable for a second paragraph, which penalises the use of another person's identity. The text is quoted below in an English translation of the consolidated text.

Article 190a Penal Code (Poland), English translation

§ 1. Whoever, by persistent harassment of another person or of a person closest to that person, causes in that person a justified sense of threat, humiliation or torment, or substantially violates that person's **privacy**, shall be subject to imprisonment for 6 months to 8 years.

§ 2. The same penalty applies to whoever, by impersonating another person, uses that person's image, other personal data or other data by which that person is publicly identified, thereby causing that person property or personal damage.

§ 3. If the consequence of the act specified in § 1 or 2 is an attempt by the injured person on his or her own life, the perpetrator shall be subject to imprisonment for 2 to 15 years.

§ 4. Prosecution of the offence specified in § 1 or 2 takes place on the motion of the injured party.

Two elements of paragraph 1 are central. The harassment must be persistent, and it must cause either a justified sense of threat, humiliation or torment, or a substantial violation of privacy. Cyber stalking is therefore not a separate offence in Polish law. It is stalking committed with technical means, for example messages, the monitoring of accounts or the use of location data. The link to the international standard is Article 34 of the Istanbul Convention and Directive (EU) 2024/1385.

Identity theft

The term identity theft has no legal definition in international law, and it is not an offence in the Budapest Convention. It describes a sequence of acts, and each of them is regulated separately. The table shows how the conduct is covered by the instruments discussed in this section.

Stage of the conduct	Budapest Convention	Polish Penal Code
Obtaining the data of another person by breaking into a system, or by intercepting communication	Article 2 (illegal access) and Article 3 (illegal interception)	Article 267 (unlawful access to information and to a system)
Using the data to appear as that person, in order to cause damage	Article 7 (computer-related forgery) and Article 8 (computer-related fraud)	Article 190a § 2 (impersonation), Article 286 (fraud) and Article 287 (computer fraud)
Disseminating an image of a person without consent	No specific provision	Article 191a (recording and dissemination of the image of a naked person or of a person during a sexual act)

The Polish solution in Article 190a § 2 is unusual, because it places impersonation among the offences against liberty and not among the offences against property. The protected interest is the person whose identity is used, and the offence requires damage, which can be property damage or personal damage. The protection of personal data as such, for example the liability of controllers and the rights of data subjects, belongs to data protection law. It is discussed in the next section of the course and is mentioned here only as a reference.

Questions for discussion

1. Should the law criminalise grooming before any meeting has taken place? Which risks does an early threshold create for the principle of legality?
2. Why does a treaty on children define the offences by reference to information and communication technologies and not to named services?
3. Is Article 190a § 2 of the Penal Code a sufficient answer to identity theft? Which conduct remains outside it?

Remember this

- The **Lanzarote Convention** (2007, in force 2010) is the binding treaty on the protection of children against sexual exploitation. Article 23 concerns grooming.
- Polish law criminalises online contact with a child under 15 for a sexual purpose (**Article 200a**), without requiring a meeting.
- **Stalking** is Article 190a § 1 of the Penal Code. Its second paragraph penalises **impersonation**. International sources: Article 34 of the Istanbul Convention and Directive (EU) 2024/1385.
- **Identity theft** has no legal definition. It is covered by several offences, for example illegal access, forgery, fraud and impersonation.

European Union law on cybercrime

The Budapest Convention is a treaty of the Council of Europe. Within the European Union, the same subject is regulated by directives and regulations, which are binding in the manner described in Section 1: a directive binds the Member States as to the result, and a regulation applies directly. The Union has competence in criminal law only on the basis of Article 83 of the Treaty on the Functioning of the European Union, for serious crime with a cross-border dimension, and this explains why Union law on

cybercrime consists of directives that set minimum rules. The table gives a map of the most important instruments.

Instrument	Subject	Relation to the Budapest Convention and to national law
Offences (minimum rules)		
Directive 2013/40/EU on attacks against information systems	Illegal access (Article 3), illegal system interference (Article 4), illegal data interference (Article 5), illegal interception (Article 6), tools (Article 7), incitement, aiding and attempt (Article 8)	The Union counterpart of Articles 2 to 6 of the Budapest Convention. The corresponding Polish provisions include Articles 267, 268a and 269 to 269b of the Penal Code
Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography	Offences concerning abuse, exploitation, child pornography and solicitation (Article 6); measures against websites	The Union counterpart of Article 9 of the Budapest Convention and of the Lanzarote Convention
Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment	Fraud with payment instruments and information system-related fraud	Corresponds to Article 8 of the Budapest Convention
Directive (EU) 2024/1385 on combating violence against women and domestic violence	Cyber stalking, cyber harassment, non-consensual sharing of intimate material, cyber incitement	No counterpart in the Budapest Convention. Transposition by 14 June 2027
Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online	Removal orders for terrorist content, to be executed within one hour	Regulation of content, with cross-border effect of removal orders
Procedure and cooperation		
Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 (e-Evidence package)	European production and preservation orders addressed directly to service providers, and the designation of legal representatives	The Union counterpart of the Second Additional Protocol to the Budapest Convention
Directive 2014/41/EU on the European Investigation Order	Obtaining evidence between Member States on the basis of mutual recognition	Replaces mutual legal assistance in the Union, which Article 25 of the Budapest Convention regulates between other states
Regulation (EU) 2016/794 (Europol), Regulation (EU) 2018/1727 (Eurojust), Regulation (EU) 2017/1939 (European Public Prosecutor's Office)	Institutions for cooperation and for prosecution	Institutional law of the Union: networks of national authorities coordinated by Union bodies
Related regulation, discussed in the following sections		
General Data Protection Regulation, Digital Services Act, Digital Markets Act	Data protection, liability and duties of online platforms, and competition in digital markets	Referred to here only. Each of them is covered in the following sections of the course

Three observations follow from the table. First, the Union does not accede to the Budapest Convention, but all the Member States are parties to it, and Union law is designed to be compatible with it. Second, Union law makes the procedural part of the Convention more effective within the Union, because the e-Evidence package allows an authority of one Member State to address a service provider directly, without the intervention of the authority of the second state. This is a notable shift from the model of mutual legal assistance, in which the second state decides. Third, the instruments illustrate how international and regional law support each other: the Budapest Convention gives the global standard, and Union law gives deeper integration for a smaller group of states.

Remember this

- EU criminal law on cybercrime consists of **directives with minimum rules** (Article 83 TFEU). Key instruments: Directive 2013/40/EU (attacks against information systems), Directive 2011/93/EU (child sexual abuse) and Directive (EU) 2019/713 (payment fraud).
- The **e-Evidence package** (Regulation (EU) 2023/1543 and Directive (EU) 2023/1544) allows orders directly to service providers in other Member States.
- The Union is not a party to the Budapest Convention. The Member States are.

The Hanoi Convention

The United Nations Convention against Cybercrime, known as the Hanoi Convention after the place where it was opened for signature, was negotiated by an ad hoc committee established by the General Assembly of the United Nations. The General Assembly adopted it in December 2024 and it was opened for signature in Hanoi. It enters into force after it has been ratified by forty states. Like every treaty, it binds only the states that have ratified it:

- it requires the parties to criminalise a set of core cyber-dependent offences and certain cyber-enabled offences, such as fraud, and offences concerning child sexual abuse material;
- it provides for procedural powers to investigate crime and to secure electronic evidence;
- it provides for international cooperation, including mutual legal assistance, the use of a contact point available around the clock, and the sharing of electronic evidence of serious crimes;
- it contains provisions on the protection of human rights, which are a central issue in the debate.

	Budapest Convention	Hanoi Convention
Adopted by	Council of Europe, with participation of non-members	General Assembly of the United Nations
Membership	Open to non-members by invitation	Universal in principle
Scope	Defined list of offences and procedural powers	Wider scope: certain crimes committed by means of information and communications technology and the sharing of electronic evidence of serious crimes
Status	In force since 2004	Opened for signature in Hanoi; in force after forty ratifications
Debate	Seen as an established standard, criticised for its age and for its reach to non-members	Supporters stress its universal reach. Critics fear that broad powers and weaker safeguards may be misused

Current number of ratifications

- **Budapest Convention: 83 Parties.** A further 14 states have signed it or have been invited to accede. Source: Council of Europe, Cybercrime Division website (<https://www.coe.int/en/web/cybercrime/the-budapest-convention>), consulted in October 2026.
- **Hanoi Convention: 3 ratifications and 76 signatories, as of May 2026.** The states that had ratified were Qatar, Azerbaijan and Viet Nam. The Convention is not yet in force: it requires forty ratifications and enters into force on the ninetieth day after the fortieth instrument is deposited. It remains open for signature until 31 December 2026. The official status is kept by the United Nations Treaty Collection (<https://treaties.un.org>).

The two instruments are not mutually exclusive. A state may be a party to both. Their relationship raises a question familiar from other parts of international law, such as the law of the sea or international environmental law: the **fragmentation** or **convergence** of rules when several treaties regulate the same subject. In both areas, the question is whether one treaty becomes the global standard or whether several regimes co-exist.

Questions for discussion

1. What is the significance of the fact that the Hanoi Convention was adopted by the General Assembly and that the Budapest Convention is a regional treaty?
2. Which safeguards should a treaty on cybercrime provide for suspects and for users?
3. Is the sharing of electronic evidence of any serious crime compatible with the protection of human rights?

Remember this

- The **Hanoi Convention** (UN Convention against Cybercrime) was adopted by the General Assembly in December 2024. It binds only the states that ratify it and enters into force after forty ratifications.
- The Budapest and Hanoi Conventions can both apply to one state. Their relationship is a question of **fragmentation or convergence**, as in the law of the sea and environmental law.

Summary of the law of cybercrime

This part of the course has described how international law and national law respond to cybercrime. The main points are the following.

- **No legal definition.** International law does not define cybercrime. The treaties list offences that the parties must criminalise.
- **Binding treaties.** The Budapest Convention (2001) and the United Nations Convention against Cybercrime (the Hanoi Convention, 2024) bind only the states that ratify them. They are supplemented by the two Additional Protocols to the Budapest Convention and, within the European Union, by Union law on electronic evidence.
- **Three elements.** The treaties harmonise offences, give authorities procedural powers to collect electronic evidence, and establish international cooperation. Offences must be committed intentionally and without right.
- **Jurisdiction.** The parties establish jurisdiction on the grounds of territory, flag, registration and nationality (Article 22 of the Budapest Convention). Where several states claim jurisdiction, they must consult. Enforcement remains limited by the territory of each state.
- **National implementation.** States implement the treaties in their own criminal law, for example the Polish Penal Code. The wording of national offences differs from the treaty text, and students must always compare them.
- **Safeguards.** Powers to investigate must respect human rights, legality and proportionality.

The central lesson is that **cybercrime is countered by the state, through criminal law, criminal procedure and international cooperation**. Victims, companies and security researchers have no power to investigate, to search or to punish. Their role is to protect their systems, to report incidents and to cooperate with the competent authorities.

Important

Active cyberdefence, which is discussed next, is not a lawful way to fight cybercrime. It is a contested measure of cybersecurity. When a private person or a company accesses the systems of an alleged attacker, that conduct may itself be a criminal offence, for example illegal access under Article 2 of the Budapest Convention and its counterpart in national law. The lawful route against a perpetrator is to report the crime and to leave investigation to the authorities.

The next part of the course moves from the law of cybercrime, which reacts to offences that have been committed, to the law of cybersecurity, which concerns the prevention of attacks and the resilience of systems. Active cyberdefence is introduced there as a debated question of cybersecurity policy and law. It is not part of the law of cybercrime.

Cybersecurity

The first part of this section discussed cybercrime, which the law counters after offences were committed, through criminal law and cooperation between states. This part concerns cybersecurity: the prevention of attacks, the resilience of systems and the responsibility of states. It begins with a contested practice, active cyberdefence, and then turns to the law of the European Union and of Poland, to international law and to selected current questions.

Active cyberdefence

How can a person protect themselves from cybercrime? How can a company be made cybersecure? One of the most contested answers is active cyberdefence: measures by which the victim of an attack does not only protect its own systems, but also acts against the attacker, for example by accessing the attacker's system, retrieving or deleting data, or tracing the attack. This practice is often called hack back.

Case study: Jack and Mike

Jack runs a start-up company in a shared office space (box 101). In the same office space (box 102), a competitor is run by Mike. One morning Jack finds that his client database has been deleted from his computer, together with all local backup copies. During the lunch break Mike implies that he now owns the database. Jack hires a company to steal back the database, to take a copy of Mike's database and to destroy all local copies of it.



Figure 8. Shared office space. Source: DeskTime.

Is Jack right to do so? The following points can structure the discussion:

- **Criminal law.** Accessing Mike's computer and copying and deleting his data are, in principle, offences of illegal access and data interference, in the Budapest Convention and in the national criminal law. Hiring a company to do so does not remove Jack's responsibility, since a person who orders an offence can be liable as an instigator or accomplice.
- **Justification.** Criminal law recognises self-defence and necessity, but only under strict conditions: the attack must be present and unlawful, and the response must be necessary and proportionate. Jack's data had already been deleted, and the retaliation took place later, so the attack was not ongoing. The deletion of Mike's data goes beyond retrieving what belongs to Jack.

- **Alternatives.** Jack can report the crime to the police, request the preservation of evidence and ask a court for an injunction or compensation. These measures use the enforcement jurisdiction of the state and are not private.
- **Collateral damage and attribution.** A person who strikes back may hit the wrong target, for example a server of an innocent third party that the attacker has used. Attribution of an attack is difficult and often uncertain.

The debate on hack back

Status: not enacted

The Active Cyber Defense Certainty Act is a proposal. It is not law. The bill (H.R. 4036) was introduced in the United States House of Representatives in October 2017 and was referred to a committee. It was not adopted and it lapsed at the end of that session of Congress. A later version was introduced in 2019 and was not enacted either. No United States statute authorises private active cyberdefence. Unauthorised access to another person's computer remains an offence under section 1030 of title 18 of the United States Code.

The bill proposed to amend section 1030 of title 18 of the United States Code, the federal statute on computer fraud and abuse. As a summary in the author's words, and not a quotation, it would have done four things: exempt from liability tools that identify the source of an intrusion (so-called attributional technology); create a defence to prosecution for a victim of a persistent intrusion who accesses the attacker's computer to establish attribution, to disrupt the intrusion or to monitor the attacker; exclude measures that destroy the data of others, recklessly cause injury or financial loss, or affect the computers of government and of the justice system; and require the defender to notify the Federal Bureau of Investigation before acting.

The screenshot displays the official page for H.R. 4036 - Active Cyber Defense Certainty Act on the Congress.gov website. The page header includes the Congress.gov logo and navigation links. The main content area shows the bill's title, sponsor (Rep. Graves, Tom), and committees (House - Judiciary). The latest action is listed as 'House - 11/01/2017 Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations'. A progress tracker shows the bill's status: Introduced, Passed House, Passed Senate, To President, and Became Law. The page also includes a summary section and links to related bills and documents.

Figure 9. H.R. 4036, Active Cyber Defense Certainty Act (a bill, not enacted). Source: congress.gov.

The debate resembles an old discussion about the use of private force at sea. States once issued letters of marque to private ships, the so-called privateers, which were allowed to attack enemy vessels. Today, shipping companies hire private security companies for protection against piracy. The question is whether private actors in cyberspace should be allowed to use defensive measures that go beyond the protection of their own systems, and under whose control. In international law, countermeasures against internationally wrongful acts can be taken by states, not by private companies, and a state that tolerates private hack back may become responsible for it.

A contrast: Chinese law

Chinese law, as reviewed for this course, contains no provision comparable to the proposed Active Cyber Defense Certainty Act. It does not allow private entities to access the computers of attackers. Its approach is state centred and defensive. The Cybersecurity Law, in force since 1 June 2017, requires network operators to take technical measures against data leaks and theft and to report incidents, and it imposes stricter duties on operators of critical information infrastructure, together with requirements on the location of data and on the use of licensed virtual private networks. The Criminal Law penalises illegal intrusion into computer information systems and the destruction of such systems (Articles 285 and 286).

Two later statutes of 2021, the Data Security Law and the Personal Information Protection Law, are closer to the problem of foreign orders discussed in this section. The Data Security Law restricts the provision of data stored in China to foreign judicial and law enforcement bodies, which requires the approval of the competent authorities (Article 36). The Personal Information Protection Law provides for the export of data in legal assistance only on application (Article 41), allows the blacklisting of foreign organisations that harm Chinese interests (Article 42), and allows the government to adopt retaliatory measures against foreign governments that impose discriminatory prohibitions or sanctions on China (Article 43). The Data Security Law repeats this anti-sanction clause (Article 26). These provisions regulate the response of the state to foreign measures. They resemble blocking rules, such as Article 48 of the General Data Protection Regulation, more than they resemble a right of private active defence.

Questions for discussion

1. Where is the line between defence of one's own systems and an attack on the systems of others?
2. Would you support a statute that legalises hack back under conditions? Which conditions would you propose?
3. Under which conditions can a state be responsible for acts of private companies that it did not forbid?

Remember this

- **Hack back**, that is, counter-intrusion by a victim of an attack, is legally contested. In principle, the powers of enforcement belong to states and not to private persons.
- The US Active Cyber Defense Certainty Act is **only a bill. It is not law.**

International law and cybersecurity: responsibility and norms

Cybersecurity law is often presented as a matter of compliance, but it is also part of general international law. This part describes the legal framework that applies when a state, and not a private person, is behind a malicious cyber operation.

State responsibility

The law of state responsibility, which is codified in the Articles on Responsibility of States for Internationally Wrongful Acts of the International Law Commission (2001), applies to cyber operations. A state is responsible for a breach of an international obligation if the conduct is attributable to it. Attribution depends on the status of the actor or on the control that the state exercises over the conduct. Attribution in cyberspace is a technical and a legal challenge, because the identification of the author is difficult and each state decides for itself whether it will make an attribution public. A state

may react to an internationally wrongful act with countermeasures, but only under strict conditions, such as proportionality, and only after the state responsible was called upon to cease the act. This is the point that distinguishes lawful state action from the hack back by private persons, which was discussed above: countermeasures are an instrument of states.

Sovereignty and due diligence

The question whether sovereignty is a binding rule of international law that cyber operations can breach, or only a principle, is debated. The majority of states and the experts of the Tallinn Manual 2.0 (2017) treat it as a rule. Some states, for example the United Kingdom, have taken the view that it is a principle without an independent prohibition. A related question is whether states have a due diligence obligation not to allow their territory to be used for acts that harm other states. The same concept is familiar from environmental law and the law of the sea. It illustrates how rules from one field of international law are used to answer questions in another.

Norms of responsible state behaviour

The United Nations General Assembly has endorsed the reports of groups of governmental experts (2013 and 2015) and of an open-ended working group, which state that international law applies in cyberspace. The reports of 2015 list voluntary, non-binding norms of responsible state behaviour. They are political commitments and soft law. They do not create obligations, but they shape the expectations of states and may contribute to the formation of customary law through state practice and *opinio juris*. After the work of the open-ended working group in 2021 to 2025, the United Nations established a permanent mechanism for the dialogue of states on cybersecurity. The Union, for its part, has adopted a framework for a joint diplomatic response, the Cyber Diplomacy Toolbox, which includes the restrictive measures mentioned above.

Type of norm	Examples in this part of the course	Binding?
Treaty law	Budapest Convention, Lanzarote Convention, Hanoi Convention	Yes, for the states that are parties
Union law	NIS 2 Directive, Directive 2013/40/EU, Regulation (EU) 2023/1543	Yes, within the Union, as described in Section 1
Customary international law and general principles	State responsibility, sovereignty, due diligence	Yes, and their content in cyberspace is debated
Soft law and political commitments	Norms of responsible state behaviour, Tallinn Manual 2.0, guidance notes of the Cybercrime Convention Committee	No, they are non-binding, although they may influence interpretation and practice
Technical standards	NIST Cybersecurity Framework, ISO/IEC 27001	No, unless a law makes them binding by reference

Remember this

- Cyber operations of states are governed by **state responsibility**: attribution, and **countermeasures**, which only states can take.
- The UN **norms of responsible state behaviour** are voluntary and non-binding. They are soft law.
- Always distinguish **binding law**, **soft law**, **political commitments** and **technical standards**.

Cybersecurity law: the NIS 2 Directive

The cybersecurity of networks and information systems is regulated in the European Union by Directive (EU) 2022/2555, known as the NIS 2 Directive. It replaced the first NIS Directive. As Section 1 explained, a directive is binding as to the result to be achieved and must be implemented in national law. The

Member States were required to adopt the implementing measures by October 2024, and the national acts, not the Directive itself, create obligations for companies. The Directive aims at a high common level of cybersecurity across the Union.

Who is covered?

The Directive applies to public and private entities that are active in sectors of high criticality and in other critical sectors, when they are at least medium-sized. In some cases it applies regardless of size. Such entities are classified as **essential** or **important**, which determines the intensity of supervision.

- **Sectors of high criticality** include energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, management of information and communications technology services, public administration and space.
- **Other critical sectors** include postal and courier services, waste management, chemicals, food, manufacturing of certain products, digital providers such as online marketplaces, search engines and social networking platforms, and research.

What are the main obligations?

- **Governance.** The management bodies of the entities must approve the cybersecurity risk-management measures and oversee them. They can be held accountable for their infringement.
- **Risk management.** Entities must take appropriate and proportionate technical, operational and organisational measures. They include risk analysis, incident handling, business continuity, supply chain security, vulnerability handling, the use of cryptography and access control.
- **Incident reporting.** Entities must notify significant incidents to the national authority or to the computer security incident response team (CSIRT). The process has three steps: an early warning within 24 hours of becoming aware of the incident, an incident notification within 72 hours, and a final report within one month.
- **Supervision and penalties.** Competent authorities supervise compliance. The maximum administrative fines are at least 10 million euros or 2 percent of the total worldwide annual turnover for essential entities, and at least 7 million euros or 1.4 percent for important entities, whichever is higher.

Institutions and cooperation

Each Member State designates one or more competent authorities, a single point of contact and one or more CSIRTs, and adopts a national cybersecurity strategy. At the Union level, the Directive established a cooperation group, a network of CSIRTs, the European cyber crisis liaison organisation network (EU-CyCLONe) and relies on the European Union Agency for Cybersecurity (ENISA). This is an example of the institutional law and global governance that shapes cybersecurity: a network of national authorities coordinated by Union bodies.

NIS 2 also deals with jurisdiction. In general, an entity falls under the jurisdiction of the Member State in which it is established. Certain providers, for example of domain name system services, are subject to the jurisdiction of the Member State in which they have their main establishment in the Union. An entity that is established outside the Union but offers services in the Union must designate a representative in the Union. This is a further example of the effects principle: the Union regulates conduct outside its territory when it affects the Union.

The Directive is accompanied by other Union instruments, in particular the Cyber Resilience Act, Regulation (EU) 2024/2847, which sets cybersecurity requirements for products with digital elements,

and the Directive on attacks against information systems, which establishes minimum rules for the definition of offences.

The table lists the main Union instruments that are connected with NIS 2.

Instrument	Subject
Regulation (EU) 2019/881 (Cybersecurity Act)	Mandate of the European Union Agency for Cybersecurity (ENISA) and European cybersecurity certification schemes. The Act is under review
Directive (EU) 2022/2557 (Critical Entities Resilience Directive)	Resilience of entities that provide essential services against all hazards, including physical ones
Regulation (EU) 2022/2554 (Digital Operational Resilience Act)	Digital operational resilience of the financial sector, which is a specific regime next to NIS 2
Regulation (EU) 2024/2847 (Cyber Resilience Act)	Cybersecurity requirements for products with digital elements
Regulation (EU) 2025/38 (Cyber Solidarity Act)	European cybersecurity alert system and a mechanism for emergency response
Council Regulation (EU) 2019/796 and Council Decision (CFSP) 2019/797	Restrictive measures against persons and entities responsible for cyber-attacks. They are used by the Union as a response to malicious cyber activity, outside the criminal process

A voluntary counterpart: the NIST Cybersecurity Framework

NIS 2 is binding Union law. The Cybersecurity Framework of the United States National Institute of Standards and Technology (NIST) is a different kind of instrument. It is a voluntary technical standard, not a treaty or a statute. Version 1.1 was released in April 2018 and was developed for critical infrastructure. NIST states that it has been adopted voluntarily by large and small organisations across all industry sectors, and by governments. A Presidential Executive Order of 2017 directed United States federal agencies to use it, which shows how a voluntary standard can acquire legal weight through national law.

The Framework organises cybersecurity activities into five functions, shown in the figures below: Identify (understand assets, risks and governance), Protect (safeguards such as access control, training and data security), Detect (monitoring and recognising anomalies), Respond (planning, communication, analysis and mitigation) and Recover (restoring services and learning from incidents). Version 1.1 added guidance on authentication and identity, self-assessment of risk, management of supply chain risk and vulnerability disclosure. A later version, 2.0, published in 2024, added a sixth function, Govern, which places cybersecurity within the management of the organisation.

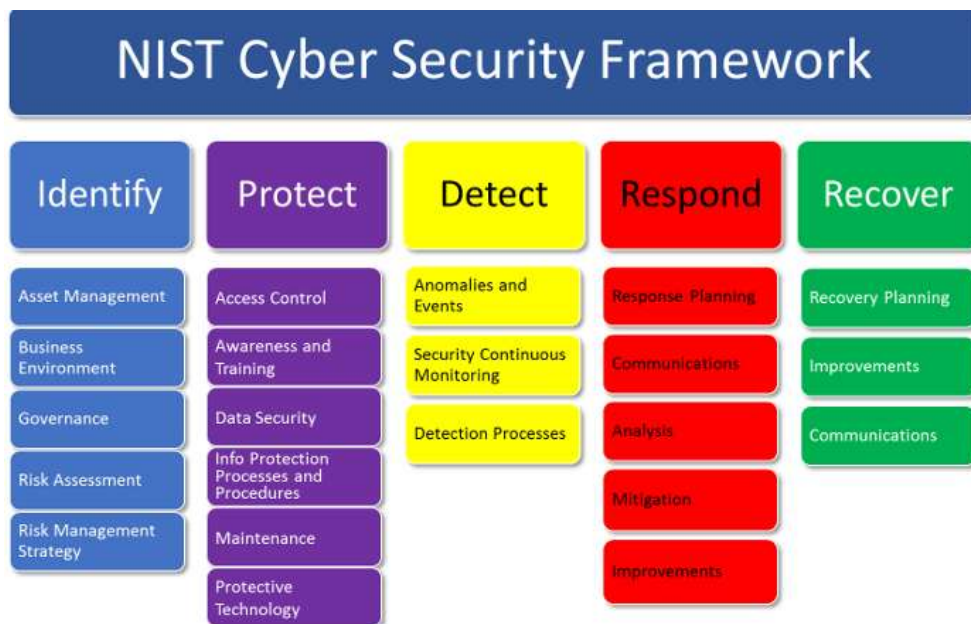


Figure 10. The NIST Cybersecurity Framework: five functions and their categories.



Figure 11. The five functions of the NIST Cybersecurity Framework, version 1.1.

The comparison is useful for legal analysis. The five functions correspond to the risk-management measures and the incident handling that NIS 2 requires, but NIS 2 turns them into legal obligations with supervision and fines, while the NIST Framework remains a guide that organisations choose to apply. For this reason, entities subject to NIS 2 often use frameworks of this type to show compliance. The instrument also illustrates the difference between binding law, technical standards and soft law, a distinction introduced in Section 1. Source: NIST, news release of 16 April 2018 on version 1.1 of the Framework.

Questions for discussion

1. Why does the Directive hold the management bodies of entities accountable?
2. What are the advantages of a three-step incident reporting procedure?
3. Is a company in a third state, which provides cloud services to customers in the Union, covered by the Directive?

4. What is the legal difference between NIS 2 and the NIST Framework, and how can a voluntary standard become relevant for legal compliance?

Remember this

- **NIS 2** is Directive (EU) 2022/2555. It binds Member States as to the result, and **national acts** create the obligations for companies.
- Entities are **essential** or **important**. Management bodies are accountable.
- Incident reporting has three steps: **24 hours** (early warning), **72 hours** (notification) and **one month** (final report).
- The **NIST Framework** is a voluntary standard (soft law or technical standard), not binding law.

The Polish national cybersecurity system

Poland implemented the first NIS Directive by the Act of 5 July 2018 on the national cybersecurity system (ustawa o krajowym systemie cyberbezpieczeństwa), Journal of Laws 2018 item 1560, as amended. The Act is the main statute of Polish cybersecurity law. Under the hierarchy of sources described in Section 1, it is a statute, and implementing regulations are issued on its basis. The legislator has been amending the Act to implement the NIS 2 Directive, so students should always check the current consolidated text.

In summary, the Act, in the version known to us, regulates the following matters. This summary is not a quotation of the Act.

- **Entities covered.** Operators of essential services, who are identified in administrative decisions, providers of digital services and certain public entities.
- **Obligations.** Operators must carry out risk estimation, apply technical and organisational measures, manage incidents, and notify serious incidents to the competent CSIRT.
- **Institutions.** The Act establishes three national computer security incident response teams, called CSIRT GOV (government), CSIRT MON (Ministry of National Defence) and CSIRT NASK (Research and Academic Computer Network, NASK), which are responsible for different groups of entities. It also designates the minister competent for computerisation and sectoral authorities, and establishes a single point of contact for cooperation within the Union.
- **Strategy and coordination.** It provides for the national cybersecurity strategy and for coordination of the system.
- **Sanctions.** It provides for administrative fines for infringements of the obligations.

The Polish approach illustrates the relationship between Union law and national law: the Directive sets the result, and the national statute chooses the form and the methods. Students should compare the categories of the Polish Act with the categories of the Directive and observe the differences.

Questions for discussion

1. Which sources of law apply to the cybersecurity obligations of a Polish hospital?
2. What is the role of the CSIRTs, and why are there several of them?
3. How does the Polish Act ensure the cooperation of the Polish system with the institutions of the Union?

Remember this

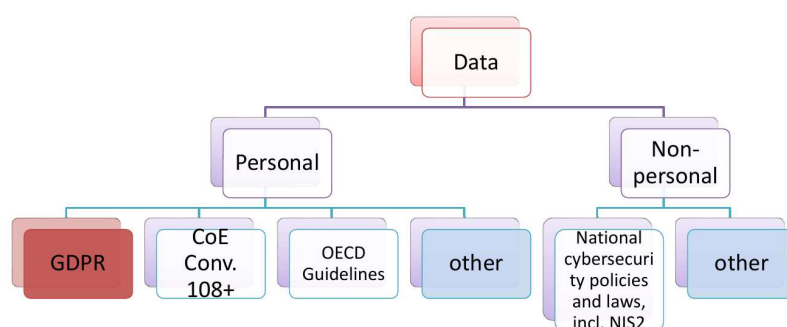
- The Polish **Act of 5 July 2018** on the national cybersecurity system is the main statute. It must be read with the NIS 2 Directive, and the current consolidated text should always be checked.
- Three national computer security incident response teams (CSIRTs) handle incidents for different groups of entities.

Further topics: data, surveillance and encryption

The following topics extend the lecture. They show how the principles of jurisdiction, the protection of rights and cybersecurity meet in situations that are likely to interest students of computer science. They can be used for discussion in the meetings on cybercrime and cybersecurity, or in Section 3, which deals with data.

Jurisdiction and data governance

Data can be divided into personal data and non-personal data. Different legal regimes apply. For personal data, the main instruments are the General Data Protection Regulation of the European Union, Convention 108+ of the Council of Europe and the Guidelines of the Organisation for Economic Co-operation and Development (OECD). For non-personal data, the rules are found in national cybersecurity policies and laws, including the NIS 2 Directive, and in other sectoral instruments.



J. Kulesza, Legal Aspects of Computer Science 2025

35

Figure 12. Data governance: legal regimes for personal and non-personal data.

The question of jurisdiction over data is difficult, because data can be stored in one state, controlled from another, and concern persons in a third. States use different connecting factors: the place where the data are stored, the place of establishment of the service provider, or the place where the data subject lives. The CLOUD Act of the United States, which was mentioned in Section 1, uses control by a provider that is subject to US jurisdiction as its criterion, regardless of the place of storage.

A well-known example of the misuse of personal data is the Cambridge Analytica case, in which personal data collected through a social network were used for political profiling. The case contributed to the debate on data protection and the regulation of platforms.

State surveillance and the legal basis of mass surveillance

In 2013, press reports based on documents released by Edward Snowden revealed a programme of the United States National Security Agency called PRISM (Planning Tool for Resource Integration, Synchronization, and Management). The lecture lists three related elements:

- **Upstream:** gathering data from the infrastructure of the internet;
- **XKeyscore:** analysing the collected data;

- **Bullrun:** attempts to weaken encryption, that is, to obtain backdoors.



Figure 13. Press report on the PRISM programme. Source: The Washington Post.

The legal basis of such programmes for foreigners is found in United States statutes. The European Parliament study on cybercrime and privacy in the cloud, which is cited in the lecture, describes how legislative changes broadened the reach of surveillance, in particular the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISAA). It states:

European Parliament study, Fighting cyber crime and protecting privacy in the cloud, p. 34

There followed a test case at the Foreign Intelligence Surveillance Court of Review, which held definitively that the Fourth Amendment requirement for a specific warrant only applied to surveillance directed at US persons. This opened the door for Congress to enact FISAA §1881a in 2008, which authorized mass-surveillance of foreigners (outside US territory), but whose data was within range of US jurisdiction. However, the most significant change escaped any comment or public debate altogether. The scope of surveillance was extended beyond interception of communications, to include any data in public cloud computing as well. This change occurred merely by incorporating “remote computing services” into the definition of an “electronic communication service provider”.

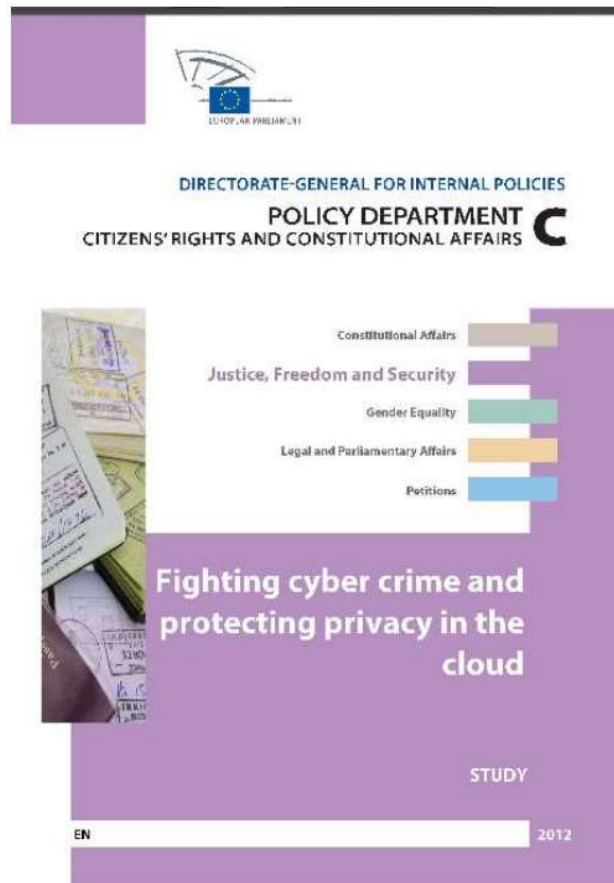


Figure 14. Cover of the study: D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer, *Fighting cyber crime and protecting privacy in the cloud* (European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Brussels, 2012). Available at: [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET\(2012\)462509_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf)

For students of international law, such programmes raise the question of the extraterritorial effect of national surveillance statutes, the protection of privacy of persons outside the territory of the state that conducts surveillance, and the relationship between the law of the state where the data are stored and the law of the state that requests them.

Spyware: the Pegasus case

Pegasus is spyware developed by NSO Group, a private company. According to product documentation shown in the lecture, it can be installed on mobile phones of several operating systems, collects data from the infected device and transmits them to the operator. The data that can be collected include messages, emails, photos, contacts, calendar records, browsing history, location and the recording of the microphone. Reports on the use of Pegasus against journalists, lawyers and politicians in several states led the European Parliament to set up a committee of inquiry, the PEGA committee, to investigate the use of Pegasus and equivalent surveillance spyware.

Figure 1: Pegasus High Level Architecture

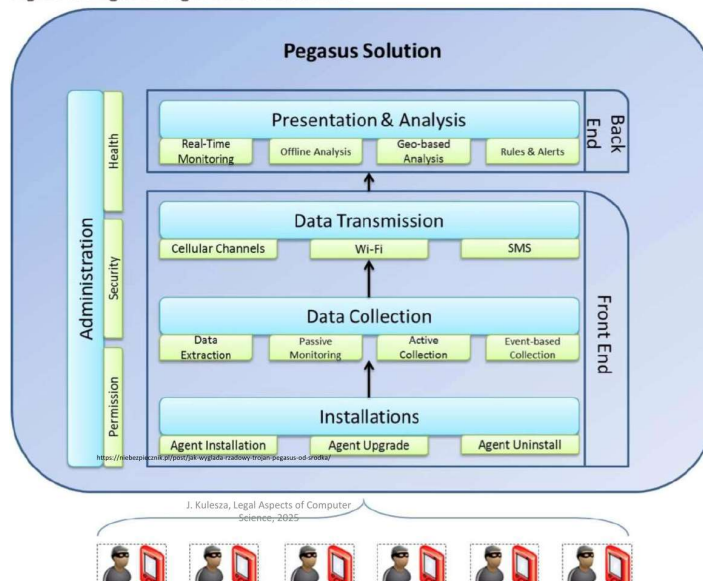


Figure 15. High level architecture of the Pegasus solution. Source: product documentation.

Figure 4: Collected Data



Figure 16. Data that can be collected from the target device. Source: product documentation.



Multimedia Centre
Parlament Europejski

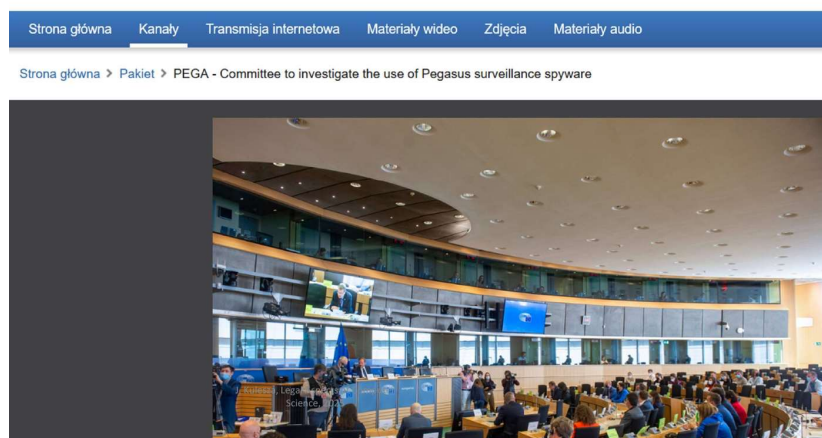


Figure 17. Hearing of the PEGA Committee of the European Parliament. Source: European Parliament.

The legal issues include the lawfulness of surveillance (a legal basis in a statute, a legitimate aim, necessity and proportionality, and independent oversight), the responsibility of a state that buys and uses such technology, and the regulation of the export of surveillance technology. Human rights bodies

require that interferences with the privacy of communications have a basis in law that is accessible and foreseeable, and that they are subject to effective safeguards.

Anonymity and encryption: Tor and VPN

Technologies that protect anonymity and privacy raise questions for the law. **Tor** (The Onion Router) routes the communication of a user through a series of volunteer nodes, so that none of them knows both the sender and the recipient. A virtual private network (**VPN**) creates an encrypted connection between the user and a server, and hides the traffic from the local network and the internet access provider. These tools are used by journalists, activists and ordinary users, but also by offenders.

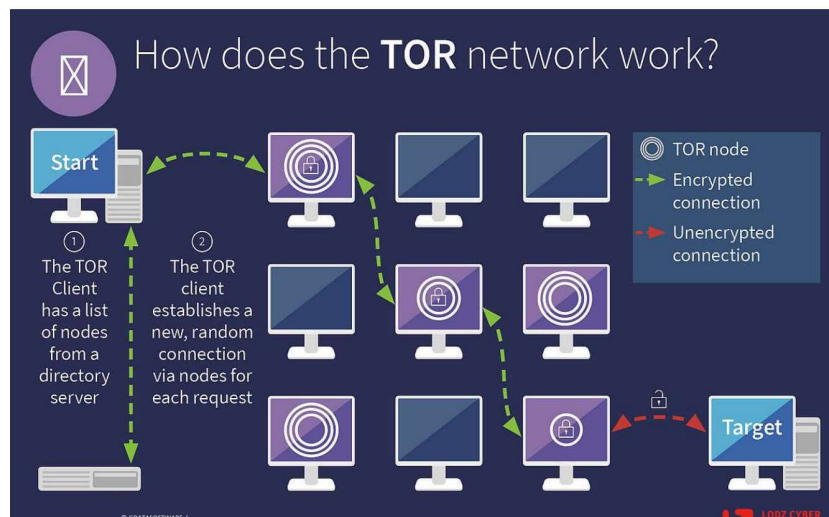
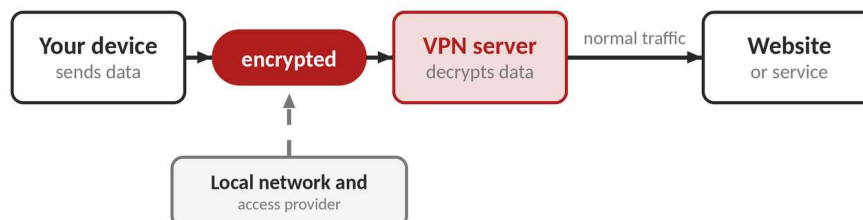


Figure 18. How the Tor network works. Source: G DATA.



They see only encrypted traffic to the VPN server, not its content or destination.
The website sees the address of the VPN server, not that of the user.

Figure 19. How a VPN protects data. Diagram prepared by the author.

Encryption is the transformation of readable data into a form that is unreadable without a key. In symmetric encryption the same key is used for encryption and decryption. In asymmetric (public-key) encryption, a pair of keys is used: a public key to encrypt and a private key to decrypt. In end-to-end encrypted communication, only the sender and the recipient can read the message, and an eavesdropper on the network, or the provider, cannot.

Symmetric encryption



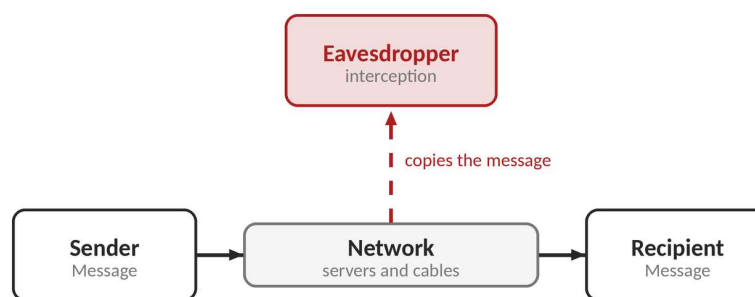
The sender and the recipient use the same key, which must be exchanged in secret.

Asymmetric (public-key) encryption



Anyone can encrypt with the public key. Only the owner of the private key can decrypt.

Figure 20. The principle of symmetric and asymmetric encryption. Diagram prepared by the author.



Without encryption the content is readable. With encryption it is not.

Figure 21. Communication over a network and an eavesdropper. Diagram prepared by the author.

Messaging applications differ in their security features and in the jurisdiction in which the provider is based, which may determine whether authorities can require the provider to disclose data. The table below lists the features that matter most for the law. It does not rate individual applications, because their features and the places of establishment of their providers change over time.

Feature	What it means	Why it matters legally
End-to-end encryption by default	Only the sender and the recipient hold the keys. The provider cannot read the content.	A provider may be unable to disclose content even if ordered to do so. This is the centre of the debate on access for law enforcement.
Metadata held by the provider	Data about the communication, such as who communicated with whom, when, and from which device.	Metadata may be disclosed to authorities even when content is encrypted. Its collection is also regulated by data protection and communications law.
Place of establishment of the provider	The state whose law applies to the provider and whose authorities can order it to act.	It determines the jurisdiction to prescribe and to enforce, the conflicts between orders of different states, and the rules on mutual legal assistance.
Open source code and independent audits	The code can be examined, and independent experts have checked the security of the application.	They allow users and regulators to verify security claims. Standards and audits are technical measures, not binding law, unless a statute refers to them.
Registration with a phone number or without	Whether the user must identify himself with a personal identifier to create an account.	It influences anonymity, the identification of suspects, and the personal data that the provider holds.

The dark web and online markets

Anonymity technology is also used for illegal online markets. The Silk Road website, which sold drugs and other illegal goods for bitcoins, was seized by the Federal Bureau of Investigation in 2013. A later

market, Hydra, was a large Russian-language marketplace that was shut down by law enforcement in 2022. These cases show the importance of the cooperation of authorities in different states and the link between jurisdiction, evidence and technology.

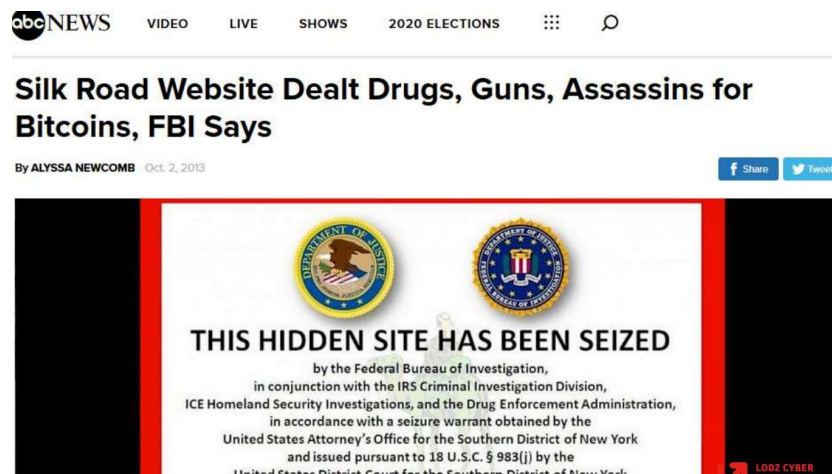


Figure 22. Notice of seizure of the Silk Road website. Source: ABC News.

The right to cryptography as a human right?

Is there a human right to use encryption? States take different positions. Some recognise a general right to encryption. Others require a minimum or maximum strength of encryption, require licences, control the import and export of cryptographic products, or oblige providers or individuals to assist authorities, for example by disclosing keys. The UNESCO publication Human rights and encryption, shown in the lecture, argues that encryption is a means of protecting the rights to privacy and to freedom of expression. The opposing argument is that strong encryption hinders the investigation of serious crime, and states therefore need access to encrypted data under judicial control.

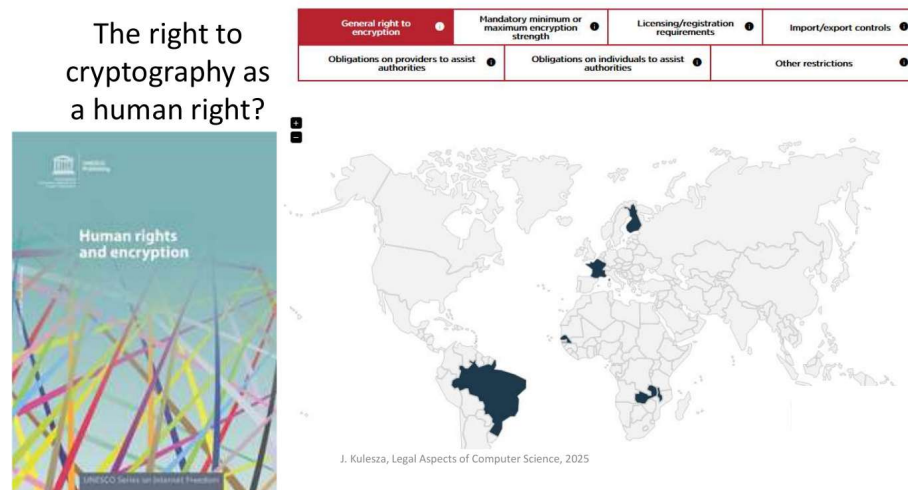


Figure 23. The right to cryptography as a human right? Legal approaches to encryption in the world. Source: UNESCO.

Questions for discussion

1. Should a state be allowed to require a provider of an encrypted messaging service to build in a means of access for authorities? What are the consequences for security?
2. Which safeguards should apply to the use of spyware by state authorities?
3. Which state has jurisdiction over a messaging provider established in one state, with servers in a second state and users in a third state?

Selected case law of European courts

The cases below illustrate how courts apply the principles of jurisdiction, privacy and legality to cyber matters. They are a starting point for discussion, and students should read the judgments.

Case	Court and year	Legal point	Relevance
Google v CNIL (C-507/17)	Court of Justice of the European Union, 2019	Union law does not require an operator of a search engine to remove links on all its versions worldwide, but it does not prohibit it. Removal is required for the versions in all Member States	Territorial reach of Union law and the limits of the effects principle
Glawischnig-Piesczek v Facebook Ireland (C-18/18)	Court of Justice of the European Union, 2019	Union law does not preclude an injunction against a platform to remove identical or equivalent content worldwide, within the framework of the relevant international law	Extraterritorial effect of a national court order
Schrems II (C-311/18)	Court of Justice of the European Union, 2020	The Court invalidated the Privacy Shield decision because United States surveillance law did not offer protection that is essentially equivalent to Union law	Link between foreign surveillance, such as the PRISM programme, and data transfers
Digital Rights Ireland (C-293/12) and La Quadrature du Net (C-511/18 and C-512/18)	Court of Justice of the European Union, 2014 and 2020	General and indiscriminate retention of communications data is disproportionate, except in limited situations of serious threats	Limits of investigative powers and of the procedural part of cybercrime treaties
EncroChat (C-670/22)	Court of Justice of the European Union, 2024	The Court set the conditions for using a European Investigation Order to obtain data intercepted by another Member State, and required respect for the rights of the defence	Cross-border electronic evidence
Big Brother Watch v United Kingdom	European Court of Human Rights, Grand Chamber, 2021	The bulk interception regime violated Articles 8 and 10 of the European Convention on Human Rights, because it lacked sufficient safeguards	Mass surveillance and the minimum safeguards
Podchasov v Russia	European Court of Human Rights, 2024	An obligation to retain communications and to decrypt them on request, which would weaken encryption for all users, violated Article 8	Encryption and the right to privacy

The regulation of platforms, the protection of personal data and the regulation of digital markets, which these cases touch, are covered in the following sections of the course: the Digital Services Act, the Digital Markets Act and the General Data Protection Regulation.

Remember this

- Data can be stored in one state, controlled from another and concern persons in a third. This makes **jurisdiction over data** a central problem, and conflicts between the laws of states (for example between the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) and the General Data Protection Regulation (GDPR)) are possible.
- **Encryption** protects security and privacy, and also limits access for law enforcement. The legal question is the balance between these interests.

Case studies

The five fictional case studies below apply the material of this section. They are intended for discussion in class or for individual study.

Case study 1: A ransomware attack with many links

A criminal group based in State A develops ransomware and rents it to affiliates. One affiliate, a national of State B who lives in State C, uses it to encrypt the network of a hospital in State D. The command server is rented from a provider in State E, and the ransom is paid in a cryptocurrency to a wallet whose owner is unknown.

The police of State D open an investigation. They find that several of the states involved are parties to the Budapest Convention, and that State A is not.

Questions for discussion

1. On which principles of jurisdiction can each state claim jurisdiction over the attack?
2. What is the difference between prescriptive, adjudicative and enforcement jurisdiction in this case, and which of them is the most difficult to exercise?
3. Which offences defined in the Budapest Convention were committed, and how can the police of State D obtain the data from the provider in State E?
4. What does the Convention require from states that are in conflict over who should prosecute?

Case study 2: Extradition of a national

A national of State X, living in State X, accessed from his home computer the network of a government agency in State Y and copied internal documents. State Y requests his extradition. The constitution of State X prohibits the extradition of its nationals. Both states are parties to the Budapest Convention.

The suspect argues that his conduct was a protest and that he caused no damage. He also asks the authorities of State X not to prosecute him, because the effects occurred in State Y.

Questions for discussion

1. Which principles of jurisdiction allow State Y and State X to claim jurisdiction?
2. What does the Budapest Convention require from State X if it refuses extradition solely on the basis of nationality?
3. How is the obligation to consult relevant for the choice of the state that will prosecute?
4. Which human rights and which safeguards should be taken into account in the extradition procedure?

Case study 3: A hospital and the NIS 2 Directive

A private hospital group in a Member State of the European Union is the victim of an attack. On Monday morning, at 8 a.m., the security team finds that the patient information system has been encrypted. The group informs the board on Tuesday. On Wednesday, the board decides to notify the authority. The national act that implements the NIS 2 Directive has been in force for some months.

The hospital group also uses a cloud provider based in a non-European state. The provider says that, as it has no establishment in the Union, the Directive does not apply to it.

Questions for discussion

1. Is the hospital group an essential or an important entity, and why does the classification matter?
2. Which reporting steps and time limits did the group have to observe, and when did the time start?
3. Who can be held responsible within the hospital group, and what penalties are possible?
4. Is the cloud provider covered by the Directive, although it is established outside the Union?

Case study 4: Hack back by a software company

A software company discovers that a group of hackers has stolen its source code and is selling it on a forum. The security team traces the attack to a server in another state. The team decides to access that server in order to delete the stolen code and to collect the identity of the buyers. It turns out that the server belongs to a small business that was itself the victim of the hackers.

The company argues that it acted in self-defence and that the authorities were too slow.

Questions for discussion

1. Which offences might the company and its employees have committed?
2. Under which conditions could self-defence or necessity justify the measures? Were these conditions met?
3. What legal and practical alternatives did the company have?
4. Could the state in which the company is established be responsible for the acts of the company under international law?

Case study 5: Spyware on the phone of a journalist

A journalist investigating corruption learns from a technical analysis that her phone was infected with spyware, which the manufacturer states it sells only to governments. The spyware was able to collect her messages, location and contacts, and to activate the microphone. The authorities of her state deny the use of spyware.

The journalist wants to bring a complaint. The company that produces the spyware is established in another state, and the operator of the servers is based in a third state.

Questions for discussion

1. Which rights of the journalist may have been infringed?
2. What conditions must be satisfied by a legal basis for surveillance by state authorities?
3. Which state has jurisdiction over the producer of the spyware, and what tools exist to hold a private company accountable?
4. What can the European Union and the Council of Europe do in such cases, and what is the legal value of their instruments?

Quiz

Choose one correct answer for each question.

1. A criminal group abroad launches an attack on a national hospital system, and the harm occurs on the territory of State D, although the offenders have never been in State D. State D wishes to prosecute them. Which principle of jurisdiction is the most important legal basis for State D to claim jurisdiction over this conduct?
 - A. The universality principle, which allows every state to prosecute any criminal offence irrespective of any link with the offender, the victim or the place of the act.
 - B. The effects principle, which allows a state to regulate conduct abroad that has substantial effects on its territory, and which is especially important for cyberspace.
 - C. The active personality principle, which allows a state to regulate the conduct of its own nationals abroad but does not cover foreign offenders at all.
 - D. The protective principle only, which is limited to the forgery of currency and does not apply to offences that cause harm to private persons.
2. A state wants to arrest a suspect who is in another state, and it asks its police to enter the other state's territory without notifying its authorities. Which statement correctly describes the rules of international law on jurisdiction in this situation?
 - A. A state may enforce its criminal law anywhere in the world as soon as it has prescriptive jurisdiction under one of the principles of jurisdiction.
 - B. Enforcement is permitted without consent whenever the suspect is a national of the state that wants to arrest him, because nationality overrides territory.
 - C. The question is purely technical, because international law regulates only the adoption of statutes and has no rules on enforcement by the police.
 - D. Enforcement jurisdiction is in principle territorial: the police may act on foreign territory only with the consent of that state or on the basis of a treaty.
3. The Budapest Convention contains a provision on jurisdiction. According to this provision, what must a party do when it refuses to extradite an alleged offender solely on the basis of his or her nationality, after a request for extradition?
 - A. It must establish jurisdiction over the offence so that it can prosecute the offender, which expresses the idea of *aut dedere aut judicare*.
 - B. It must release the person, because the Convention does not allow the prosecution of a national for offences committed in the territory of another party.
 - C. It must hand the case to the Secretary General of the Council of Europe, who decides which party should prosecute and informs the parties.
 - D. It must establish jurisdiction only if the other party offers a reciprocal promise to extradite its own nationals in similar cases.

4. A security researcher is accused of producing a program that can break into computer systems. The program was written to test the security of a system, and the owner of the system had asked for the test. How does the Budapest Convention treat this situation under the offence of misuse of devices?

- A. The researcher is liable in all cases, because the Convention bans every program capable of illegal access, whatever its purpose and the consent of the owner.
- B. The researcher is liable unless the program has been registered with the Council of Europe, which keeps a list of approved security tools for this purpose.
- C. The Convention does not require criminalising devices produced for the authorised testing or the protection of a computer system, as this is not done with the intent to commit an offence.
- D. The researcher is liable only if the program was sold, because the Convention does not cover the production or possession of tools for security testing.

5. The United Nations Convention against Cybercrime (Hanoi Convention) is often compared with the Budapest Convention. Which statement correctly describes a difference between the two instruments, or the legal position of the Hanoi Convention?

- A. It was adopted by the Council of Europe, and it replaces the Budapest Convention for all states from the day on which it was opened for signature.
- B. It was adopted within the United Nations, so it has a universal reach in principle, and it enters into force only after the required number of ratifications; it binds only ratifying states.
- C. It binds all members of the United Nations automatically from adoption by the General Assembly, since the Assembly may adopt legally binding rules for all states.
- D. It is a political declaration that creates no legal obligations, similar to the resolutions of the General Assembly, and it needs no ratification by states.

6. A medium-sized company in the energy sector in a Member State of the European Union suffers a significant cyber incident. Under the NIS 2 Directive, as transposed in national law, what are the reporting steps that the company must take?

- A. An early warning within 24 hours of becoming aware of the incident, an incident notification within 72 hours, and a final report within one month.
- B. A single report within 30 days of the incident, sent to the European Commission, which decides whether the national authority should be informed.
- C. No report is needed if the incident is solved within a week, because the Directive requires only an annual report on all incidents of the previous year.
- D. A report to the police within one hour, after which the national authority takes over and the company has no further duties of notification.

7. A national statute adopted to implement the NIS 2 Directive imposes obligations on a hospital group. The group argues that, because the Directive is addressed to the Member States, the group itself is not bound by anything. Which response correctly explains the relationship between the Directive and national law?

- A. The group is right, since directives never create obligations, and the national statute may be ignored until the Court of Justice confirms it.
- B. The group is wrong, because a directive applies directly to private persons in the same way as a regulation and the national statute has no role.
- C. The group is right only before the deadline for implementation, after which the national statute must be applied only if a regulation repeats it.
- D. The Directive binds the Member State as to the result to be achieved, and the state chooses the form and methods; the obligations of the group arise from the national implementing statute.

8. Poland regulates cybersecurity in the Act of 5 July 2018 on the national cybersecurity system. Which statement correctly describes an element of the national system established by that Act?

- A. A single private company, chosen by tender, handles all incident reports from all sectors and decides on the administrative fines for infringements.
- B. The Act applies only to public authorities, and it does not create any obligation for private operators of services that are essential for society.
- C. Three national computer security incident response teams (CSIRT GOV, CSIRT MON and CSIRT NASK) are responsible for different groups of entities, and serious incidents are notified to them.
- D. The Act abolishes the competence of the minister responsible for computerisation, whose functions are taken over by a court that supervises operators.

9. A company that was attacked by hackers decides to access the server of the alleged attacker in another state, to delete the stolen files and to identify the buyers. Which assessment is the most accurate from the point of view of criminal law and international law?

- A. The company acts lawfully, because every victim of a cyberattack has an unlimited right of retaliation against the attacker, wherever the attacker is located.
- B. The company may commit offences such as illegal access and data interference. Self-defence and necessity require strict conditions, and private countermeasures are not recognised in international law.
- C. The company acts lawfully if it hires an external firm to do the work, because the responsibility for the offences then passes to the contractor.
- D. The company acts lawfully, because international law allows private entities, like states, to take countermeasures against internationally wrongful acts.

10. Messaging applications differ in their use of end-to-end encryption and in the state in which the provider is established. A government wants to require the providers of encrypted messaging to build in a means of access for the authorities. Which statement best reflects the legal and policy debate on encryption?

- A. International law prohibits all strong encryption, and all states therefore require licences and keys for every cryptographic product used by individuals.
- B. The debate has been settled by a binding treaty that recognises a human right to encryption without any limitation and forbids states from requiring assistance.
- C. Encryption is relevant only to the technical standards of internet access providers, and it has no connection with human rights, jurisdiction or criminal procedure.
- D. Encryption protects the rights to privacy and expression, while states argue that it hinders investigations; the approaches vary from a general right to encryption to licensing and duties to assist the authorities.

Summary

This summary brings together the main points of Section 2.

1. **Jurisdiction.** Jurisdiction is the legal power of a state to regulate conduct, to decide disputes and to enforce its decisions. It is exercised primarily territorially, and extraterritorial jurisdiction is exercised under the authority of international law. Conflicts of jurisdiction require principles for their elimination.
2. **Principles.** The territorial, effects, personality, protective and universality principles link a state to an event. Prescriptive, adjudicative and enforcement jurisdiction correspond to the legislative, judicial and executive powers. Enforcement is in principle territorial.
3. **Cybercrime.** The Budapest Convention requires states to criminalise offences against the confidentiality, integrity and availability of data and systems, computer-related forgery and fraud, offences related to child sexual abuse material and copyright infringements, and to give authorities procedural powers. It provides for jurisdiction over offences on several grounds and for consultation in case of conflict.
4. **International cooperation.** Since evidence and suspects are abroad, cooperation is the condition for enforcing national criminal law. The tools include mutual legal assistance, extradition, preservation requests, contact points and cooperation of agencies. The Hanoi Convention extends this system on a universal basis, with a wider scope and a debate on safeguards.
5. **Cybersecurity.** The NIS 2 Directive requires essential and important entities to manage cyber risks and to report significant incidents in three steps: 24 hours, 72 hours and one month. Management bodies are accountable, and fines can be high. The Directive reaches providers outside the Union through the effects principle and the requirement of a representative.
6. **Polish law.** The Act on the national cybersecurity system sets the national framework, including three CSIRTs, and is being adapted to NIS 2. The Directive determines the result, and the national statute determines the form and methods.
7. **Active cyberdefence.** A victim of an attack has no general right to retaliate. Criminal law recognises self-defence and necessity only under strict conditions, and international law recognises countermeasures only by states.
8. **Data, surveillance and encryption.** Jurisdiction over data is difficult because data are mobile. State surveillance and spyware raise questions of legality, necessity and proportionality, and encryption and anonymity tools are at the centre of the debate between privacy and security.

The common message is that cybercrime and cybersecurity cannot be handled by one state alone. They require a combination of national statutes, European and international instruments, and cooperation. Understanding which state has jurisdiction, and which rule applies, is the first step in solving a legal problem.