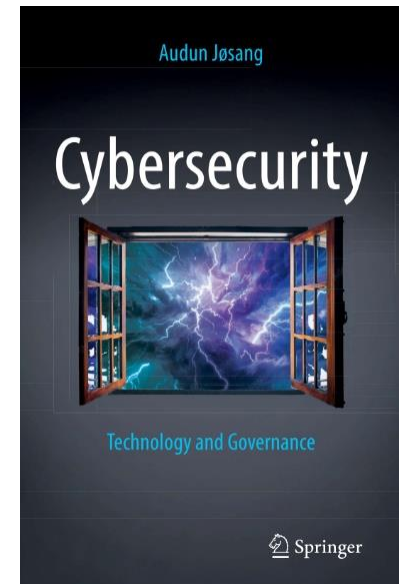


Chapter 17: Cyber Organizations and Regulation

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.



Overview



- a. Concepts of laws and regulations
- b. US cyber organizations and regulation
- c. EU cyber organizations and regulation
- d. Russian cyber organizations and regulation
- e. Chinese cyber organizations and regulation

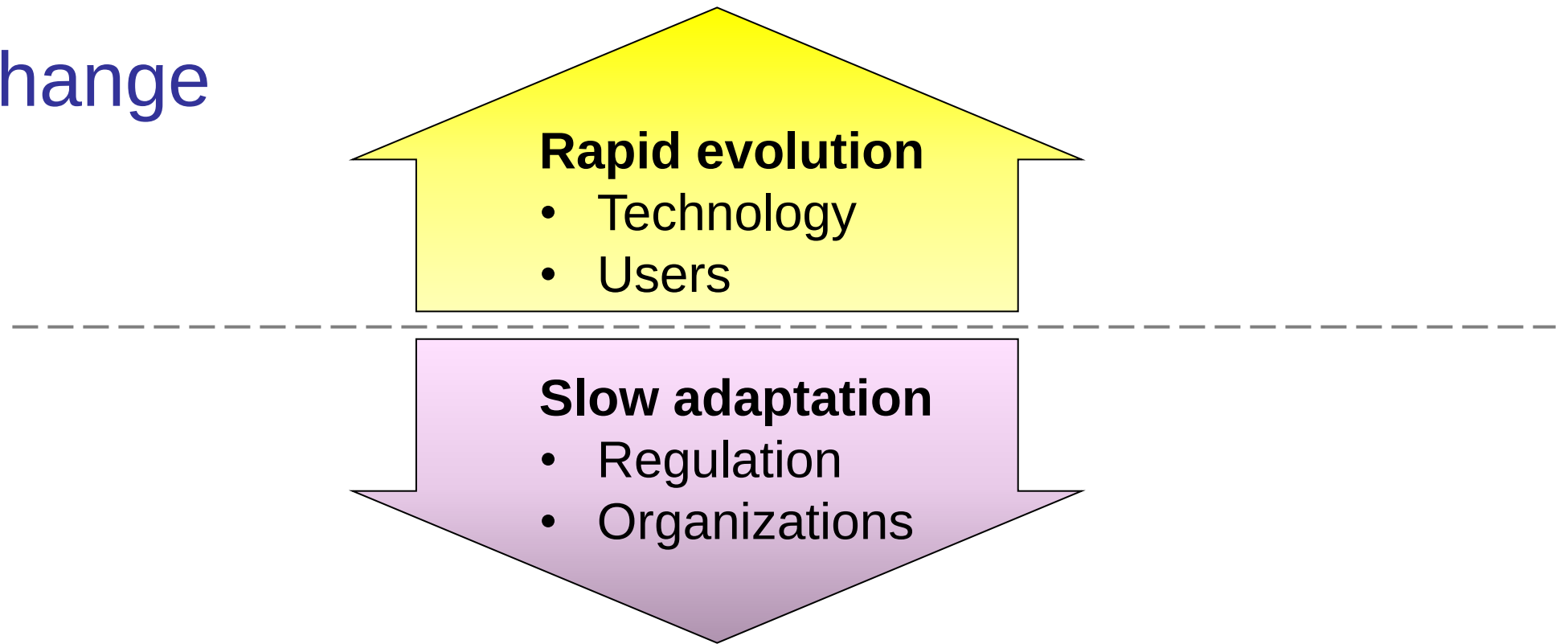
Legal Jurisdiction and Competence

- Jurisdiction, in law, is the authority of a court to hear cases and the ability to make a decision with binding effect on those affected by the cases.
- Another word for authority is competence
 - In legal terminology, competence is not used to describe competence, as we understand this word in everyday speech.
 - Legal competence refers to the legal “ability” of a court to exert jurisdiction over a person or a “thing” (property) that is the subject of a suit.

Responsibility and Accountability

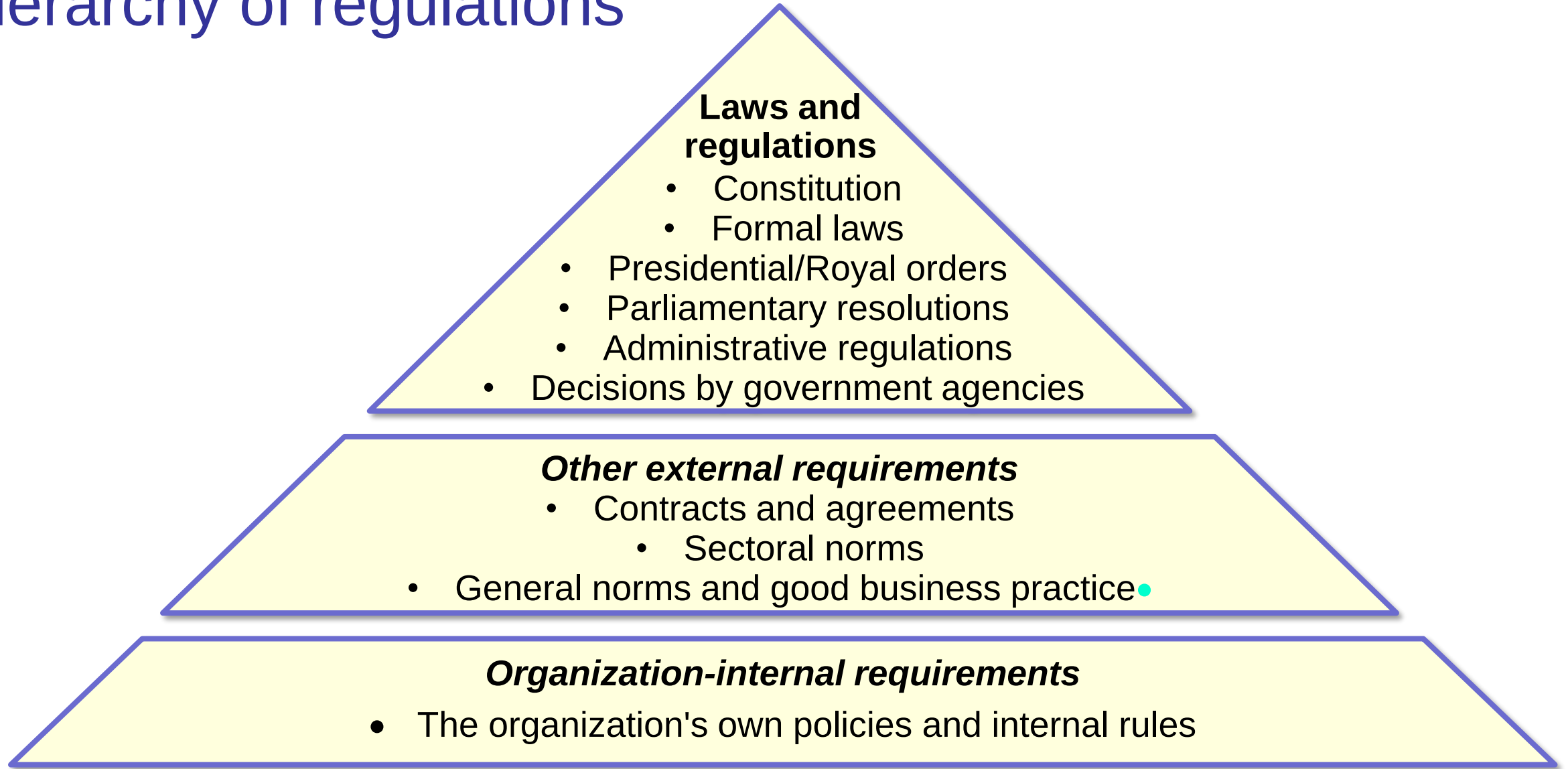
- Responsibility means to have specific tasks and duties (for compliance).
- Accountability means to be subject to questioning (about compliance), and to possible sanctions and penalty i.c.o. non-compliance.
- Top management and owners are generally accountable for ensuring that the operation of the business comply with regulations.
- In the event of non-compliance, the company can be fined, which is a company penalty. Alternatively, or in addition, individuals can be subject to fines or imprisonment, which is a personal punishment.
- An employee who clicks on a malicious link in a phishing email is not accountable, even if it causes a security breach with significant loss for the company.
- Although everyone in the company has responsibility for information security, the accountability always lies with the top management.

Pace of change



- It is desirable to have stable and long-term regulation, which means that we must try to create technology-neutral laws and regulations.
- However, deep technical insight and long foresight are often required to be able to create technology-neutral regulation.

Hierarchy of regulations



Compliance

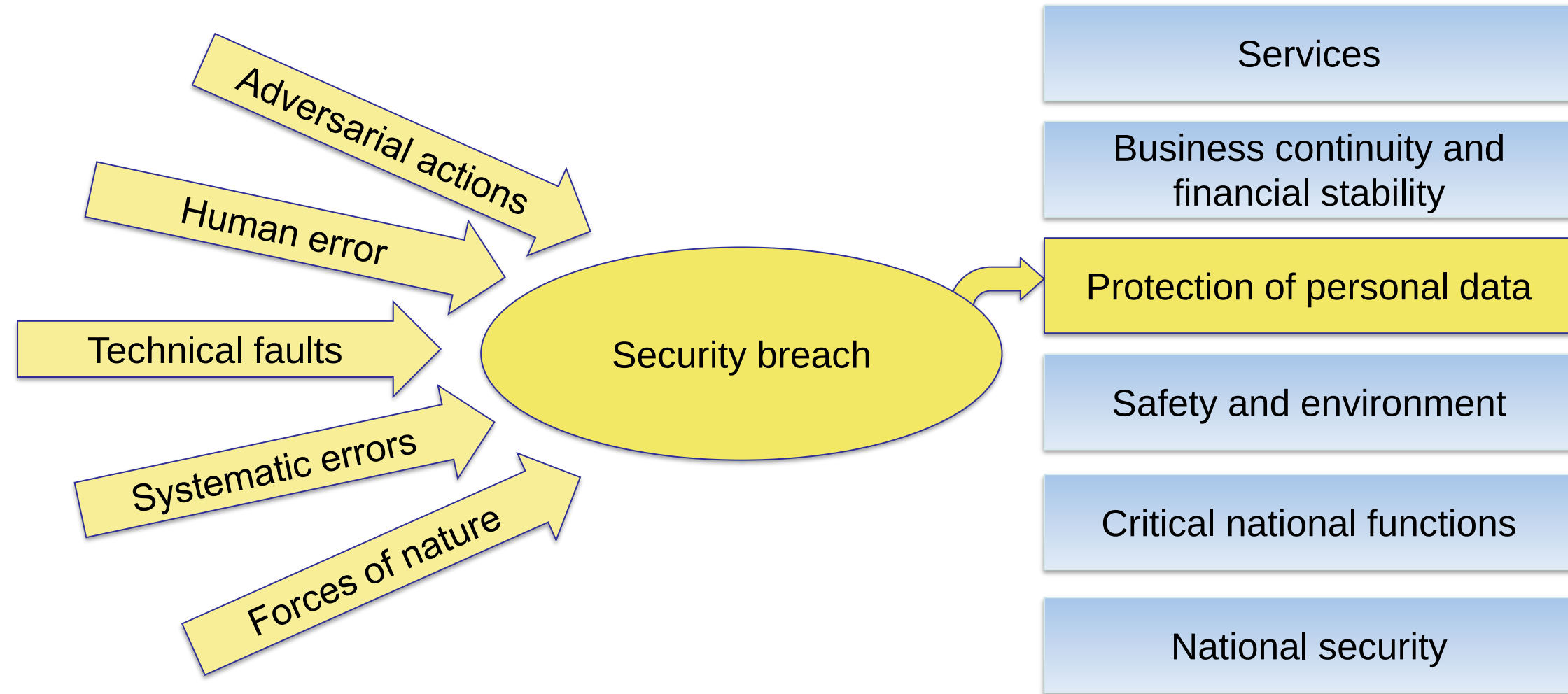
- Compliance with different types of regulations:
 - Laws and regulations
 - Decisions from the authorities
 - Contracts and agreements
 - Norms and good business practice
 - The company's own policy and internal rules
- The company's risk management usually includes a type of risk called compliance risk
 - There is a cost to ensuring compliance with various regulations
 - Failure to comply can e.g. result in penalties, fines, and sanctions that are considered a loss
 - The business must consider the cost of compliance against the risk of loss in the event of non-compliance

The purpose of the GDPR



- The EU GDPR (General Data Protection Regulation) provides provisions for the processing of personal data to take place without high risk to our "privacy rights and freedoms". (GDPR art. 35)
- “Data Protection” is EU jargon for privacy of personal information.
- The term "rights and freedoms" primarily means the rights described in GDPR Articles 12–22, but also rights enshrined in the UN’s Universal Declaration of Human Rights, and in the European Convention on Human Rights, which describe, among other things, the right to privacy, freedom of communication, freedom of expression, freedom of religion, the right to organize, and freedom from discrimination.
- The GDPR does not mention specific sources of threats against data protection; hence it covers all types of threats, i.e. “all hazards”.
- See Chapter 10 on information privacy.

Focus of the GDPR

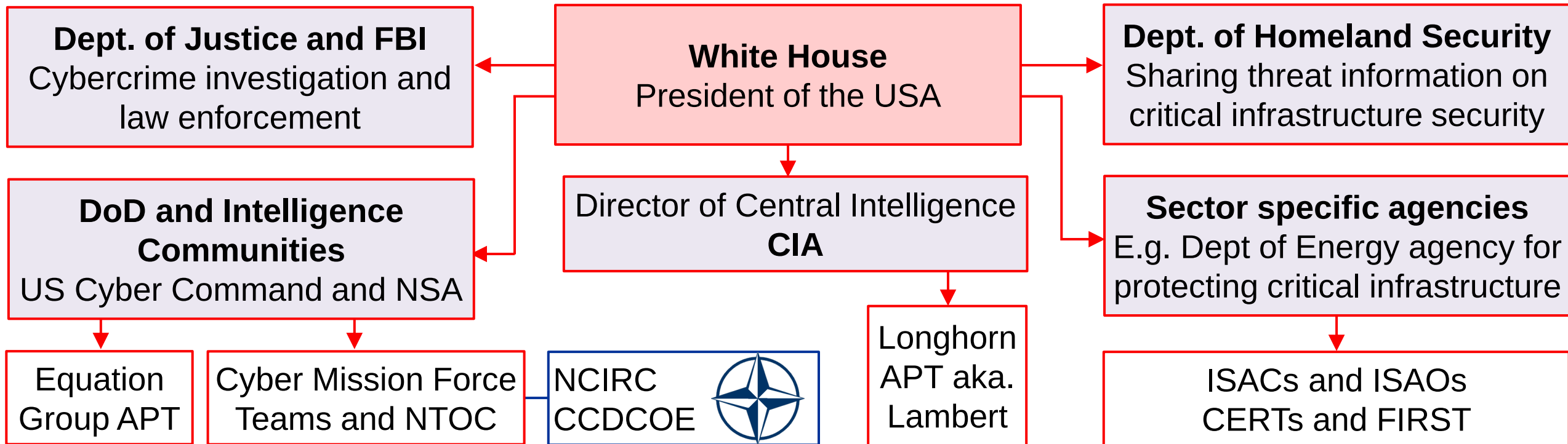


National regulations



- Countries have many national laws and regulations with provisions related to information security
- In addition, there are laws and regulations that regulate public administration, duty of confidentiality, right of access and similar matters that may affect information security.

Structure of cyber organizations in the United States



Computer Fraud and Abuse Act



CFAA (Computer Fraud and Abuse Act), 1986, is the primary federal law addressing cybercrimes and cyberhacking. Provisions cover

- **Unauthorized Access:** It is illegal to access a computer without authorization.
- **Obtaining National Security Information:** It is illegal to access a computer system to obtain national security information without authorization.
- **Computer Fraud:** It is illegal to defraud or to commit identity theft with a computer.
- **Unauthorized Damaging:** It is illegal to knowingly cause damage to a computer system without authorization. This includes the transmission of malware or viruses.
- **Trafficking in Passwords:** It is illegal to involve in trafficking of passwords or other access credentials that facilitate unauthorized access to computer systems.
- **Extortion Involving Computers:** It is illegal to use a computer to extort others. This covers ransomware attacks.
- **Conspiracy and Attempt:** The CFAA also criminalises conspiracy to commit offenses under the Act and attempts to violate its provisions, even if the actual offense is not completed

Federal Information Security Management Act



FISMA (Federal Information Security Management Act), 2002, prescribes a framework for improving the security of federal information systems: Objectives are:

- **Establishment and Use of Security Standards**
- **Risk Management Framework:** Agencies are required to adopt a riskmanagement..
- **Security Assessments and Authorization:** Agencies are required to conduct security assessments of their information systems, to evaluate security controls.
- **Continuous Monitoring:** Agencies are required to perform continuous monitoring of information systems to detect and respond to security threats in real-time.
- **Incident Response and Reporting:** Agencies are required to establish incident response capabilities to respond to security incidents promptly.
- **Annual Reporting Requirements:** Agencies are required to submit annual reports on their information security programs and compliance with FISMA requirements.

Cybersecurity Information Sharing Act



CISA (Cybersecurity Information Sharing Act), 2015, has provision for sharing CTI (Cyber Threat Intelligence) between the government and private sector entities in order to strengthen cybersecurity and incident response capabilities. Key provisions are:

- **Facilitation of Information Sharing:** CISA provides a basis for voluntary sharing of CTI, vulnerabilities and cybersecurity issues between the private sector and federal agencies. This includes liability protections for private sector entities for sharing CTI in good faith.
- **Privacy and Civil Liberties Protections:** CISA protects privacy and civil liberties by requiring the removal of personal information that is not directly related to a cybersecurity threat before sharing information with the government.
- **Use of Shared Information:** CISA gives federal agencies the right to use shared CTI for cybersecurity purposes as well as for investigating and prosecuting cybercrime.

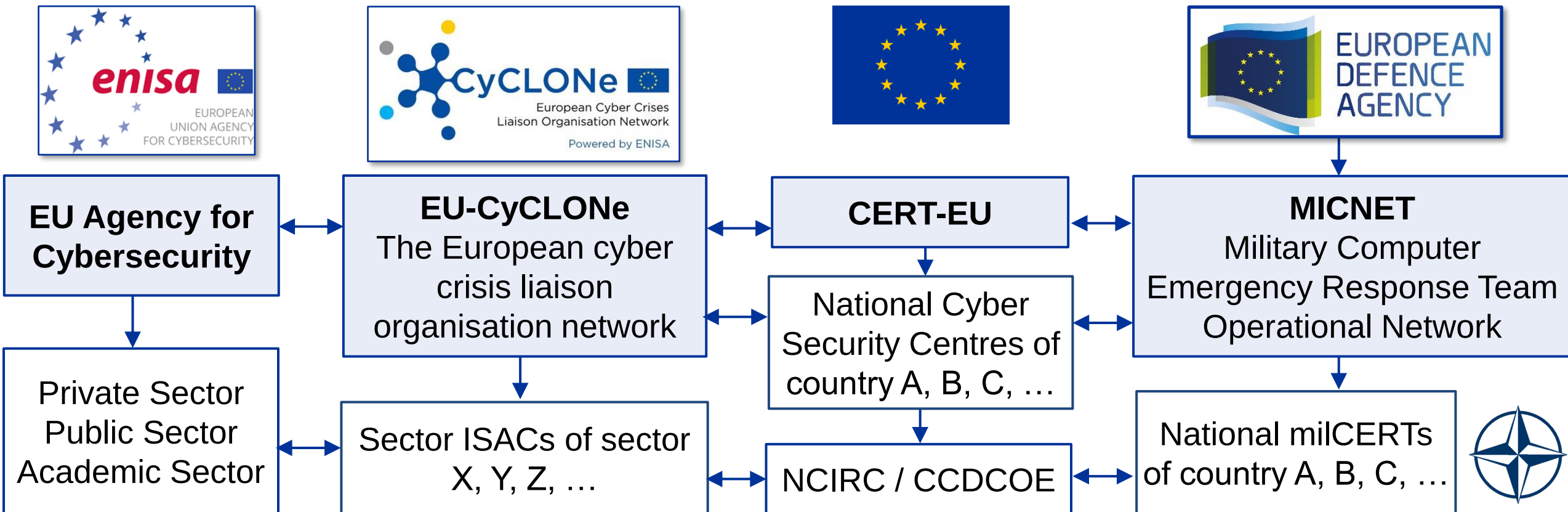
Health Insurance Portability and Accountability Act



HIPAA (Health Insurance Portability and Accountability Act), 1996, focuses on protecting the privacy and security of patients' health information. Indirectly this sets requirements for cybersecurity within the healthcare sector. Provisions are

- **Privacy Rule:** HIPAA mandates the safeguard of patients' “protected health information (PHI), thereby necessitating robust cybersecurity measures to safeguard electronic PHI (EPHI) from unauthorized access, disclosure, alteration, or destruction.
- **Security Rule:** HIPAA establishes national standards for safeguarding EPHI.
- **Data Breach Notification:** HIPAA requires health care entities to notify affected individuals, the Department of Health and Human Services (HHS), and sometimes the media in the event of a data breach of EPHI.
- **Penalties for Non-Compliance:** HIPAA violations can result in significant penalties, including fines, civil monetary penalties, and even criminal charges in cases of wilful neglect.

Structure of cyber organizations in the EU



EU Acts



- The EU has a comprehensive set of directives and regulations, collectively called “acts”.
- An EU directive must be implemented in national laws with approximately the same content as the directive.
- As a general rule, an EU regulation must be implemented as national law exactly as it is articulated by the European Commission, only translated into the national language.
- The EEA countries (Norway, Island and Lichtenstein) decide together whether an EU directive or an EU regulation shall apply in the EEA countries, which means that it will be incorporated into the EEA Agreement itself.
- For the EEA, the principle of all-or-none applies, i.e. an EEA country cannot decide alone whether or not to include an EU directive or an EU regulation.

NIS2 directive (Network and Information Security nr. 2)



- The NIS2 directive applies from 2023, and replaces the previous NIS directive from 2016. Elements of NIS2 include:
 - cooperation on a European cyber crisis management infrastructure through the EU-CyCLONe (European Cyber Crises Liaison Organisation Network)
 - harmonising safety requirements and reporting obligations
 - ensures that member states' cybersecurity strategies cover supply chain security, vulnerability management, core security and overall cybersecurity culture and cyber hygiene;
- The NIS2 directive takes into account “all hazards”, i.e. not only adversarial attacks, but also human error, system failure and natural disasters.

Other EU Cyber Acts (1)



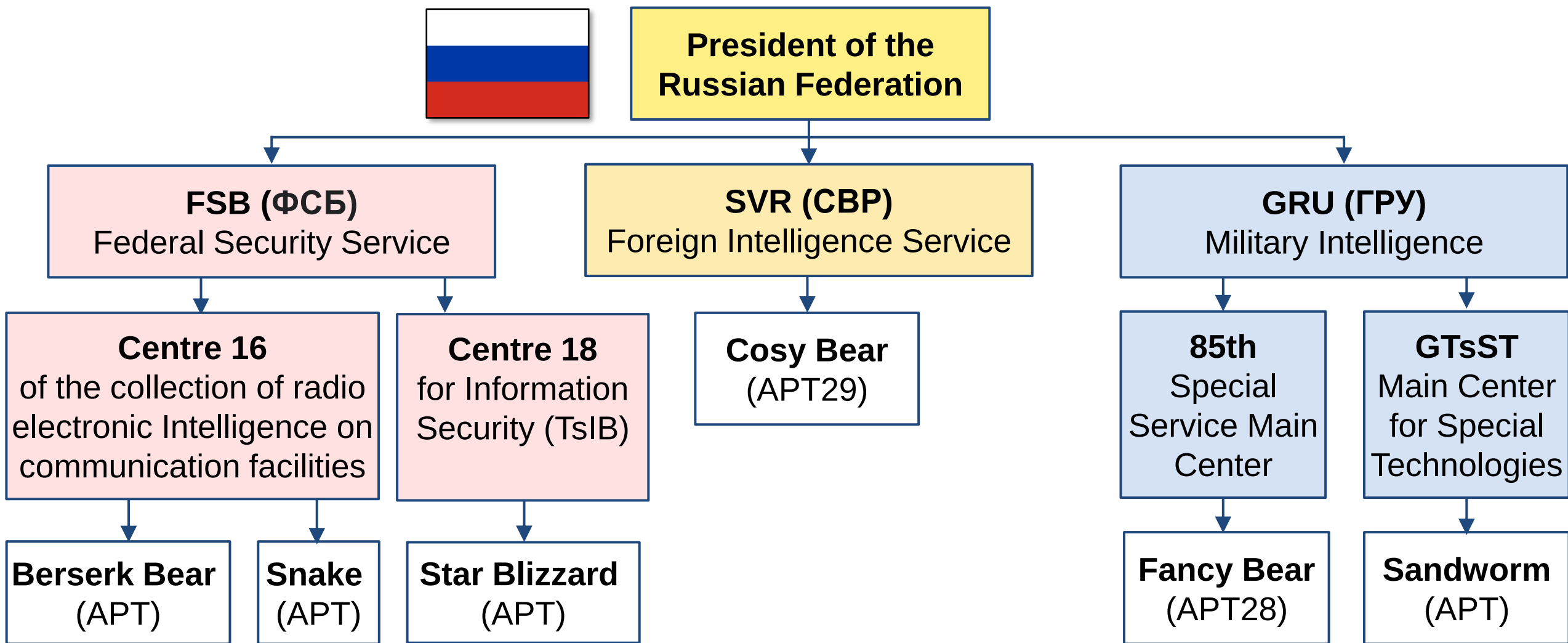
- GDPR (General Data Protection, Regulation), 2018 (see Chapter 10)
- eIDAS 2.0 Regulation (electronic IDentification And trust Services), 2024
- eIDAS is described in section 8.7.2.
- PSD2 (Payment Services Directive), 2019
 - PSD2 (Payment Services Directive No. 2) regulates payment services in the EU's internal market, and has been implemented in the Financial Institutions Act and the Payment Services Regulations, among other things. An important aspect is that the Directive allows bank customers to use players other than traditional banks to carry out financial operations
- Directive for the EU Electronic Communications Code, 2024
 - The directive aims to stimulate investment in and roll-out of secure high-speed networks throughout the EU, strengthen the internal market and strengthen consumer rights.

Other EU Cyber Acts (2)



- Cybersecurity Act, 2023 (regulation)
 - The pretentious name of this regulation is a misnomer. The regulation mainly concerns ENISA (European Union Agency for Cybersecurity), which through the regulation is given a permanent status with a specific mandate. ENISA was established in 2004 as the European Network and Information Security Agency, but had no permanent status and was dependent on annual budget allocation from the European Commission. The Cybersecurity Regulation gives ENISA permanent status, a strengthened budget, more staff and a strengthened mandate.
- Cyber Resilience Act (in progress)
 - The Cyber Resilience Act proposal focuses on setting security requirements for digital products, both hardware and software. Cyber resilience can be translated as cyber resilience, or anglicized as cyber resilience. This regulation can be linked to the certification of ICT products that are part of the Cybersecurity Regulation described above.

Structure of cyber organizations in Russia



Federal Law on Personal Data



Federal Law on Personal Data, 2006, last emended in 2023, is similar to GDPR.

- The law defines what constitutes personal data and special categories of personal data such as health data, union memberships and religious faith. The law defines legal bases for processing, rights of data subjects, and security requirements to protect personal data.
- Transfer of personal data outside of Russia is restricted, but not a complete ban. The Russian data protection authority (Roskomnadzor) can issue adequacy decisions for specific countries if their data protection laws offer equivalent protection to those in Russia.
- Data breaches must be notified to data subjects and to Roskomnadzor.
- Personal data must be deleted on data subject request or consent withdrawal.
- Fines from 10,000 roubles (ca. \$130) to 18 million roubles (ca. USD 230,000).

Criminal Code of the Russian Federation



The Criminal Code's Chapter 28, 1996, contains clauses related to computer crime, where the main articles are listed below.

- Article 272 penalises unauthorized access to computer information that is legally protected. Computer information means any message or data which is presented in electronic form.
- Article 273 penalises the creation, dissemination, and usage of harmful computer programs through a computer with malicious intent.
- Article 274 penalises the violation of the rules of operation of computers, computer systems, and networks.

Russian Sovereign Internet Act



The Sovereign Internet Law is a nickname for a set of 2019 amendments to the existing “Law on Communication” and “Law on Information, Information Technologies, and Information Protection.” The main amendments are:

- The compulsory installation of technical equipment at ISPs for inspecting and controlling Internet traffic.
- Centralized management of telecommunication networks and control mechanism for Internet traffic in and out of Russia.
- The implementation of a separate Russian national Domain Name System (DNS).

The amendments mandate Internet surveillance and grants the Russian government powers to isolate Russia from the rest of the Internet with a national fork of the Domain Name System.

The FSB (Federal Security Bureau) Act

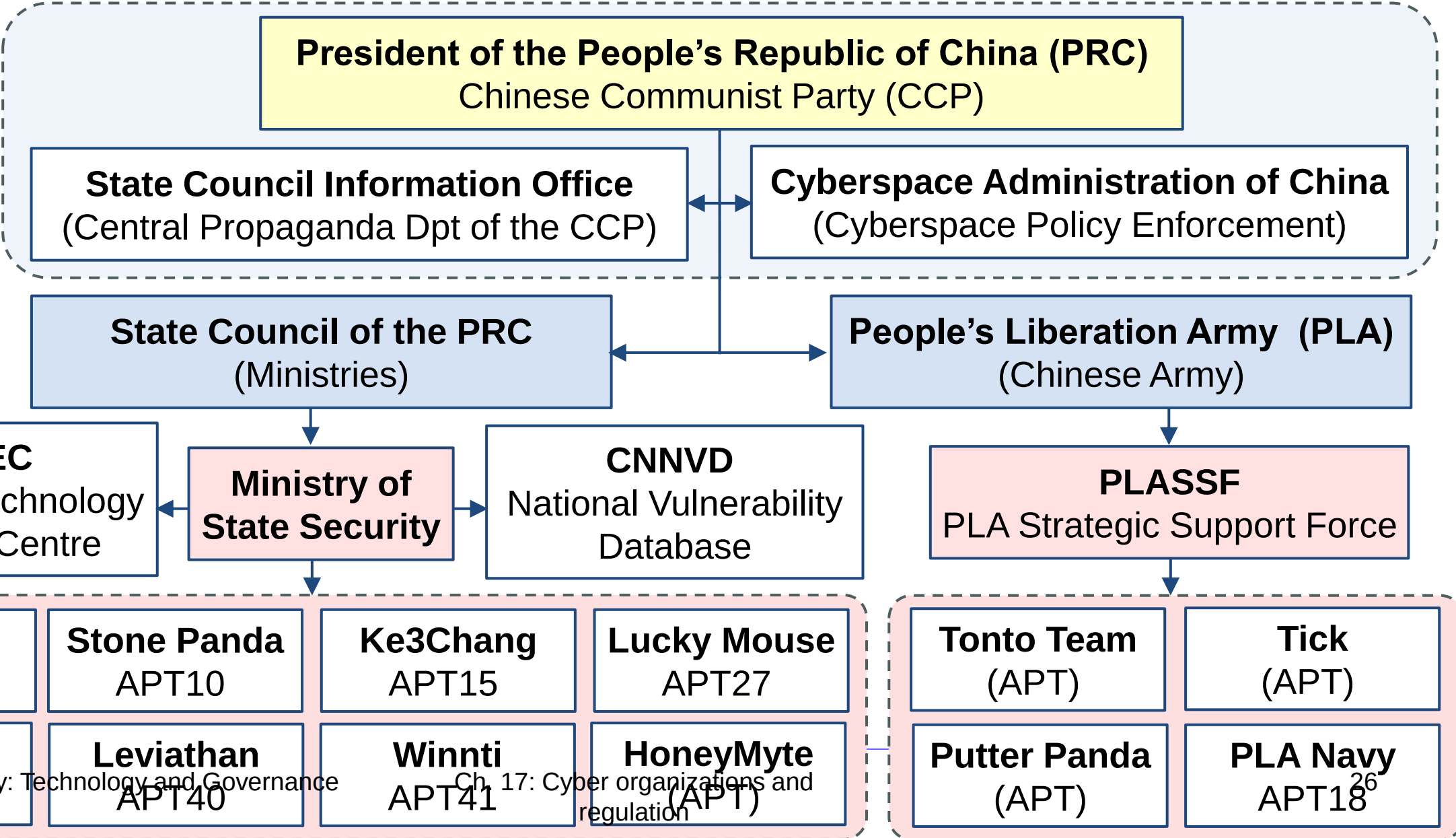


The FSB Act Article 11.2 establishes FSB as the authority in the information security field, including government encryption technology, and for enforcing restrictions on encryption in the private sector. Article 13 covers the FSB's general authorities.

According to Article 13, the FSB is entitled to:

- conduct cyberops to fight espionage, organized crime, corruption, illicit arms and drug smuggling and threats to Russia's national security;
- penetrate foreign intelligence services, criminal groups, and organizations;
- conducting espionage and other activities damaging Russia's security;
- ensure secrecy of cryptographic material in cryptographic entities in state bodies, enterprises, institutions and organizations irrespective of ownership;
- assist businesses, institutions and organizations irrespective of ownership in developing measures to protect trade secrets.

Structure of cyber organizations in China



The Cybersecurity Law (CSL) of China



The Cybersecurity Law, 2017, amended 2022, is the primary legislation governing cybersecurity. The main purpose of the law is to ensure state control over the Internet in China. The main provisions are:

- **Real-name requirements:** Anonymity online is not tolerated, meaning that every messaging service and social network in China must verify users' identity.
- **Data localization:** Article 31 requires that citizens' personal information must be stored within China borders. Some foreign tech companies such as Apple, were forced to store their user data in China which caused backlash from some users.
- **Prohibited content:** Communication and social network operators are required to censor content and remove any illegal material.
- **Technology “backdoors”:** Network operators can be requested to provide necessary technological support and assistance to law enforcement.
- **Critical information infrastructure sectors:** CII sector entities must implement additional checks and measures for establishing security safeguards.

The Data Security Law (DSL) of China



The Data Security Law (DSL) defines a data classification scheme based on the data's potential impact on Chinese national security, and regulates its storage and transfer depending on the data's classification level. The law can be seen as a response to the *U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, which gives U.S. law enforcement agencies the authority to compel companies falling under U.S. jurisdiction to produce requested data regardless of where the data is stored .

The Personal Information Protection Law (PIPL)



PIPL is similar to EU's GDPR in that it gives Chinese consumers the right to access, correct and delete their personal data gathered by businesses. Fines can be draconian.

- **Consent Requirements:** The legal basis for processing can be legal consent, or other reasons. This is similar to EU's GDPR Article 6.
- **Data Deletion Requirements:** Data handlers are required to delete the collected personal data when there is no longer a purpose.
- **Restrictions on Overseas Transfer:** For cross-border transfers, the foreign country must have data protection at least as stringent as that of PIPL.
- **General Compliance Requirements:** Personal data handler must assess their information security risks and implement necessary policies and controls.

Despite PIPL, government agencies in China perform widespread collection and processing of personal data as part of the Social Credit System (SCS) which is managed by the National Development and Reform Commission (NDRC). It must be assumed that NDRC has a legal basis for data collection and processing.

The National Intelligence Law



The National Intelligence Law, 2017, grants authorities broad powers to compel organizations and individuals to support and cooperate with intelligence work. This law has implications for cybersecurity regulation and data privacy. The resources that China dispose of are substantial and integrate human with technical components :

- **Global reach of Chinese companies:** Both the human and technical reach of Chinese companies now give the intelligence services opportunities to gain direct access to many governments within the developing world as well as many allied and European countries with which China maintains economic and cultural collaboration.
- **Everyone can be compelled to assist state security:** National intelligence institutions may, according to Article 14, “request relevant organs, organizations, and citizens to provide necessary support, assistance, and cooperation”.

These aspects are the reason for why most Western countries banned Huawei from delivering 5G networks. Hence, every branch of a Chinese company located in China or overseas must be considered as an instrument for Chinese state intelligence.

End of presentation