Key legislation on critical and digital infrastructure have been introduced to strengthen the EU's resilience against online and offline threats, from cyberattacks to crime, risks to public health or natural disasters.

The EU introduced a raft of cyber legislation recently, but only few of those initiatives have a direct impact on PGM industry. However, many might have indirect consequences for businesses.

Relevance for PGM industry

- It's clear that cyber threats are of high relevance for businesses. The top cyber threats in 2022 and beyond included ransomware, malware, social engineering threats, threats against data, threats against availability of services or the internet, disinformation/misinformation, and supply-chain attacks.
- Proper cyber hygiene and strong controls should be considered valuable, not only to protect the business but also because a cyber event could increase regulatory scrutiny and litigation.
- Hypothetical scenario: In the future, it might be possible that in the energy sector certain hydrogen production facilities might be considered a critical infrastructure, potentially meaning that also their supply chain would come into focus of cyber protection regulation.

The following information is intended to better understand and navigate the EU Cyber Security regulation landscape. .

Overall Strategy

The European Commission presented a new EU Cybersecurity Strategy at the end of 2020. The strategy covers the security of essential services such as hospitals, energy grids and railways. It also covers the security of the ever-increasing number of connected objects in homes, offices and factories. It
The strategy focuses on building collective capabilities to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace.

Key EU legislation

Legislation came into force to bolster cybersecurity requirements to protect critical and digital infrastructure for applicable entities in member states, such as

- NIS2,
- the Resilience of Critical Entities (CER),
- the Digital Operational Resilience Act (DORA), and
- (not yet implemented in EU members states, end of transition period in 2024) EU Cyber Resilience Act (CRA).

NIS2 Directive on measures for a high common level of cybersecurity across the Union

- Cybersecurity threats are almost always cross-border, and a cyberattack on the critical facilities of one country can affect the EU as a whole. The Directive applies not only to critical infrastructure operators, but to organisations of all types and sizes. These include providers of public electronic communications networks and services, data centre services, wastewater and waste management, manufacturing of critical products, postal and courier services and public administration entities, as well as the healthcare sector more broadly.

- The Directive on security of network and information systems (NIS Directive), which all countries have now implemented, ensures the creation and cooperation of such government bodies. This Directive was reviewed at the end of 2020. As a result of the review process, the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) was presented by the Commission in December 2020.
- The NIS2 Directive entered into force on 16 January 2023. Member states will have **21 months** from the entry into force of the directive in which to incorporate the provisions into their national law (actual date: 18 October 2024).

- The NIS2 Directive is intended to complement the Cyber Resilience Act (CRA) and significantly expands the sectors and type of critical entities falling under its scope.
- The Cyber Resilience Act (CRA) and the Resilience of Critical Entities Directive (CER) are both EU regulations aimed at improving cybersecurity and resilience. However, they have different scopes and target different entities.

Cyber Resilience Act (CRA)

- The CRA is a regulation that applies to all digital products that are placed on the EU market. This includes products such as smartphones, laptops, smart home devices, and industrial control systems.
- The CRA requires these products to meet certain cybersecurity standards, such as having strong passwords and being regularly updated with security patches.
- The CRA is yet not implemented, but EU Parliament cleared the way for the trilogue process on 19 July 2023. Parliament proposes modified definitions, deadlines and distribution of responsibilities. Products are classified into different lists. These are based on their criticality and the level of cybersecurity risk they pose. Products such as identity management system software, password managers, biometric readers, smart home assistants, smart watches and personal security cameras are also to fall under the CRA. Security updates are to be installed automatically and separately from function updates.

Resilience of Critical Entities Directive (CER)

- The CER is a directive that applies to critical entities, which are organizations that provide essential services to society, such as energy,

water, transport, and financial services. The new CER Directive replaces the European Critical Infrastructure Directive of 2008.
  - The CER requires critical entities to assess their cybersecurity risks and put in place appropriate measures to mitigate those risks, including natural hazards, terrorist attacks, insider threats, or sabotage.
  - This legislation was influenced by the sabotage act against the Nord Stream pipeline.
- Until October 2024, EU Member States must transpose the requirements of the CER Directive into national law.

Digital Operational Resilience Act (DORA)

- The Digital Operational Resilience Act (Regulation (EU) 2022/2554) solves an important problem in the EU financial regulation. Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience. After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.
- This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.
- As the Digital Operational Resilience Act (DORA) is a Regulation, not a Directive, it is binding in its entirety and directly applicable in all EU Member States.
- DORA Regulation will apply from 17 January 2025.

What else is there…

In February 2023 a new **European Center against disinformation** was presented which is not directly relevant for PGM industry – but interesting from wider business perspective (***see article further below***).

ENISA (European Union Agency for Cybersecurity)

ENISA is the EU agency that deals with cybersecurity. It provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

In April 2023, the Commission proposed a targeted amendment to the EU Cybersecurity Act, which gave ENISA a permanent mandate, and empowered it to contribute to stepping up both operational cooperation and crisis management across the EU. It also has more financial and human resources than before.

Also in April 2023, the EU Commission unveiled a new legislative package aimed at stepping up the EU's fight against cyberattacks, building on the EU Cybersecurity Strategy.

- The cyber package includes the **EU Cyber Solidarity Act**, to improve the response to cyber threats across the EU, and a **Cybersecurity Skills Academy**. The EU Academy is intended to bundle private and public initiatives that improve cybersecurity skills at European and national levels.
- The Commission proposes the establishment of a **European Cybersecurity Shield**. This will create a Europe-wide infrastructure of **Security Operations Centers** (SOCs). These SOCs will detect and defend against cyber threats, using cutting-edge technology such as AI and advanced data analytics. In doing so, they will enable government agencies to respond more efficiently and effectively to major cyber incidents**.** These centers could be operational as early as 2024.

--- --- --- --- --- --- --- --- --- ---

Not directly relevant for PGM industry – but interesting from wider business perspective is the new European center against disinformation presented in February 2023.

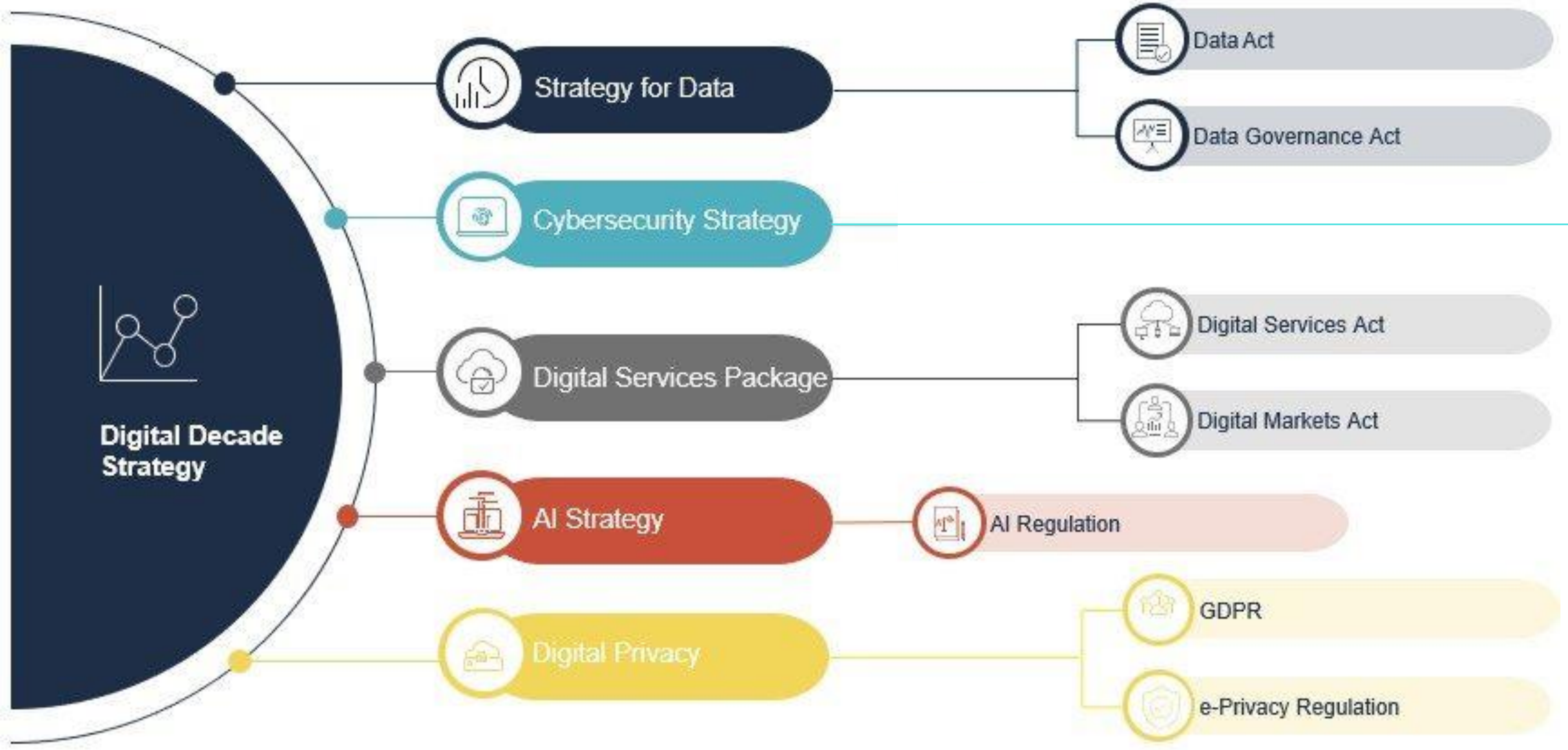
EU creates new center against disinformation *(by Table.Media, February 2023)*

The EU wants to counter Chinese and Russian disinformation campaigns more effectively with a new platform. A newly created "Information Sharing and Analysis Centre" within the Diplomatic Service of the European Union (EEAS) will track disinformation from outside the EU and also coordinate with the 27 member states and civil society actors, EU chief diplomat Josep Borrell announced in February 2023. "Authoritarian regimes try to create misinformation and manipulate it," Borrell warned. The idea is to create **a decentralized platform for sharing information in real-time with countries, cybersecurity authorities, and NGOs**. In this way, already existing disinformation campaigns should be better investigated and understood. It should also be able to respond more quickly to emerging narratives. Further details on the size and staffing of the center were not initially disclosed. Beyond the platform, **Borrell also announced plans to add disinformation experts to EU delegations abroad**.

China also active in the Western Balkans

Over the past year, the People's Republic has mostly engaged in information manipulation in connection with the Ukraine war, according to a first report on the issue by the EU's existing disinformation unit, the Stratcom department of the EEAS. The circulated narratives had mainly focused on supporting the Russian invasion, it said. "A majority of Ukraine-related reports in international channels of Chinese **state-controlled media have been based on official Russian sources**," the Stratcom report explains.

For the report, the Stratcom unit studied around 100 cases of information manipulation in greater detail. The report shows that the **disinformation is predominantly image- and video-based, multilingual, and spread via a dense network of actors**. On Twitter, the channels of diplomatic representatives from China and Russia are particularly involved. Apart from the war narrative, **China is also very focused on its own reputation**. "China's parallel aim is to suppress competing, and potentially critical stories about itself, also by using intimidation and harassment", the report says. For example, it would attempt to influence reports on human rights issues. **China is also particularly active in the Western Balkans**.



- Security of Network and Information Systems Directive “NIS 2“
- Cyber Resilience Act (CRA)
- Resilience of Critical Entities Directive (CER)
- Digital Operational Resilience Act (DORA)
- ENISA (EU Agency for Cybersecurity)
- Cyber Solidarity Act (incl. European cyber protection shield)
- Information Sharing and Analysis Centre within the Diplomatic Service of the European Union (EEAS)

EU Cyber Legislation Has Expanded in Scope

Year	Legislation	
May-16	NIS Directive	Sectors covered include healthcare, transport, banking and financial market infrastructure, digital infrastructure, water supply, energy and digital service providers.
Mar-19	EU Cyber Security Act	EU framework of cybersecurity certification of products, services and processes, and reinforced the mandate of the EU Agency for Cybersecurity (ENISA).
Sept-22	Cyber Resilience Act Proposal	Commission adopts proposal for cybersecurity requirements for digital hardware/software products.
Nov-22	Digital Operational Resilience Act Adoption	DORA regulation establishes uniform requirements for the security of network and information systems supporting the business processes of financial entities. This includes information and communication technology (ICT) risk-management; reporting of major incidents and voluntary notification of significant cyber-threats; digital operational resilience testing; and rules for the oversight framework for critical ICT third-party service providers.
Jan-23	NIS2 Replaces NIS Directive	Expanded sectors to providers of public electronic communications networks or services, digital services, social networking platforms and data center services, waste water and waste management, manufacturing of critical products, space, postal and courier services, and public administration, food, expanded scope of healthcare sector.
Jan-23	CER Directive	Resilience of Critical Entities strengthens resilience of critical infrastructure against cyber risk related to natural hazards, terrorist attacks, insider threats, or sabotage applies to 11 sectors deemed critical: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space and food.
Oct-24	NIS2, CER Directives	Compliance deadline
Jan-25	DORA	DORA regulation applies

Source: Fitch Ratings, European Commission, European Council of the EU.