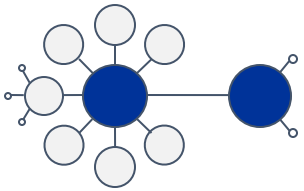
EUROPEAN CENTRAL BANK

EUROSYSTEM



CIISI-EU

Cyber Information and Intelligence Sharing Initiative (CIISI-EU)

FIGI Cyber Resilience

(online, 15 June 2021)

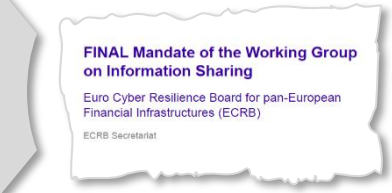
Problem Statement

1. **Cyberattacks continue** to be a major threat to financial services. Attacks are sophisticated, well-funded and coordinated

2. Currently, MIs are at **different levels of maturity** in terms of usage of intelligence

3. Currently, MI's are **fragmented** using different services, technologies, products and intelligence data sources

4. Currently, MI's **do not systematically share** intelligence between themselves



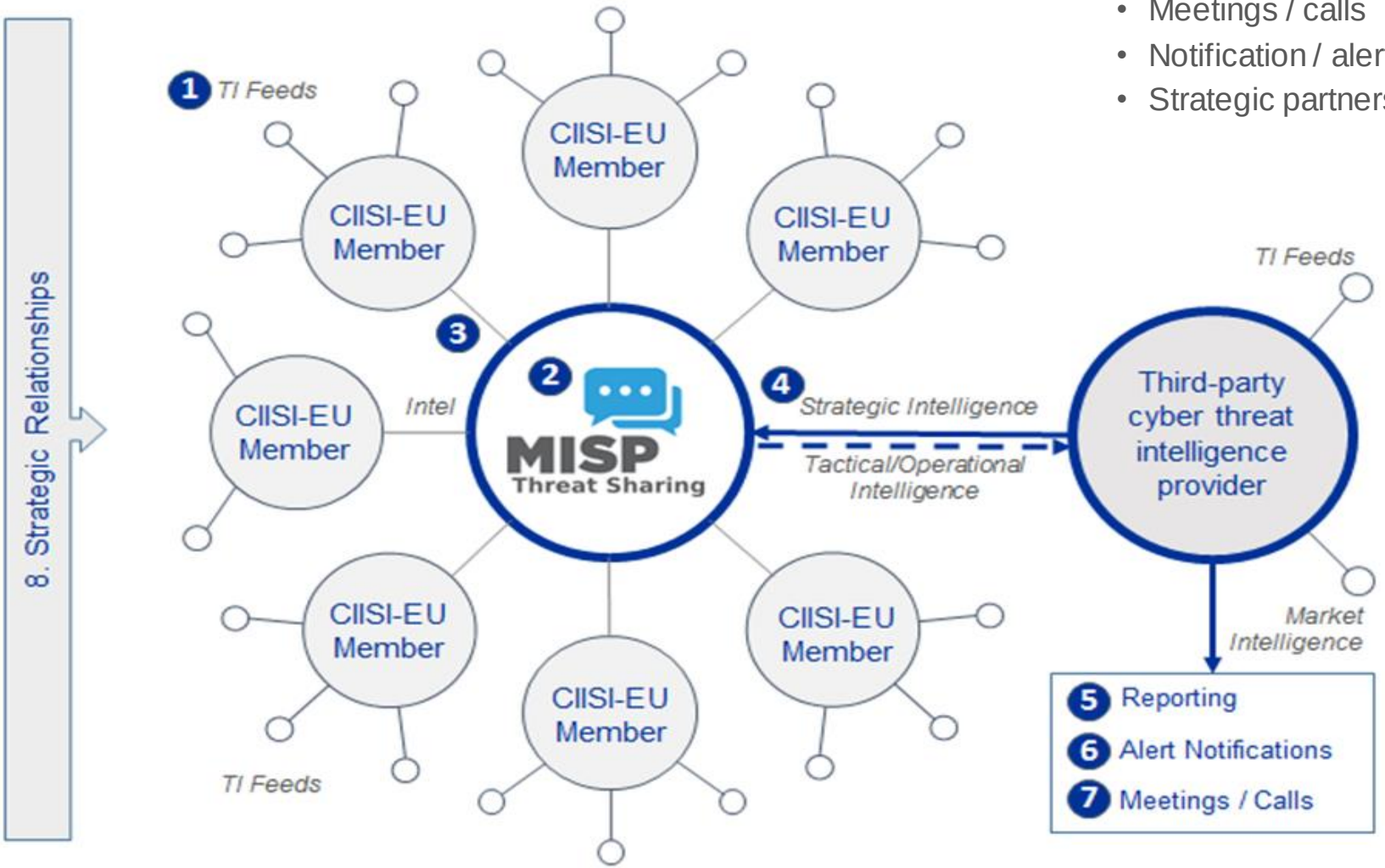
A unified approach for cybersecurity intelligence sharing across major European infrastructures, given their criticality, is needed

Who decided to join the CIISI-EU intelligence sharing initiative?

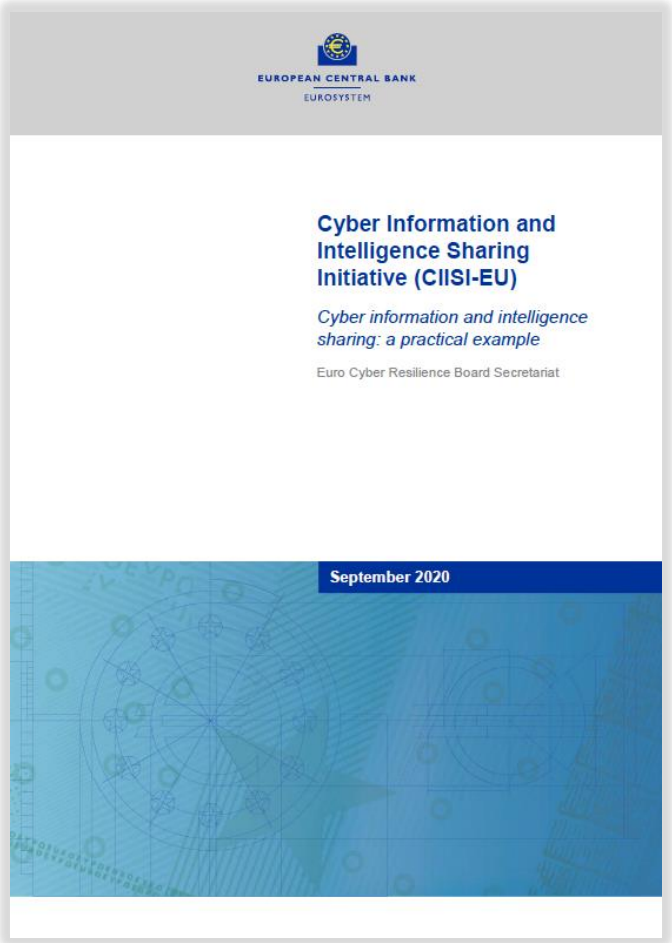
EU market infrastructures, central banks, settlement system operators, payment service providers, network providers, intelligence agencies, law enforcement …

Topology

- Threat intel feeds
- Shared platform
- Third-party analyst
- Meetings / calls
- Notification / alerts
- Strategic partners



CIISI-EU – Building block for you…..


EUROPEAN CENTRAL BANK
EUROSYSTEM

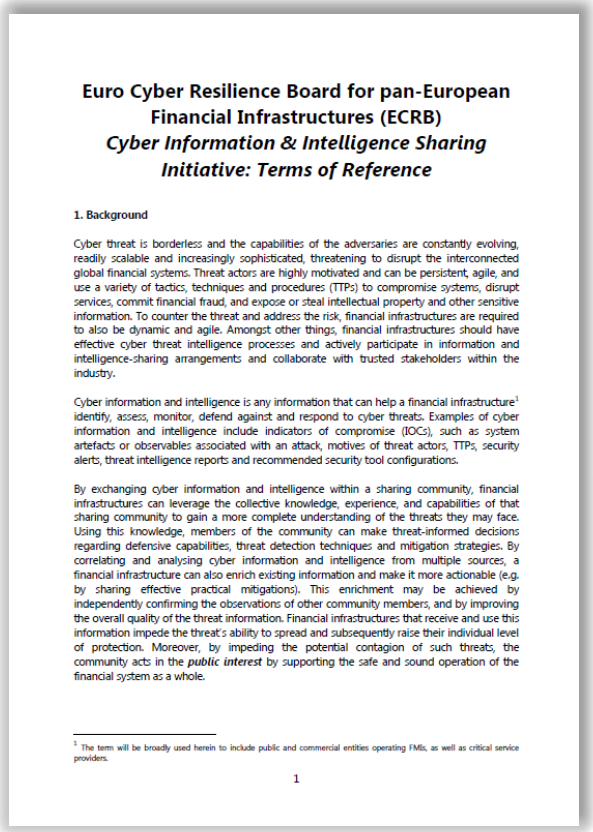
Cyber Information and Intelligence Sharing Initiative (CIISI-EU)

Cyber information and intelligence sharing: a practical example

Euro Cyber Resilience Board Secretariat

September 2020

Look at ECB's ECRB webpage for these docs and more information www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html


Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)
Cyber Information & Intelligence Sharing Initiative: Terms of Reference

1. Background

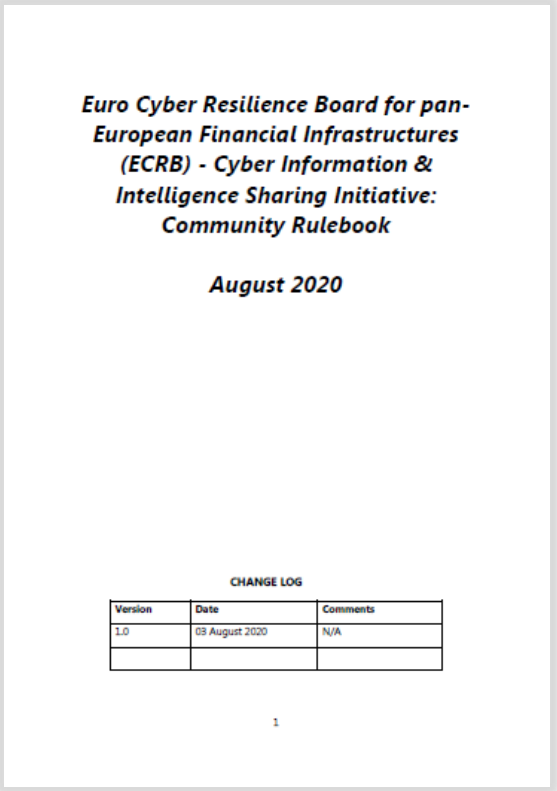
Cyber threat is borderless and the capabilities of the adversaries are constantly evolving, readily scalable and increasingly sophisticated, threatening to disrupt the interconnected global financial systems. Threat actors are highly motivated and can be persistent, agile, and use a variety of tactics, techniques and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. To counter the threat and address the risk, financial infrastructures are required to also be dynamic and agile. Amongst other things, financial infrastructures should have effective cyber threat intelligence processes and actively participate in information and intelligence-sharing arrangements and collaborate with trusted stakeholders within the industry.

Cyber information and intelligence is any information that can help a financial infrastructure[1] identify, assess, monitor, defend against and respond to cyber threats. Examples of cyber information and intelligence include indicators of compromise (IOCs), such as system artefacts or observables associated with an attack, motives of threat actors, TTPs, security alerts, threat intelligence reports and recommended security tool configurations.

By exchanging cyber information and intelligence within a sharing community, financial infrastructures can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-informed decisions regarding defensive capabilities, threat detection techniques and mitigation strategies. By correlating and analysing cyber information and intelligence from multiple sources, a financial infrastructure can also enrich existing information and make it more actionable (e.g. by sharing effective practical mitigations). This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information. Financial infrastructures that receive and use this information impede the threat's ability to spread and subsequently raise their individual level of protection. Moreover, by impeding the potential contagion of such threats, the community acts in the ***public interest*** by supporting the safe and sound operation of the financial system as a whole.

[1] The term will be broadly used herein to include public and commercial entities operating FMIs, as well as critical service providers.

1


Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) - Cyber Information & Intelligence Sharing Initiative: Community Rulebook

August 2020

CHANGE LOG

Version	Date	Comments
1.0	03 August 2020	N/A

1