EU2019.FI

9 September 2019

Informal ECOFIN, 13-14 September 2019

Resilience of financial market infrastructure and the role of the financial sector in countering hybrid threats

- Presidency Issues Note for the Informal ECOFIN Working Session Ia -

- The Strategic Agenda for 2019-2024 adopted by the European Council in June calls for a comprehensive approach to protecting Europe from malicious cyber activities and hybrid threats. Discussion at the informal ECOFIN working session is intended to raise awareness about the role of the financial sector in countering hybrid threats and to provide political impetus for follow-up. The Presidency will prepare a summary letter of the discussions.

Introduction

- The financial sector provides critical services to our societies. Financial transactions are the lifeblood of the economy. Without access to finance, ownership data and the possibility of making payments, all economic activity would quickly grind to a halt. The repercussions for other essential services such as logistics networks, food supplies and continuity of government would be severe. Even short interruptions can cause not only major economic losses, but social disturbances too.
- Unlike other critical infrastructures such as energy or telecommunications grids, financial services are not tied to any specific location. Technological and regulatory developments have created the possibility for highly integrated cross-border infrastructure networks to come into being, whereby core activities of financial service providers may be processed across Europe or even worldwide. These developments have created efficiencies, reduced costs and enhanced competition. At the same time, they have made financial markets, and consequently societies, highly dependent on the continuity of cross-border communications. While the rise of cross-border financial activity has been matched by a substantial integration of European financial regulation and supervision, there is far less cooperation on continuity arrangements, and responsibility for national security aspects remains with the Member States.
- The European Union's security environment has changed dramatically in recent years. Threats come in new, often less easily detectable forms. They

include hybrid threats, a mixture of coercive and multidimensional activity and conventional and unconventional methods that can be of a diplomatic, military, economic or technological nature. State or non-state actors engaging in hybrid action can use various methods in a coordinated manner to achieve specific objectives, for example causing economic damage or destabilising societies, while remaining below the threshold of formally declared warfare. Hybrid action usually seeks to exploit the vulnerabilities of the target and generate ambiguity in order to hinder decision-making processes.

- Hybrid activity can include cyber-attacks, spreading disinformation and exerting a malicious influence on critical infrastructure. There are various potential targets for such activity, but the financial sector — which is highly dependent on public trust and digital infrastructure continuity, and where the impact of disruption on society at large can be very substantial — is clearly among the most attractive.

A European response to hybrid threats

- Since 2016 the EU has introduced a broad array of counter-measures, in a substantial number of policy areas, relating to hybrid threats. The 2016 Communication 'Joint Framework on Countering Hybrid Threats – a European Union response' identified 22 actions ranging from improving information fusion and situational awareness, to protecting critical infrastructure, cybersecurity, building resilient societies and stepping up cooperation with the North Atlantic Treaty Organisation.
- The 2016 Joint Framework identifies well-functioning financial and payment systems as one of the critical areas where action should be taken to strengthen resilience. The Communication states that to deal with hybrid threats against EU financial services, the industry needs to understand the threat, to have tested its defences and to have the necessary technology to protect the industry from attacks.
- In recognition of the evolving nature of the threat and following the call made by the March 2018 European Council, the Commission and the High Representative adopted a Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats in June 2018. This reinforced the focus on strategic communications and situational awareness, chemical, biological, radiological and nuclear threats, resilience and cybersecurity as well as counter intelligence.
- In the area of financial services, implementation of the Joint Framework and the 2018 Joint Communication has been referred to the Commission 2018 FinTech Action Plan. The Commission identified several areas and aspects where stronger cyber resilience and enhanced ICT security of financial market participants across the Union would contribute to strengthening the stability of the EU's highly integrated financial sector.

- Building on the Joint Advice published in April 2019 by the three European Supervisory Authorities in the financial sector (the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority), the Commission is reflecting on ways of addressing the current fragmentation in relation to the scope, granularity and specificity of cyber security-related provisions across the Union's financial services legislation.
- To support measures for the prevention of cyber threats, in June 2018 the Commission organised a public-private workshop aimed at assessing the existence and extent of any possible regulatory or non-regulatory barrier preventing threat-intelligence sharing. The discussions did not point to clear barriers preventing the flow of threat-related information among financial market participants although further clarification has been sought by the stakeholders.
- Various steps have been taken by EU institutions to enhance cyber security in the financial sector. Banking and financial markets infrastructure have been included in the framework of the NIS (Network Information Security) Directive. This Directive provides a legal basis for cooperation between national competent authorities, CSIRTs, and ENISA. The ECB has established the Euro Cyber Resilience Board for pan-European Financial Infrastructures, which includes the Commission, EUROPOL, EBA, ESMA and ENISA.

Challenges

- Awareness of cyber risks within the financial sector is generally high though somewhat uneven across market segments or Member States. Financial institutions and authorities have already made considerable efforts to enhance cybersecurity, in particular in the area of financial market infrastructures and payment systems and services. Nevertheless, pockets of vulnerability may remain. For example, it is not clear if the efforts to strengthen cybersecurity have effectively addressed broader risk scenarios, where cyber-attacks are used to deliberately take down significant parts of the financial system as part of a broader campaign to exert political influence on the EU and its Member States. From the commercial and business continuity viewpoint, such events are often considered as a tail risk, triggering force majeure conditions and thus being seen as tolerable. Authorities, for their part, might not prepare adequately to react to such crisis.
- Addressing financial sector resilience is part of society-wide resilience challenge. Modern society is characterised by a web of complex interdependencies, and the financial sector sits at the heart of that web. Financial services depend on the continuity of other parts of critical infrastructures such as telecommunications and energy. Such interlinkages go both ways, and major disruptions in any of these sectors will have serious repercussions in others.

- Harmonisation of financial supervision and regulation is well advanced. However, its purpose has been to establish a well-functioning internal market for financial services with a focus on prudential regulation, market integrity, conduct and consumer and investor protection. Considerations of continuity, resilience and national security have not been central to this work. While in many Member States core financial services have been designated as critical functions and financial infrastructure is considered part of national arrangements on critical infrastructure protection, such a designation has not been made at EU level. As a result of this, the financial sector has not been included, for example, within the scope of the Directive 2008/114 on European Critical Infrastructure. Developing preparedness and managing major incidents requires cross-sector cooperation between the relevant authorities. Discrepancies in definitions of critical infrastructure may lead to a lack of cooperation and information sharing.
- The European Commission has evaluated the 2008 Directive on critical infrastructure protection. The evaluation shows an evolution in the threats facing Europe. The evaluation also emphasizes that the EU's approach to critical infrastructure protection must be flexible and risk-based so as to reflect the threats and vulnerabilities that critical infrastructures are likely to face in the decades to come[1]. The evaluation suggested that there are additional sectors that the Member States consider worthy of additional protective action at European level[2]. Based on the evaluation's findings there are grounds for examining the scope of the EU's critical infrastructure policy framework with a view to encompassing additional sectors.
- In this context, it would be worthwhile considering a broadening of the definition of critical infrastructure to cover digital infrastructure and supply chains, including areas such as banking and finance, food and health care services. However, there are concerns that the designation of financial services as critical infrastructure might lead Member States to increasingly declare financial regulation a matter of national security, thus undermining internal market objectives. While this is a relevant concern, given the critical role of the financial sector and the changes in Europe's security environment, it would seem necessary to find ways of addressing critical security issues in the EU's financial services policy while at the same time safeguarding the integrity of the internal market for finance. An approach reconciling security and internal market objectives is therefore needed.

[1] Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (Commission Staff Working Document, SWD(2019) 308 final).
[2] It should be further noted that the EU Network Information Security (NIS) Directive (Directive 2016/1148) covers activities such as banking and financial infrastructure, health, information and communications technology (ICT) and the drinking water supply.

Questions for discussion

- Do you agree that it is necessary to enhance cross-sectoral cooperation to ensure that hybrid threats are taken into account in financial sector regulation and supervisory action?
- Should financial services be considered part of the Union's critical infrastructure?
- To what extent should the resilience and continuity of financial services in all parts of the EU be seen as a joint responsibility of the Union?
- Do you agree that adequate resilience arrangements for financial services can be implemented while respecting the integrity of the single market?
- Is the Union appropriately prepared to respond — involving all critical sectors — in the event of a major disruption in financial services?

Further reading

- Joint Framework on countering hybrid threats - a European Union response, Joint Communication to the European Parliament and the Council, 6.4.2016
- Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, Joint Communication to the European Parliament and the Council, 13.6.2018
- Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, Joint Staff Working Document, 28.5.2019
- Protecting Europe - The EU's response to hybrid threats, European Union Institute for Security Studies (EUISS), Chaillot Paper 151, April 2019