Cybersecurity in Finance:
Getting the policy mix right!

19 September 2017 | Place du Congres 1, 1000-Brussels

1. OVERVIEW

Hundreds of thousands of computers in over 150 countries were infected in May 2017 by what was reported to have been the WannaCry ransomware cyber-attack. According to Europol, this attack was unprecedented in scale and affected many large organisations in different sectors, notably car and telecoms industries, and health and education systems. No financial organisation has confirmed to have been affected, but the financial sector is not immune to such large-scale attacks in the future. This single event is a timely reminder of the need to develop an open, safe and secure cyberspace for financial services, as underlined in the Cybersecurity Strategy of the European Union.[1]

Beyond the risk of large-scale attacks that disrupt digital infrastructure, cybersecurity is essentially an everyday phenomenon. This threat is especially difficult to manage because it is constantly evolving, as cybercriminals find new ways to attack, breach and exploit organisations. All financial providers are exposed to such risks, in particular those that grow through acquisitions and need to absorb legacy IT infrastructures. Furthermore, as they are currently undergoing profound digital transformation, financial providers are adjusting their processes and integrating new types of technologies. The learning process inherent to this transformation poses significant challenges to cybersecurity as well.

While EU and national policymakers are gradually creating the necessary conditions to tackle cybersecurity risk in financial services, numerous policy issues remain unresolved. In order to address cybersecurity, the EU has focused on three main objectives in recent years: increasing cybersecurity capabilities and cooperation across organisations and countries; making the EU a stronger player in cybersecurity; and mainstreaming cybersecurity in EU policies.[2] At the core of the EU's digital strategy

[1] The text of the Cybersecurity of the European Union can be found here: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

[2] See the publication of the European Commission on EU cybersecurity initiatives (2017): http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

is the Directive on Network and Information Security (NIS). Adopted in July 2016 and expected to be implemented by May 2018, it covers banking and financial market infrastructures. Several other recent pieces of legislation include specific rules to cope with rising cybersecurity risks for financial services: the Payment Service Directive II (PSD2), the Anti-Money Laundering Directive (AMLD), the General Data Protection Regulation (GDPR), etc. Such diversity in the rules addressing cybersecurity risk require a clear analysis of the interplay between the relevant regulations to improve the consistency of the whole regulatory framework and to discern what types of new rules might be needed.

Between September 2016 and January 2017, CEPS-ECRI conducted a first successful Task Force on specific FinTech issues for retail financial issues.[3] The ensuing action plan was keenly endorsed and presented to different organisations such as the Financial Services Committee (FSC) of the Council of the EU, the European Commission DG FISMA, the European Banking Industry (EBIC), etc. As a follow-up to this first round, CEPS-ECRI will organise a second Task Force that will focus on the policy issues primarily related to cybersecurity in the market of financial services. A preliminary survey was submitted to members of CEPS, ECRI and ECMI to start defining the scope of this Task Force. The results of that survey revealed six priorities:

1. Cooperation, coordination and consistency in cybersecurity: the objective is to draw up recommendations for how and to what extent coordination and cooperation can be improved across companies and countries, how capacities in cybersecurity can be reinforced and how the robustness of the regulatory framework for cybersecurity can be enhanced (especially by analysing the interplay between the GDPR, PSD2 and the NIS Directive);

2. EU labelling scheme for ICT security products: the objective is to draw up recommendations for how and to what extent a harmonised EU ICT security certification framework can be developed, and how and to what extent this certification can contribute to the development of a single market for financial services;

3. Data breaches: the objective is to formulate recommendations for the determination of a risk threshold beyond which the financial provider has to notify consumers of breaches;

4. Regulation of clouds: the objective is to draw up recommendations for how to better harmonise rules, standards and guidelines for clouds, and for the need or not to remove prescriptive regulations on data location (GDPR, Art. 30) within the EU and with third countries;

5. Digital authentication: the objective is to recommend how and to what extent policies can contribute to the development of a balanced digital authentication system that strikes the right balance between security and convenience for consumers.

6. Regulation of blockchain: the objective is to recommend the types of policies needed to stimulate the development of the blockchain technology and the rules needed to alleviate specific risks related to blockchain;

[3] The report of the Task Force on FinTech can be found here: https://www.ceps.eu/system/files/TFRFutureFinancialServices.pdf.

2. ORGANISATION

A kick-off meeting of the Task Force will be held on 19 September on "Achieving cybersecurity in financial services – what policy mix?". Selected individuals will be invited to this meeting, to provide ample opportunity for exchange with the moderator and the speakers. As described below, the agenda will comprise three presentations, followed by interactive discussions with the participants. Mr Pearse O'Donohue from the European Commission, DG CONNECT, will present the latest developments in the European Commission's work on cybersecurity (TBC). Mr Jeremy Borot, Associate Partner at McKinsey, will present the key trends in cybersecurity in financial services (TBC). Finally, Mr René Van Dee from ThreatMetrix will focus on global digital identity intelligence and how it contributes to reduce fraud (TBC).

During the kick-off meeting, the Task Force will agree a priority list of issues to be discussed. CEPS will bring in its own expertise on digital economy, cybersecurity, data protection and financial regulation; other external experts will be invited to kick off the debate. The final scope of the financial products to be covered will be defined at this meeting.

This CEPS-ECRI Task Force will meet three times before February (in addition to the kick-off meeting). The first meeting will identify and conceptualise the key characteristics and challenges related to the development of an adequate level of cybersecurity for financial services. During this meeting, the first elements of an action plan for European policies will be discussed. A second meeting will complete the key findings of the discussion held during the first meeting. Finally, another meeting will finalise the action plan, based on a broad consensus among Task Force Members.

At the end of the Task Force, CEPS-ECRI will publish and circulate among EU and member state policy circles an authoritative analysis, with policy recommendations, together with a Task Force Report. This will be officially published as a CEPS Task Force Report and distributed internationally. The report will be based on discussions in the meetings, supplemented by research carried out by the rapporteur.

This ECRI Task Force is principally designed for ECRI members but participation will also be open to non-members, for a fee:[4]
-ECRI Member: free
-CEPS Member: 1,500 euros (excl. tax)
-ECMI Member: 1,500 euros (excl. tax)
-Corporate that is not ECRI Member, ECMI or CEPS Member: 5,000 euros (excl. tax)

[4] The fee covers participation in all workshops, documentation, lunches and three copies of the final report; upon request, CEPS will mail additional copies of the final report to persons identified by participants.

3. AGENDA FOR THE FIRST MEETING

12:30	Registration & Lunch
13:00	Opening & Welcome **Karel Lannoo**, *CEO, CEPS*
13:05	Opening remarks by the Chairman of the Task Force **Filip De Wolf**, Partner, PwC
13:20	Latest developments in the work of the European Commission on Free Flow of Data and Cloud Security **Pierre Chastanet**, Deputy Head of Cloud and Software, European Commission, DG CONNECT
13:50	Main challenges of providers of products related to cybersecurity **Jan Neutze**, Director of Cybersecurity Policy, Microsoft
14:20	Main challenges of financial organisations for cybersecurity issues **Erik Van Zuuren**, Founder, TrustCore.eu
14:50	Blockchain, KYC and cybersecurity **Simon Wilkinson**, Operating Director at Tradle
15:20	Discussion on the structure of the Task Force
16:00	End of the Meeting