SPEECH

Building a solid cyber defence for the new geopolitical season

Introductory remarks by Piero Cipollone, Member of the Executive Board of the ECB, at the tenth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Frankfurt am Main, 21 November 2024

As any good sports coach will tell you, you need to deploy different defensive tactics against different teams. As an example, let me talk about a couple of different opponents you may face in the world of football.

You may have to play a team that uses the high-press approach – or gegenpressing – as popularised by Jürgen Klopp's Borussia Dortmund. This team aggressively chases after your defenders, hoping to force a mistake and win the ball off you as quickly as possible. Or you could play against a more counter-attacking team such as José Mourinho's Inter Milan. They will patiently sit back and let you play and, when the moment is right, use their quick forwards to surprise you with a break-away goal.

I will argue that what we face today in the world of cyber security is similar to the challenges faced by football managers as they prepare their defence for the season to come. In both cases, the different tactics of the opposing teams' attack will require different defensive strategies.

Facing cyber threats in a new geopolitical and technological environment

So, with this analogy in mind, let me start by outlining what threats we are facing in the current geopolitical environment. I will focus on two key trends: geopolitics and technology.

Geopolitics

It is a long-held truism that geopolitical tension drives cyber activity. As competing nation states seek to advance their interests and disrupt their adversaries, more intense cyberattacks take place. But this is not just a truism, it is also backed up by hard data – and these data reveal that we are not moving in the right direction.

At the aggregate level, recent empirical analysis by the IMF[1] confirms that countries facing heightened geopolitical tensions have a relatively greater likelihood of experiencing a cyberattack. And here in Europe our exposure to such tensions has increased significantly. For evidence of this, look no further than the geopolitical risk index of the euro area, which is now at a historically very heightened level[2], as my colleague Claudia Buch recently highlighted.[3]

This picture is also reflected in recent European cyber threat assessment reports, which provide evidence on the activities of new state-related threat actors.

For example, the latest ENISA Threat Landscape report[4] highlights a significant increase in the number of cyber events that have occurred in the EU over the past year, with the financial sector being the third-most targeted segment. The report attributes the increase in large part to the various geopolitical tensions that the EU is currently facing.

Multiple analyses – including from French[5] and US authorities – provide details on the increasing number of observed attacks whose aim seems to be espionage. These are often undertaken by state-backed actors and are becoming more sophisticated in their use of stealthy techniques.[6]

Technology

The second key driver of the threat landscape relates to technology. Various technological changes are ongoing, and each tends to expose more potential targets to cyber attackers.

The number of online devices we use is growing and so is the amount of time we are spending on them. In addition, as I emphasised in my remarks at the last ECRB meeting[7], infrastructure operators are increasing their reliance on outsourcing and other types of third-party service provision. Together, these trends multiply the number of potential cyberattack targets and increase the amount of time per day that those targets are available.

So, we face an apparent proliferation of sophisticated and deep-pocketed state-sponsored threat actors launching complex cyberattacks. And at the same time, there are more and more potential targets available to them.

It is therefore difficult to escape the conclusion that the overall threat outlook is deteriorating. In other words, our team will have its work cut out to defend our goal this season.

Policy and oversight in support of strong cyber defence

Thankfully, infrastructure operators do not have to face these challenges alone. Let me share my thoughts on how policy and oversight can support operators in firming up their defences.

The recently updated Eurosystem cyber resilience strategy sets out the three pillars of this support: entity readiness, sector resilience and regulator-industry engagement.[8]

Overseers work with entities to enhance their individual cyber readiness and assess their cyber maturity in an objective way using the Eurosystem's cyber resilience oversight expectations and the TIBER-EU framework for red-team testing. We will continue to strengthen these efforts to firm up entity readiness over time.

Given the highly interconnected nature of financial market infrastructures, sound risk management requires a strong emphasis on sector-wide resilience. Overseers have various tools to assess cyber risk and supply-chain risk at the sectoral level. This includes the Eurosystem's critical service provider survey, which is based on a self-assessment by the entities. This enables overseers to accurately map the sector, identifying the critical nodes and interdependencies within the European financial ecosystem.

To come back to my footballing analogy, if someone on the European financial infrastructures team concedes a goal in the cyber "game", we are all in danger of losing. It is therefore important to test the

match fitness of our defences from a collective perspective. In this context, the updated cyber strategy introduces industry-wide scenario-based testing exercises to assess sectoral preparedness. Exercises will simulate an extreme but plausible cyberattack to test how prepared the sector is to respond to attacks, including in terms of the time needed to resume services.

Most relevant for today's event, the ECRB helps to stimulate a healthy level of strategic engagement between regulators and the industry. In an environment where the attackers we face and the techniques they use are quickly shifting, this forum provides leaders with a valuable opportunity to exchange ideas on how best to tackle emerging challenges.

This dialogue is vital to address our shared challenges. I look forward to making further progress together in key areas, such as sustainably building up the labour force in cyber security.

Like in football, the market for talent is highly competitive. According to a recent IMF report[9], there is a global shortage of approximately four million cybersecurity professionals. In this context, it feels like we are all chasing the same scarce talent to boost our cyber defences.

But unlike competing football clubs, our incentives are more aligned. There is greater scope for collaborative solutions to nurture cyber talent, and I would welcome creative ideas on how to achieve this.

Investing in cyber security at entity level to support long-term success

Notwithstanding this collective dimension to cyber security, let me also emphasise that the ultimate responsibility for ensuring an institution's cyber resilience lies with the institution itself.

Unfortunately, in today's geopolitical and technological environment the overall cyber threat level is steadily increasing. Entities face a growing number of deep-pocketed state cyber actors and must protect an attack surface that is broadening due to technological trends.

In this context, entities may find that maintaining robust cyber defences will require even more time and effort. Committing more resources to defence may create tensions within organisations, as this may divert them from other endeavours. However, in the end, achieving high cyber resilience is a core part of the product offering of financial market infrastructures. So investing sufficiently to achieve a high level of cyber resilience is necessary for long-term success.

In addition, the geopolitical environment is tilting the threat landscape further towards state actors. For some time now, these players have been responsible for the most serious cyber threats, and this is likely to continue.

Our defensive tactics must consider this reality. Rather than preparing for traditional criminally motivated cyberattacks seeking ransoms, we must be nimble in devising ways to detect attackers that take a more patient, underhand and counter-attacking approach.

Conclusion

To conclude, let me say that the challenges we face in organising our cyber defences are clearly greater than those faced in the world of football.

After all, football managers only need to organise their defence to face one team at a time, and once the 90 minutes are over, there is time to rest and recover. By contrast, in the cyber environment we need to defend against all cyber actors at the same time, all day every day. In other words, our defence must play against the attackers of all our opponents at the same time – and the referee will never blow for full-time.

But we do have some things on our side. Unlike in football management, we have much more scope to collaborate. This allows us to strengthen our defences both at the individual and the collective level. So, with that in mind, I look forward to open discussions today and to sharing knowledge and ideas on how we can further boost our defensive capabilities.

Thank you.

1.

International Monetary Fund (2024), "Rising Cyber Threats Pose Serious Concerns for Financial Stability", *IMF Blog*, 9 April.

2.

Geopolitical tensions are captured by the geopolitical risk index (see Caldara, D. and Iacoviello, M. (2022), "Measuring Geopolitical Risk," *American Economic Review*, April, Vol. 112, No 4, pp.1194-1225), which consists of a measure of adverse geopolitical events and risks based on a tally of newspaper articles.

3.

Buch, C. (2024), "Global rifts and financial shifts: supervising banks in an era of geopolitical instability", speech at the eighth European Systemic Risk Board (ESRB) annual conference on "New Frontiers in Macroprudential Policy", 26 September.

4.

ENISA (2024), *ENISA Threat Landscape 2024*, 19 September.

5.

French National Cyber Security Agency (2023), *Cyber Threat Overview*.

6.

Such stealthy techniques can include "living off the land", which allows attackers to avoid detection by blending in with normal built-in Windows system and network activities. See CISA (2023), *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, 24 May.

7.

Cipollone, P. (2024), "One step ahead: protecting the cyber resilience of financial infrastructures", speech at the ninth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, 17 January.

8.

Cyber resilience and financial market infrastructures.

9.

World Economic Forum (2024), “Global financial stability at risk due to cyber threats, IMF warns. Here's what to know”, *Centre for Cybersecurity*, 15 May.

CONTACT