G7 2019 Conference – Banque de France, 10 May 2019

Cybersecurity: Coordinating efforts to protect the financial sector in the global economy

Conclusion by François Villeroy de Galhau

Governor, Banque de France

Press contact: Mark Deen (mark.deen@banque-france.fr).

Ladies and Gentlemen,

First, I would like to thank the moderators and the panelists for their very rich comments and the very useful ideas. We are all convinced that cybersecurity of the financial sector will remain on our agenda for a long time. The challenge is no longer about gaining awareness anymore, but to find ways to intensify and rationalise our action.

Based on the discussions today, let me start with one pre-requisite – coordination - and then propose concrete steps and tangible actions to improve our coordination in three areas: I. Regulation and supervision; II. Information; III. Preparation.

A. Global threats, coordinated action

Panel 1 questioned the importance of cyber threats for the financial sector. There is a consensus that the level of cyber threats has never been so high, but at the same time, we must acknowledge that the capacity to anticipate attacks needs to be reinforced. Following an attack, we need to address the potential contagion issues to the entire financial system or the entire economy. This is why coordination is a pre-requisite, not an easy one but a necessary one. While remaining realistic, there will not be a “world organization for cybersecurity” for obvious reasons, including trust. Hence, **coordination should be cross-jurisdictional.** Contagion can be global as our countries' financial systems are interconnected. This follows President Macron's call for an "Internet of Trust" at the UNESCO Forum in November 2018, which includes helping low-income countries to keep pace with developed countries. The IMF and the World Bank are encouraged to further develop their assistance program. In addition, **coordination should be cross-sectors**. The financial sector is not the only one concerned with cyber-attacks. Other critical sectors are also at risk, some of which are essential to the functioning of the financial sector. This reinforces the importance of a cross-sectoral approach. National security agencies use this approach, and financial sector authorities

could also do the same at their level, taking into consideration the forthcoming G7 CEG Fundamental elements.

Finally coordination should be cross-authorities, with national security agencies. As discussed in Panel 1, those agencies have the role to protect the countries' critical economic sectors, including the financial sector, against cyber-attacks. Financial authorities have the role to supervise the financial sector's capacity to manage its risks, including cyber risks. Both authorities have a mutual interest in coordination.

B. Three concrete areas to improve our coordination

I. Regulation and supervision

I would like to start with the issue of regulation, which was addressed by panel 2. One difficulty with regulation is about reaching a balanced situation. Regulation is needed, irrespective of the level of institutions' awareness and self-discipline… But, too much regulation may lead to a decrease in self-discipline and turn institutions' effort into a compliance exercise.

Since 2015, cybersecurity issues attract an increasing level of attention, and regulators have produced a large number of regulatory texts, both at national and international levels. This was called for to trigger the appropriate response and efforts from the industry. It helped the sector to reinforce its safeguards. Nevertheless, we must ask ourselves whether the multiplication of new regulations can have a counterproductive effect. From the panelists' interventions, two issues need to be addressed:

- First, we should **avoid the possible proliferation of texts** by standard-setters for banking, payments, securities services, insurance and/or financial markets. The FSB has already provided such evidence in a stock-taking exercise performed in 2017. Regulators are paying attention to cyber risks, and while they share the same objectives, regulatory texts tend to differ across regulators and as a result add to firms' burden in terms of compliance with these various regulations, with

little marginal gain. Clarity would be enhanced by reducing the multiple variations in the formulation of requirements across institutions. In turn, regulators' efforts would be streamlined and their experts employed more effectively.

How can we better coordinate regulation? Obviously, a "principle-based" regulation on cybersecurity is preferable, rather than increasingly prescriptive standards, too rigidly "rules-based". Supervision completes regulation. Principle-based regulation would give supervisors some room for manoeuvre to modulate their expectations to the risk profile of the institutions.

- But then, we should also pay attention to the **risk of regulatory arbitrage**. Regulatory differences can create opportunities. If not all regulations are aligned, some private actors could (re)locate their IT systems in less-demanding jurisdictions. This is the reason why we need homogeneity among international regulatory texts with the largest outreach.

Who could lead this coordination role on cybersecurity regulation? The G7 expert group has been extremely successful in producing "Fundamental elements", but this group has no standard-setting role and its texts can only guide regulators in their work. I believe the FSB is best placed to engage the dialogue with the various standard-setters to foster the alignment of their texts, as well as to conduct global outreach, and limit the proliferation of working groups.

II. Information

Cyber threats are increasing, but adequate and consistent measurement is challenging. I would like therefore to make two proposals:

About incident reporting. Many reporting obligations on cyber incidents have emerged, requested by various authorities. But these incident reports give little

information to measure the intensity and sophistication of threats and their evolution. The indicators requested vary from one report to another and this limits the scope of diagnosis and comparisons. The institutions themselves can struggle to transmit information about their incidents in different formats and with different details to the various authorities in charge. FSB agreed on a "cyber lexicon". [1] As we have done in the past for operational risk, I recommend that we work on a common categorization of cyber incidents to better measure the impacts of attacks, and better understand their evolution.

About information sharing and threat intelligence. As evidenced by panel 4, little information on cybersecurity is actually shared, due to sensitivity issues and trust. A pragmatic approach is for financial authorities to engage bilaterally in Memoranda of Understanding (MOUs) with authorities with whom they share mutual trust. Singapore and Hong-Kong already paved the way. This can be done between G7 countries and among other trusted countries as well.

III. Preparation for cyber crisis management through large scale exercises

The third panel showed how valuable crisis simulations are in the building of an operational preparatory capacity. The exercises organized so far, at domestic or regional levels, allowed us to acquire experience in coordinating a response and the recovery during a major incident. Our ambition must be as high as the risks to which our evolving and interconnected financial systems are exposed to, due to the increasing sophistication of cyber-attacks. In other words, and this is something that clearly emerged from today's discussions, a more global approach to cyber resilience exercises is needed.

In this regard, let me briefly insist on the G7 joint crisis management exercise to be held in early June, coordinated by Banque de France. We will have an excellent opportunity to assess our ability to exchange information and take collective decisions in a mock crisis situation. Good and clear communication

[1] FSB, 12 November 2018.

will be essential, underlying the critical role of the communication protocol designed in this regard.

But preparation against cyber threat is a moving target. A number of avenues need to be explored.

- First, if this exercise is necessary *per se*, its full potential will be delivered only if all lessons are properly drawn. Some guiding key principles, or “Fundamental elements”, to be designed in the wake of the G7 exercise, will help achieve this objective.
- Second, we must leverage on this G7 exercise: the regular practice of coordinated crisis management exercises should be encouraged in order to enhance the resilience of the financial system.
- Third, an enlargement beyond the remit of G7 countries should be considered with some other jurisdictions and/or with BIS involvement, and possibly beyond the sole financial sector actors. In future exercises, the current format will require cooperation arrangements on a wider scale.

**

Regulation and supervision, information, and preparation: these are the areas where we clearly need to improve our coordination. I would like to conclude with a last imperative: action. We all share the principles, but there was today in this conference a sense of urgency, of concrete urgency. This is where the French presidency of the G7 intends to be useful:

- First, by giving greater visibility and support to the CEG work, which is going to deliver important papers on cross-sector coordination and on the assessment of vulnerabilities.
- Second, by proposing to the FMCBG meeting in Chantilly in July to engage on three additional steps:
    - on regulation, to mandate the FSB to deal with the proliferation of regulatory texts;

- on information, to define within the CEG a categorization of cyber incidents;
- on preparation, to take stock of the lessons of the first G7 joint crisis management exercise, and be ready to extend it as appropriate.

There is no threat which we are surer of than cyber risks in the financial sector. And there is no perimeter more suitable to deal with it than the G7, although not an exclusive one. We cannot afford to wait; let us act, together.