



MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

Conférence G7

"Cybersecurity : coordinating efforts to protect the financial sector in the global economy"

**Discours de Bruno Le Maire,
ministre de l'Économie et des Finances**

Paris

Vendredi 10 mai 2019

Contact presse :

Cabinet de Bruno Le Maire

01 53 18 41 13



Monsieur le Gouverneur,
Ladies and gentlemen,

This conference on cyber security in the financial sector is a timely one, and I would say a necessary one, on a key issue. It may seem to be a technical issue, but in fact it is a political one. It is a decisive issue for global financial stability.

In a world where the importance of digital services is becoming increasingly important, cyber security is a growing and urgent concern. I would like to warmly thank Governor François Villeroy de Galhau for hosting this conference. While the transition towards a digital economy is a source of great innovation, it is also a source of new risks.

There are risks for the protection of privacy and for the data of our citizens, and these are major political issues for Europe. We saw these risks for instance in the attacks suffered by the NHS in the United Kingdom. They were aimed at accessing the confidential data of individuals.

There are risks also for our businesses. Successful global cyber-attacks such as *Wannacry* in May 2017 or *NotPetya* in June 2017 have shown that cyber-attacks lead to severe economic disruptions and major losses for the targeted firms. These are very real: Nissan had to halt production for a time. Hospitals had to postpone non critical operations.

There are risks too for our national interests. We know that some actors seek not only to harm our citizens and our companies, but also to harm us as countries. They want to destabilise our political systems and we should be aware of that. We should not be naive: they do not have our best interests at heart !

Cyber-attacks are increasing in number, in scope, and in sophistication, making it more and more difficult to predict the total impact. But what is clear is that cyber-risk has become a systemic political and economic risk for all of us.

The financial sector is particularly exposed to cyber risk.

The financial services sector has traditionally been the largest target of cyberattacks because of the potential for direct financial gain and access to very profitable confidential financial data. In 2016, the financial sector was attacked 65 % more often than any other sector.

These attacks can seriously damage financial institutions, including public ones. I think we all have in mind the attack suffered by the central bank of Bangladesh, some three years ago. The figure of the financial damage has been set at more than 80 million dollars. And had the criminals got their way and not been stopped, it could have cost a billion dollars.

Attacks on the financial sector don't just affect the financial sector, they quickly spread to the real economy. They create financial loss, they disrupt supply chains, and they contribute to a broader loss of confidence in the economic system. Confidence fuels our economy : lose it, and we are all lost.

In addition, the financial sector is special because of how integrated it is. It is by nature a global market that does not stop at borders. And it is connected to every sector of the economy, which is why we must treat cyber-attacks as a systemic risk. No country can act efficiently by itself. We need a truly coordinated global approach in order to be able to respond efficiently to attacks.



Today, I think that the main challenge we face is no longer awareness. We are all aware of the risk of cyber-attacks and we are all aware of the risk of such attacks spreading to the real economy. What we need today is action and coordinated decisions. My proposal would be to act on four major points.

The first is resilience.

Banks and financial institutions must continue to reinforce themselves against potential cyber-attacks. This is expensive and complex but it is absolutely essential. I really want to send the message to financial institutions that it is time to take big decisions to reinforce yourself against cyber-attacks. And since we are meeting at the Banque de France, I want to take this opportunity to salute its work. The Banque de France has developed technologies to test concretely and effectively banks' resistance to cyber risks. But once again, let us be clear : financial institutions also have their own job to do.

Second, we need a greater convergence of rules.

Many countries have put in place their own rules. But they will be useless if they are not based on a coordinated approach. Because those rules are not all the same. This creates complexity for financial actors. But even more importantly, there is a risk of seeing some financial actors running to the lowest bidder and relocating their information systems to countries with less strict rules in order to minimize their costs. And there is a risk that criminals target the weakest regimes – putting the whole global financial system at risk. If we do not have a coordinated approach, we run the risk of failures that might weaken the whole financial system.

More resilience and more convergence – this is what we are aiming to achieve in the EU through the Network and Information Security (NIS) directive, which was voted in 2016. And this is what the G7 Cyber Experts Group has been promoting ever since its creation in 2015.

Third, we need to find a balance between regulation and innovation.

We must make sure that the regulatory framework keeps encouraging innovation. Innovation should not be stifled.

However, it needs to be encouraged in a way that is good for growth but also protects financial stability. I want to insist on that key point: the financial sector needs stability and confidence.

Finally, we need more global coordination and cooperation.

I am deeply convinced that this is essential to fight cyberattacks. Cyber threats are proof that we need more multilateralism and more cooperation between our countries. The G7 is the right forum where we should address these issues. And it is the right forum for operational cooperation, thanks to the trust and reciprocity which makes the G7 very special.

This is why as Presidency of the G7 this year, we have decided to carry out a G7-wide cross-border cyber crisis simulation exercise next month. This is a world first and I am confident we will be able to learn a great deal from it, and collectively improve our resilience further as well as our ways of working together.

But because the only way to fight the cyber threat effectively is at the global level, our principles adopted within the G7 need to be embraced and implemented much more widely, by the G20 as a first step and beyond.



To conclude, our focus today is no longer so much about raising awareness in the financial sector on cybersecurity. It is now time to decide. It is now time to take action. We have to ensure the greater convergence of the various approaches that jurisdictions have been taking on their own to improve the resilience of the financial sector.

It was a necessary step but this is not enough. Once again, we cannot rely on a system based only on national actions and national jurisdictions. We need more integration and more coordination. And we need to learn how to work together to tackle this global challenge.

I hope this conference will help us in our efforts towards these aims and I want to warmly thank again François Villeroy de Galhau for this helpful and necessary conference.