PALAIS DU LUXEMBOURG - CYBER SUMMIT - WARM-UP WORKING SESSION
– 2026 JUNE 1er –

Building Cyber Capacities in the Balkans Under Permanent Threat

Senator Olivier CADIC, *Vice President of the Foreign Affairs, Defense and Armed Forces Committee :*

Ministers, Deputy Ministers, State Secretaries, Directors, Ladies and Gentlemen,
Dear partners and friends,

Welcome to Paris. Welcome to the French Senate.

It is a great pleasure and an honour to welcome you here today, in this institution, to discuss issues of the utmost importance: technological challenges, cybersecurity, democratic resilience, and, even more so today, the profound transformations brought about by the rapid progress of artificial intelligence. These are no longer merely technical matters.

They are questions of sovereignty, security, democratic stability and international cooperation. They concern our ability, as democracies, to protect our institutions, our citizens, our critical infrastructures and the integrity of our public debate.

As Vice-President of the Senate Committee on Foreign Affairs, Defence and Armed Forces, and as rapporteur for the budget of the French National Cybersecurity Agency, ANSSI, I am deeply convinced that cybersecurity has become one of the central dimensions of our national and collective security.

France has long been committed to international security and to the stability of Europe with its partners, that I thank for being here too.

This commitment is particularly strong when it comes to the Western Balkans.

For France, the Western Balkans are not a distant region.

They are part of Europe’s strategic environment. Their stability, their resilience and their democratic strength are directly connected to the security of the European continent as a whole.

This is why France as the European Union has developed a clear strategy for the Western Balkans, supporting reforms, regional cooperation, resilience, cybersecurity and the fight against disinformation.

It is also why the French Parliament, and the Senate in particular, has supported and voted the necessary investments to strengthen these efforts.

And I want to thanks the Western Balkans Cyber Capacity Center for its commitment, its action and for organizing this delegation at the Summit.

The countries of the Western Balkans face many of the same threats as we do. But for them, these threats are not theoretical. They are not distant. They are at their doorstep.

They face daily pressure in the information space. They face attempts to weaken democratic debate, to exploit social divisions, to target institutions and to put pressure on critical infrastructures.

In many ways, they are on the front line of the information struggle that concerns all European democracies.

This is why their experience matters so much. We are not here only to share with them what we know.

We are also here to listen and to learn from what they live, observe and confront every day.

Their experience in democratic resilience, in countering information manipulation and in strengthening institutional capacity is essential for all of us.

I also want to warmly welcome our European partners.

Their presence here is natural. We are gathered in the French Senate, but on these issues, this house is also, in a broader sense, a European house.

Because the security of France cannot be separated from the security of Europe. Because the protection of our democracies, our infrastructures and our technological environments requires European coordination, European solidarity and European action.

Allow me to mention one very concrete example of this commitment. Tomorrow, in the French Senate, I will defend three amendments as part of the Military Programming Law for 2024–2030, all of them directly linked to the challenges we are discussing today.

The first proposes to affirm the principle of a graduated and proportionate cyber deterrence doctrine, including the use of offensive cyber capabilities when necessary, in response to state-sponsored cyberattacks and hybrid threats.

Once an attack has been identified and formally attributed, the amendment provides that the Armed Forces may assume responsibility for leading the cyber response.

The second aims to strengthen the protection of critical infrastructures against remote control or interference by foreign suppliers through electronic systems embedded in strategic equipment.

The third seeks to reinforce technological sovereignty and cybersecurity requirements for connected vehicles and embedded systems used by our armed forces, public administrations and critical infrastructure operators…

… in order to reduce the risks of espionage, interference and technological dependency.

These amendments reflect a simple conviction: resilience is not only about defending ourselves against attacks.

It is also about reducing strategic dependencies, securing our technological environment and ensuring that democracies retain the capacity to deter those who seek to undermine them.

And I want to extend a very warm welcome to our American partners and to the United States delegation represented here today.

Your presence matters. It reminds us that the transatlantic relationship remains a cornerstone of our collective security.

It also reminds us that this relationship must be discussed openly, honestly and strategically, in light of the new technological, geopolitical and security realities we all face.

Allow me also to take this opportunity to wish our American friends a very happy 250th anniversary of the Declaration of Independence. This is, of course, an American anniversary. Yet the name of **George Washington** will forever be associated with that of **Lafayette**.

Also, it speaks to all democracies attached to freedom, responsibility, constitutional government and the right of peoples to determine their own future.

As we begin our discussions, I hope that our conversation will be candid, useful and concrete.

We can use the Paris Format, which is a chatham house provocative lane, each time we want to test pressure any idea..

We need to share our experiences, both the successful ones and the difficult ones.

We need to speak not only about threats, but also about capacities, decisions, methods and cooperation.

We need to understand what works, what does not, and what still needs to be built together.

In our new world, alignment in principle is no longer enough.

We need to meet.

We need to speak face to face.

We need to understand one another’s constraints, perspectives and responsibilities.

And above all, we need to build the ability to stand together.

That is the purpose of our meeting today: to meet face to face, so that we can stand side by side.

Thank you.