

Paris cyber week : Opening speech

June, 5th 2024

Democratic countries must take back the initiative.

An international cyber deterrent force must be created to destroy China's cyber wall on command.

To build this force, we need political courage, solidarity and the inspiration of Alan Turing and Bobby Fisher.

Ladies and Gentlemen,

Thank you Sébastien for this invitation.

I've been in the Senate for 10 years, representing the French abroad.

60% of my time abroad. 537 trips to 114 countries.

VP Commission AE Def

I have included the fight against Fakenews in the 2018 military programming law.

In the latest military programming law for 2023,

I integrated the guarantee of freedom of maritime movement

by our navy in the South China Sea and Taiwan Strait.

In charge of cyber for 7 years

I'm a cyber paranoid.

In 99, I launched my market place on a Friday at 15.00.

On Monday, my marketing manager was bragging about the exceptional traffic figures on our server.

My IT manager asked to speak to me.

At 3 a.m. on Saturday, someone broke into our servers and downloaded adult movies.

The whole world was uploading them all weekend.

My marketing manager suggested me to move to adult movie industry.

I preferred to buy a firewall.

You understand now why I developed a cyber paranoid.

Tomorrow is the 80th anniversary of D-Day.

80 years ago, thousands of soldiers lived the last day of their lives.

Tomorrow, I'll be at Omaha Beach to pay tribute to their memory

and express our country's eternal gratitude for their sacrifice.

The success of D.day owes much to Alan Turing,
who succeeded in deciphering the Enigma code used by the German army to transmit
military information.

This code, which changed every 24 hours and had billions of combinations, was considered
unbreakable.

Turing saved a considerable number of lives.

It was Alan Turing who prefigured artificial intelligence in 1950.

Yesterday, we were discussing what could be the next 80 years of security in Cyberspace.

Something tells me that our successors will continue to talk about security, that countries
will seek to decrypt encrypted data just as they did 80 years ago and today.

Quantum computing will have taken them into a new dimension.

80 years ago, thanks to heroes, Europe regained its freedom.

Just 35 years ago, the Chinese authorities massacred freedom and its students in Tiananmen
Square, because they were calling for democracy.

Its mastery of technology has enabled it to create a cyber-wall to impose social control on its
population, combining social networks, facial recognition cameras and artificial intelligence.

The Chinese Communist Party has set 2049, the year of its centenary, for China to impose its
leadership on the world.

The question before us is: What kind of world do we want to live in in 2049?

Do we want to live in a world where democracy and individual freedoms are respected, or in
a world where everyone must conform to an order determined by the party or an autocrat?

We are facing a hybrid war.

The cyber dimension, which includes the criminal sector, espionage and military action that
preoccupies us at Paris Cyber Week, is not the only one.

We should also mention the trafficking of human beings and migrants sent in waves to overwhelm our borders.

Or the environmental crimes of illegal mining and trafficking in metals and minerals.

Our commission of inquiry into drug trafficking has just published its report.

Chinese precursor chemicals make up 70% of cocaine.

I've seen their presence in these laboratories deep in the jungle two weeks ago.

These chemicals are the source of synthetic drugs such as fentanyl, responsible for some 120,000 deaths in the USA in 2023.

Along with Hong Kong, which has become the black hole of money laundering, Beijing is at both ends of the narco-trafficking supply chain, one of the components of the hybrid war to which democracies are committed.

We could also elaborate on all aspects of disinformation.

There's no cannon for destroying a lie.

Totalitarian or authoritarian states attack democracies on a daily basis, relativising the importance of respecting human rights.

In this battle of opinions, democracies must not be naive.

At the start of the Covid crisis in March 2020, the Chinese embassy in Paris issued a statement saying that France was letting its elderly people die in EPADHs.

I produced a report, and called for the creation of a "cyber reaction force", the only one capable of reacting and fighting offensively against the enemies of our republican values.

15 months later, the Viginum national agency was created in France to detect informational attacks.

Viginum now tracks down foreign interference on the Internet.

It is proving invaluable in dealing with the increasingly sophisticated modus operandi observed in the run-up to the Olympic Games.

On March 25, the US Department of Justice unveiled an indictment

against 7 Chinese nationals belonging to the APT31 hacker group,

which reports directly to the Chinese Ministry of State Security.

I would like to thank the FBI and the Justice Department for their action and for keeping us informed.

This is clearly an act of cyber-warfare, committed by a 2.0 dictatorship.

Starting this week, as part of my cyber prerogatives,

we began work in the French Senate to assess what should be done

when our country falls victim to an act of cyber warfare.

Once again, I'd like to thank Sébastien for allowing me

to bring some of the participants together in the Senate on Monday,

to share their views and open the sequence of hearings following the APT31 attack.

Are we going to stand idly by?

I set up my company at the age of 20.

My company collaborated in the creation of several weapons systems,

and I worked with Roland Moreno, the inventor of the smart card.

I used to say: Your present is my past.

Since I've been in the Senate, I feel like I'm living in someone else's past.

We're always reacting.

We're under so many cyber attacks that I feel like we're punching balls.

We're in over our heads.

The Chinese are doing things on our networks that we observe, but don't understand.

They're preparing for war.

They're already here.

Each of us has vulnerabilities.

Democratic countries must take back the initiative.

My uncle had been teaching me to play chess.

When I was 10, Every day, we'd go to the newspaper to study the games of the world championship between Bobby Fisher and Boris Spassky.

Alone against the Soviet grandmasters, who had dominated the chess world for decades, Bobby was unpredictable.

He found the loopholes and won.

Faced with China, we must follow his inspiration and act likewise.

For too long, we have failed to respond to cyber attacks.

We're told it would escalate the situation.

The CCP is no longer afraid of us.

It sees democracies as weak, predictable systems.

We have to surprise them.

An international cyber deterrent force
must be created to destroy China's cyber wall on command.

To build this force, we need political courage, Solidarity
and the inspiration of Alan Turing and Bobby Fisher.

We need to understand that no democratic country,
not even the United States,
has the critical mass to compete alone against the threats posed by China today.

Faced with a hyper-centralized China, democracies appear divided.

The fragility of our edifice stems from the fragmentation of states,
and the separation between public and private players.

The EU has taken great steps towards unity by creating a Europe of cyber sovereignty.

Even united on this issue, the EU will not have the critical size.

The United States advocates cyber solidarity. And rightly so.

And I'd like to thank Phil Stupak of the White House for all the time
he devoted to me and the trust he placed in me.

We need a strong partnership between the US and the EU,
but also with private companies.

In Washington, the people at Google told me.
Russia is bigger than Ukraine.

On the Internet, Google is more powerful than Russia.

AWS proved its ability to make Ukraine resilient at the start of the Russian invasion.

US-EU collaboration, public-private,

must be able to take place in the same way as we do in the nuclear sector, starting,

for example, by transparently sharing our mutual vulnerabilities.

I thank Daniel Le Coguic, ACN president to promote this idea.

Why were IPAC members attacked?

Because Beijing fears us.

I think we need to build an international inter-parliamentary cyber alliance

to accompany and support a policy of cyber solidarity.

There is no system without vulnerabilities.

There are ways to destroy China's cyberwall... from the inside...

and free the Chinese from this 2.0 dictatorship.

CCP proudly announces their long-term plan to rule the world by 2049.

Democracies also have a long-term plan.

It's to prevent the Chinese Communists from achieving their plan.

Thank you very much.