

EU and NATO Neighborhood Fighting Malign Foreign Influences
Speech by Olivier Cadic, senator for French citizens abroad
17/10/2023 – at Romanian Embassy in France

“Russia is the storm, China is climate change”

There is no cannon to destroy a lie.

Large-scale information manipulation campaigns constitute the new, hybrid form of foreign interference.

This is a challenge for democracies in the information and reputation war waged by certain authoritarian regimes.

Information manipulation campaigns are not new.

There is a Russian signature when it comes to disinformation that includes the spread of rumors and fake news.

The revisionist strategy dates from the Soviet era.

The Soviets became famous by attributing to the Nazis the execution of Polish officers at KATYN or the assassination of JFK at the CIA

In 2016, living in the UK, I observed the wave of misinformation during the Brexit campaign.

This intensified with the 2016 US presidential election.

Also in preparation for the French military programming law in 2018, I went to the Pentagon. Their hybrid warfare doctrine inspired me to integrate the fight against “Fake news” into the military programming law (LPM) 2019-2025.

But if we have a Russian storm, Climate Change is China.

China is the leader of the countries engaged in the challenge to the international order directed against Western countries.

In 2020, China tried to hide its mistakes in handling Covid.

The CCP has promoted China's model of Widespread Surveillance and denigrated democracies.

A press release from the Chinese Embassy in France indicated, for example, that retirement home staff had deserted and left the residents to die of hunger and disease. The Ambassador has been summoned. The press release has not been withdrawn.

As a consequence, in April 2020, I called for the creation of a cyber rapid reaction force in a report. Its title: Disinformation, cyber attacks and cyber malice, the other Covid war.

16 months later in July 2021, France created the VIGINUM agency.

Over the past 3 years, Viginum has unveiled several large-scale Russian operations.

France no longer hesitates to use NAME and SHAME.

We knew that the PARIS 2024 Olympic Games would be the subject of information attacks.

The description of a decadence of European morality is part of the Russian arsenal.

The controversy over Christ's last supper during the opening ceremony of the Olympic Games in Paris took up elements of controversy following the fire at Notre-Dame.

China is not left out.

The night following the opening ceremony, 3 districts of Paris experienced a 10-minute power outage.

The information was picked up by Chinese media.

More than 4 million Tik Tok accounts relayed the information, some announcing that only the Sacré-Coeur Basilica remained illuminated.

Digital campaigns to manipulate information have become a real instrument for destabilizing democracies.

We seek to better prepare individuals and societies.

Viginum has prepared a guide for Businesses for the Olympic Games, available in French and English.

Viginum demonstrates that we can move in this direction in order to anticipate disinformation attacks.

CCP, Russia are no longer afraid of us.

They see 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.

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.

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.

There is no system without vulnerabilities.

Taiwan is the laboratory of the Chinese disinformation attack.

To optimize our action, we need to invite Taiwan to join The NATO Cooperative Cyber Defence Centre of Excellence in Tallin and the NATO strategic communication center of Excellence in RIGA .

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

with a system without freedom

Democracies also have a long-term plan.

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

Thank you very much.