# JEAN-LOUIS GERGORIN

## Senior lecturer at Sciences Po Paris, owner of the cyber and aerospace consultancy JLG Strategy

**François Barrault, Founder and Chairman of FDB Partners, Chairman of IDATE DigiWorld**

I would now like to welcome Jean-Louis Gergorin, who was supposed to be with us today but had some issues. He will talk about the confrontation in digital space, the alternative model to war to pursue politics by other means, in other words, how the new wars are now digital rather than physical.

**Jean-Louis Gergorin**

Hello. I am very happy and honored to speak about digital technology after Covid at the Abu Dhabi World Policy Conference.

Clausewitz said that war is the continuation of politics by other means. By politics, he meant all human actions aiming to control or influence people and/or territories. The weaponization of digital technology is a modern alternative to war and the continuation of politics by other means. This new method, this tool of influence and political control, is carried out in two main ways of using digital technology that significantly intersect.

The first is hacking. Hacking is when an actor breaks into an information system to influence and gain control through sabotage and intimidation. It is virtual sabotage introduced by malware, which is activated at the time of the attacker's choosing and aims to intimidate or to prepare future actions. This includes spying, a major activity that has resulted in an enormous transfer of technology to certain powers that in the last 20 years have caught up with and even surpassed the countries they imitated.

The second is predation, which is a criminal activity. One form of this, ransomware, has grown much more common in recent years. Ransomware freezes up an information system and may or may not steal and release confidential data unless a large sum is paid to cybercriminal groups that are often very well organized and embedded in the countries where they operate completely legally because they have not signed the Budapest Convention on Cybercrime. These ransomware groups, whose names are known – REvil, DarkSide, etc. – never act against the countries hosting them or their allies.

This is what hacking is about.

The second form of action is the manipulation of digital information on the Internet, especially on social media, which, as you know, billions of people use. So this has a devastating impact when it is used to spread fake news.

It is relatively easy to combine these two activities. This was demonstrated by the hacking of the European Medicines Agency in December 2020, when information about all the internal correspondence of agency officials evaluating the Pfizer vaccine was stolen.

The theft led to the spread of manipulated information on hackers' forums and social media, where some exchanges were manipulated to give the impression that the Pfizer vaccine's side effects were much more serious and much more pernicious than they were in real evaluations. The aim was to significantly destabilize the vaccine and fuel campaigns against the vaccine, which went viral with a lot of fake news and even conspiracy theories. This has consequences: human lives are literally at stake when there is fake news about vaccination.

The use of this method is on the rise, and not only by the great powers that have integrated general staffs that do both hacking and manipulate digital information. We must react to this. How can we ensure peace, stability and security in a digital space that is somewhat misshapen by this weaponization? I think we need to distinguish between two things.

First, I think international regulation of social media is impossible. On the other hand, governments can do this, especially in countries where they directly supervise them – I am thinking of the United States –, or it is up to social media themselves to do this through self-regulation to fight fake news.

Second, hacking can escalate to the point where it gets out of control one day, unleashing digital pandemics, so to speak. It is essential to stop this. But I do not think discussions limited strictly to digital technology are enough to do that.

In one sense, the June 16 Biden-Putin summit in Geneva was very interesting. It led to a certain easing of Russian-American tensions in general. Over 50% of the talks focused on cybersecurity after a ransomware attack on Colonial Pipeline in the United States. Since then, a certain amount of restraint has been observed. Ransomware groups in Russia have not carried out any major, devastating attacks like the one on the Colonial Pipeline since an assault on Kaseya was thwarted in July 2021.

What is needed is to integrate discussions of the underlying geopolitics of conflicts with talks on moderating and limiting the weaponization of cyberspace. A forum is needed for that, and I think the most legitimate one is the United Nations Security Council. President Macron's idea of a UN Security Council members' summit fell flat. It could be revived by focusing on improving security in cyberspace.

For this to happen, heads of state obviously need to start conversations among their digital experts. But at the same time, there needs to be a discussion about the geopolitical and strategic underpinnings, i.e., conflicts.

There will be no stability in the cyber relationship between Russia and the United States and between Russia and the countries of Western Europe unless the geopolitical undercurrent, i.e., the Ukrainian conflict and the subsequent sanctions on Russia, is addressed. If it is not, détente or stability in cyberspace between Russia and Western countries will be out of reach.

This model is what Nixon and Kissinger did with Brezhnev and Gromyko during the US president's May 1972 trip to Moscow. They dealt with the overall underlying geopolitical situation at the time. Then they signed SALT 1, the first strategic arms limitation agreement. This can serve as a model for cyberspace. It is the only way. I think it could be a promising path forward.

At the same time, let's focus, in an integrated way, on the underlying geopolitical tensions especially between Russia and China on the one hand and Western countries on the other, and how they are manifested in the digital space. I think this is a promising path. In any case, I am all for it.