JEAN-LOUIS GERGORIN

Former Director of the Policy Planning Staff of the French Ministry of Foreign Affairs

Thomas GOMART

I move now to Jean-Louis for his presentation. Jean-Louis, the floor is yours.

Jean-Louis GERGORIN

Thank you, Thomas. I'm starting in French just to say that my approach to cyberattacks is closely connected to cybersecurity, in other words all the methods and analyses of hacker attacks, whether for espionage, sabotage or financial extortion, but at the same time wider and more limited.

To me, cyberattacks, to paraphrase Clausewitz, are a modern form, usually as an alternative to war, of the continuation of politics by other means. I obviously don't underestimate cyberattacks in wartime, which are used to cripple the enemy's computer systems, like the Americans did to Iraq's air defenses in March 2003, but strategically they are integrated into all the technological means, including electronic warfare, aiming to neutralize the enemy's capacities.

On the other hand, cyberattacks in peacetime are a major, steadily growing threat, the use of non-lethal means to achieve political and strategic objectives, that Professor Norodom talked about in her brilliant presentation yesterday. I would like to recall what Sun Tzu, the historic father of military strategy, said: "Winning without fighting is the height of strategy." So that's what we are going to discuss as we switch over to English.

Once we have defined cyber, what are the main tools, vehicles, to reach strategic goals through cyber? There are in fact two main ways to do it that are more and more integrated and more and more perpetrated by the same aggressors. The first one is hacking, which is the clandestine penetration of IT networks in order to steal information, to sabotage, or to extort money for example with so called ransomware attacks.

There is, however, another major way which is to reach a political goal, a strategic goal, through the manipulation of digital media. The most common such tool is the manipulation of the major social media. We have seen that, for example, in the 2016 US presidential election where a number of fake Facebook, Twitter or Instagram fake accounts, what the experts call sock puppets, were created by young staffers of the Saint Petersburg Internet Research Agency (IRA) assuming false US identities. Often these IRA "actors" were defending rather extreme political positions impersonating for example black power militants or white supremacists based in various parts of the US. Once questioned on the IRA, Vladimir Putin answered that this organization is totally independent from the Russian Government and remarked that the Soros Foundation, that the Russian authorities have long accused of trying to destabilize the regime, is independent from the US Government...

The importance of the political manipulation of social media for political purposes is demonstrated by Facebook and Twitter announcing periodically the closing of "inauthentic coordinated" accounts.

However since 2016 we are also confronted to a new way to manipulate digital information, the deep fakes which are fake audios and videos which thanks to a sophisticated artificial intelligence tool called Generative Adversarial Networks are very difficult if not impossible to distinguish from genuine ones. These fake videos can then be widely disseminated through all digital vehicles, messaging services, social media, emails, TV etc. There is a competition between a number of research centers, not mentioning those of the bad guys, to continuously to continuously improve the "quality" of these fake videos. To give you a concrete example it would be very easy to create a deep fake of Thierry de Montbrial having a politically sensitive one to one discussion with one of the VIPs present here in Marrakesh. It would be impossible to prove that this video had been artificially created. Think of the potential use of such deep fakes in future electoral campaigns.

How the major powers have reacted to digital challenges and opportunities?

The Americans for many years have mainly focused on intelligence, with an obsession to collect all possible data on people and situations, far more by the way than they could process. This addiction of the NSA to know everything, everywhere, including wiretapping the German chancellor discussing the menu of a dinner with her husband to hacking the information system of the Elysée. A lot of that in my view has been clearly excessive, not very friendly, but while the Americans were focusing mainly on intelligence other powers were focusing on the manipulation of digital information, and they started earlier. This explains their strategic surprise when they were confronted in 2016 to a sophisticated digital operation targeting the Presidential campaign with a combined use of hacking and social media manipulation.

The Russians and the Chinese as early as the beginning of the 2000s, even in the late 1990s, understood the ability of cyber, both through hacking and later through social media manipulation to gain strategic advantages. They have done that in different ways. The Russians are very bright, very brilliant. I do not think they are spending enormous resources in their digital operations. We should know that the Russian defense budget is one of the most cost effective in the world. This cost effectiveness is increased in cyber thanks to the excellent training and the very good brains of their experts.

The Chinese are focusing on two priorities. The internal one is an increasingly sophisticated use of digital tools to protect the regime by insulating the country from the global Internet and by the implementation of an Orwellian digital surveillance of the population. The external priority has been a huge economic cyber intelligence effort which has greatly helped China to close its technological gap with the US.

The core of my conclusion is the rapid rise of the threats caused by the combination of three factors:

- the continuous digital transformation of all sectors of our nations

- the obvious finding that the more we digitalize the more vulnerable we are

- the growing weight of the state sponsored operations and of the state tolerated cybercriminal activities such as ransomware in the global threats.

The private companies alone cannot face these threats because only the states have the intelligence capabilities allowing to identify the attackers. If you do not know who is attacking you, you are far less able to protect yourself. Therefore, a far better interaction on threat intelligence between business and Government is highly desirable.

The Governments have been often asked to have a doctrine of cyber deterrence. But in cyber you cannot have a deterrence similar to nuclear deterrence except to deter a massive cyberattack on the critical infrastructures of a nation. But to respond to such a daily cyber guerilla you have to demonstrate your ability to hurt the attacker in what I would call a reactive defense. You have to identify your adversary and to punish him, not to escalate but to demonstrate that you know who the adversary is and to punish him. This is essential. If we do not have that we are paralyzed.

We in Europe are facing a recent serious threat: the pre-positioning in critical infrastructures (mainly in the energy sector) of key countries growing numbers of state controlled implants giving their remote controller the capability to come back later to materially impede these infrastructures. The goal is just to intimidate and to silently tell our leaders, 'You know we can anytime disrupt for a few hours the power supply, electricity, in one of your cities, as it has happened several times in one Eastern European country. This is a major challenge.

To face all these challenges, we Europeans need both a stronger and more coordinated cyber defense and an international organization and a global dialogue to deal with cyber risks that are growing. This is what President Macron started to launch with his appeal for peace and security and trust in cyberspace almost one year ago during the Paris Peace Forum and with bilateral discussions on cyber with the major concerned powers.

Thomas GOMART

Thank you very much, Jean-Louis. I want to give Meir a chance to speak. Would you prefer to speak at the podium? There is a point of debate between Patrick and Jean-Louis about the role of companies so very briefly maybe on that topic, could you elaborate?

Patrick NICOLET

On the threat to intelligence, you are right. It is a very critical aspect. We have collaboration with a French state agency in Annecy that is providing us some information, CGHQ in the UK as well. It is not available everywhere. In India we have 110,000 people. I have zero information. However, this is complemented by the industry. We have our own large companies, such as Microsoft, Cisco, IBM, that process billions of events per day and are providing us with intelligence on the characteristics of different attacks.

We have an industry partnership that has been launched by Brad Smith, the general counsel of Microsoft called Tech Accord that brings together about 60 companies where we sit together and we exchange best practices and intelligence because ultimately it is a cost of doing business for us and there is no competitive advantage to gain. For the fun part, there is a hacker super league, so you can be informed and today I can tell you the group called Russian Bear is the number one in the super league because they can penetrate and migrate in a system in 30 minutes and the number two needs two and a half hours. It is crazy, but that is the way it works. Yes, we need the state, but the industry and the enterprise are developing their own means.

Thomas GOMART

I will let Jean-Louis respond to that after the presentation by Meir.