Switzerland and cybersecurity: reports, debates, action!

The upcoming arrival of Ambassador Alexandre Fasel, who will be primarily responsible for cybersecurity issues, heralds an increase in the foreign digital policy strategy, writes our columnist François Nordmann

Cybersecurity was at the center of the talks between Presidents Biden and Putin on June 16 in Geneva. The attacks on certain infrastructures in the United States originated in Russia: were they carried out by specialized Russian state services or by cybercriminals based in Russia? President Putin has denied any official intervention. On the American side, they demanded more cooperation from the Russian Federation. A list of 16 strategic sites has been given to the Kremlin's master: if the installations listed in this document are victims of cyber attacks, the United States, according to President Biden, are able to trigger retaliation of the same nature, for example against pipelines carrying Russian oil or gas...
Evaluation by a British institute

In Switzerland, too, the authorities are aware of the risk of hospitals, communication and transport systems and other key production centers being paralysed by attacks from electronic viruses. Two intelligence reports published last spring within a few weeks of each other, the draft security report, which is still under consultation, and the report on the annual threat assessment, give high priority to the danger of cyber attacks. The means to counter this danger have been reorganized within the federal administration. Last year, a British institute conducted an evaluation of this system. It was positive about Switzerland's efforts, but pointed out that SMEs and even some sectors of industry were not sufficiently aware of the potential breakdowns of such attacks and the precautions to be taken.

The private sector is indeed required to both further digitalize its activities to remain competitive and to protect itself from cyber attacks. The NGO ICT4Peace, which has been working for twenty years to put the cyber sector at the service of peace and development, has just proposed a "Swiss Digital Charter" which would establish norms and principles to build trust in new technologies, to maintain an open, free, prosperous and democratic cyber space, and to guarantee the necessary resilience of civil society to cyber attacks. It is also a field of action open to Swiss diplomacy. The upcoming arrival of Ambassador Alexandre Fasel, who will be the main person in charge, announces a rise in the power of the foreign digital policy strategy, which is deployed in particular within the specialized bodies of the United Nations, working groups and commissions that are concerned with setting universal standards.

Switzerland's card to play

Today, the Security Council is debating for the first time how to maintain international peace and security in cyberspace, at the initiative of Estonia, a pioneer country in the digital field. This is a theme that Switzerland could easily take up again. On the subject of security, we should mention the excellent study by former ambassador Martin Dahinden on neutrality and the exercise of self-defense in the event of attacks against our country in

cyberspace, published by ICT4Peace. The Swiss Society for Internet Governance has just devoted an interesting debate to this topic. The question is becoming more and more acute: Can the rules of international law, including those of international humanitarian law, be transferred to cyberspace without further ado?

Switzerland still tends to reinforce the place of international Geneva in the governance of the Internet: the International Telecommunication Union, which manages the related technical standards, has its headquarters in Geneva, but does a world that is so diffuse, so fluid, that creates and fills its own space and functions in networks, need a single capital city or will it accommodate several centers? This is a real challenge for our diplomats.

Translated with www.DeepL.com/Translator (free version)