FRANCE GIVES ITSELF INCREASED MEANS TO COUNTER SKYROCKETING CYBER THREATS!

Interview with Olivier Cadic, Senator for French citizens living abroad
By Marc Jacob and Emmanuelle Lamandé

Last October, Senator Olivier Cadic (Union Centriste – French citizens living abroad) was elected vice-chairman of the Senate's Foreign Affairs, Defence and Armed Forces Committee, and re-appointed, for another three years, co-rapporteur for opinion on the budget appropriation dedicated to the SDGSN (in charge of the State Information Systems Security Policy) and the ANSSI. An opportune time for us to discuss his activities, but also assess the state of cyber threats in France.

Global Security Mag: What would you say is the state of the cyber threat in our country today?

Olivier Cadic: As a consequence of technological evolution, and the increasingly broad use of digital technology, the cyber threat has grown, taking different shapes.
Cybercrime has become professional; I would even say industrial. It has developed on a large scale, through ever more effective 'ransomware'. The figures given by the director of the ANSSI are especially striking: 128 ransomware attacks handled by the agency as of 30 September 2020, compared with 54 over all of 2019!
For cybercriminals, it's an easy way to make money; it's even a way to obtain foreign currency for 'rogue states'!
Public organisations and critical operators, such as hospitals, are no longer spared, and attacks against regional authorities, who are only just starting to take the full measure of the problem, are on the rise.
Espionage, a more traditional danger, is also on the rise, with targets such as strategic information on foreign and defence policies, but also access to industrial data and trade secrets, as well as the theft of personal data. By creating access points into many systems, remote working could offer attackers new openings. It is imperative to work towards making the tools of remote working more robust and more secure.
There's also been an increase in acts of piracy and sabotage, especially against our institutions and public administrations. These are carried out by ideologically-motivated cyberactivists, or cybergroups controlled by foreign powers.

IN 2019, THE ANSSI HANDLED 81 DIGITAL SECURITY INCIDENTS THAT AFFECTED FRENCH MINISTRIES

Over the year 2019, the ANSSI had to deal with 81 digital security incidents that affected French ministries – a slightly higher number (+3%) than the previous year (see table below).
Meanwhile, the Ministry of the Armed Forces, through Cyberdefence Command (COMCYBER), handles the detection of digital attacks against its own information systems. It recorded 88 events in 2019, compared to 13 in 2018. To us, this sharp increase is proof of an improvement in COMCYBER's detection capabilities. Let's not forget it was only created in 2017.
Let me conclude with the cyber threats that specifically target our democracy. Our enemies make increasing use of insidious actions – manipulation,

Number of incidents resulting from digital attacks processed by the ANSSI in 2019, by ministry.

Ministry	Number of incidents processed by the ANSSI	Comments
Ministry of Agriculture and Food	8	Including one major incident
Ministry of Territorial Cohesion	1	
Ministry of Culture	6	
Ministry of the Armed Forces	21	
Ministry of Economy and Finance	11	
Ministry of National Education, Youth and Sports	22	
Ministry of Higher Education, Research and Innovation	1	
Ministry of Europe and Foreign Affairs	14	
Ministry of the Interior	14	
Ministry of Justice	6	Including one cyberdefence operation
Ministry of the Overseas	1	
Ministry of Solidarity and Health	3	
Ministry for the Ecological Transition	8	
Ministry of Labour, Employment and Economic Inclusion	7	

disinformation, propaganda – carried out over various networks. The potential of mobilisation of such actions for the purpose of carrying out terrorist attacks or destabilising our societies is high. This is an extremely serious threat that we must also take into account.

'DISINFORMATION, CYBERATTACKS, CYBERCRIME: THE OTHER COVID-19 WAR'

GS Mag: Last May, you published a report entitled 'Disinformation, cyberattacks, cybercrime: the other COVID-19 war'[1]. What are the main lessons to be drawn from it?

Olivier Cadic: yes, my colleague Rachel Mazuir and I wanted to react fast and held several hearings, because the health crisis proved a fertile ground for the deployment of influence strategies by certain foreign powers, and increased the exposure to digital danger. Our report contains five recommendations, is deliberately alarming and brought disinformation to the foreground.
Indeed, the crisis triggered a communication war fanned by some foreign powers. For example, everyone was able to see on the website of the Chinese embassy in Paris how China disseminates inaccurate or incomplete information, in order to claim success against the pandemic or showcase how essential it is in the global struggle, through the supplying of healthcare products.
We also underlined how active Russia is in Africa when it comes to maligning France's presence there and criticising its initiatives. Rumours are also spreading across that continent, false information attributing the responsibility for the pandemic, or its consequences, to the French, and Westerners in general. This week in Jeune Afrique, the President of the French Republic confirmed this by denouncing the disinformation being carried out in Africa against French forces and French interests, and emanating from Russia and Turkey.
We also reached the conclusion that it is urgent for our government to establish a cyber reaction force to fight the campaigns of disinformation or influence of totalitarian and authoritarian countries that attack democracies. Otherwise, to quote George Orwell, 'a dictatorship can be established in silence'.

Recommendations of the 'Disinformation, cyberattacks, cybercrime: the other COVID-19 war' report

1. Establish a cyber reaction force in order to respond to false information in the field of health and attacks against democratic values, as well as to combat campaigns of disinformation or influence from certain foreign operators;
2. Invest in the digital security of actors in the field of health;
3. Immediately launch a large-scale communication campaign to promote the cybermalveillance.gouv.fr [2] platform and disseminate knowledge of digital protective measures;
4. Initiate the regular announcement, through the media, of a Top 10 of cybercrimes witnessed in the country;
5. Standardise and centralise the channels for receiving and handling complaints about cybercrimes filed online, which currently fall under the purview of local police and gendarmerie authorities.

5G: 157 APPLICATIONS HAVE BEEN FILED WITH THE ANSSI IN 2020

GS Mag: Back in January 2019 already, you challenged Foreign Minister Jean-Yves Le Drian over the dangers that Huawei represents for our security in terms of 5G. What is the current situation?

Olivier Cadic: The commercialisation of 5G offers in France is imminent. My colleague Mickaël Vallet and I took stock of the application of the 1 August 2019 law on the security of 5th generation mobile networks. This law entrusts the ANSSI with granting telephone service providers the authorisation to use equipment intended to build their networks – following risk assessment and for a limited time period.
The continuity requirement of these networks is highly strategic. As 5G will enable a new leap forward in the use of digital technology, especially for businesses, it is essential that telecommunication providers use secure hardware that will not be susceptible to service interruptions. Unfortunately, such risk cannot be ruled out when the equipment is supplied by a company like Huawei, subjected to the laws of its country and the pressure of its leaders. The possibility of aggressive action by a foreign power using this channel is a major, recognised threat to our security; one that is no longer in question.

For all that, the government still meant to take into account both the market balance and the situation of telephone service providers, who don't all use the same supplier.
Over the year 2020, France's four telecommunication providers filed 157 applications with the ANSSI, for a total of some 65,000 pieces of hardware, mostly antennas destined for urban areas. Around half of those applications (82) resulted in an authorisation being granted for the maximum duration allowed by the law, eight years. A third (53) resulted in an authorisation for a shorter duration than the maximum allowed. Finally, 22 were rejected. All the decisions resulting in rejections or shorter authorisations concerned Huawei hardware.

CYBERSECURITY: CONSIDERABLE PROGRESS HAS BEEN MADE IN THE PAST 10 YEARS UNDER THE ANSSI'S AEGIS

GS Mag: In conclusion, do you believe that France has made enough efforts in terms of cybersecurity?

Olivier Cadic: the appropriations in this field, which are subject to our oversight, have increased, and that is a sign that this important issue is indeed taken into consideration by the government.
Known as the 'cyber fire brigade' for its interventions in case of cyberattacks, the ANSSI is first and foremost tasked with preparing the State and critical operators to the threat, as well as reinforcing their protection and their resilience.
In 2021, the Agency will join the Cyber Campus, which will bring together in the same location, in the La Défense district in Paris, various actors of the cyber sector. I am pleased to see the ANSSI be a part of this landmark project, which aims to enable the structuring of a 'French cybersecurity ecosystem'.
2021 will also see the establishment of a branch of the ANSSI in Rennes, as part of the creation of a centre of expertise in cyberdefence which will include the Ministry of the Armed Forces, along the lines of what I saw in Beer Sheva in Israel. It will have room for 200 agents.
In the end, considerable progress has been made in the past 10 years under the ANSSI's aegis in terms of cybersecurity.

We are facing an increasingly strong cyber threat, and the race is now on. France is among the nations of 'the first circle'. Our skill is known and highly regarded. We should be glad of it, even though everyone knows that in this field, one should always remain humble! ■■■

[1] http://www.senat.fr/fileadmin/Fichiers/Images/commission/affaires_etrangeres/Coronavirus_suivi/4_pages_-_CYBER_vedf160420-2_01.pdf
[2] https://www.cybermalveillance.gouv.fr/