EUROPEAN CYBER DEFENCE AND CYBER SECURITY HAVE YET TO BE BUILT

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

Senator Olivier Cadic is currently preparing a report on the provisions concerning cyber defence. He believes several approaches must be taken in that area. First, it is necessary for the Military Planning Law to take better measure of the threat posed by information warfare. Moreover, European cyber defence and cyber security have yet to be built.

Global Security Mag: as a senator, you are a member of the Foreign Affairs, Defence and Armed Forces Committee, and rapporteur on the Military Planning Law and cyber defence. What are your duties within that committee?

Olivier Cadic: My colleague Rachel Mazuir and I are tasked to offer our views on the budget allocated to the ANSSI (National Agency for the Security of Information Systems), as part of the yearly government budget review. As part of the review process on the 2019-2025 military planning law (MPL), I suggested to Christian Cambon (president of the committee) that he entrust us with writing a report on all provisions concerning cyber defence.

THE BUDGET ALLOCATED TO CYBER DEFENCE HAS BEEN DOUBLED FROM THE PREVIOUS MPL

GS Mag: what progress has been made in the MPL concerning cyber security?

Olivier Cadic: In the MPL, cyber defence is included in every operational contract of our armed forces, and a permanent cyber posture is going to be created under the aegis of ComCyber (cyber defence command). The budget allocated to cyber defence has been doubled from the previous MPL (1.6 billion over 7 years), which will give us the means to better respond to attacks. Finally, 1,123 positions will be created, to be added to the 2,900 already extant within the military.
In order to strengthen our prevention system, the MPL gives telecommunication operators the possibility to put in place within their network cyber-attack detection apparatuses. These can then receive technical markers from the ANSSI, allowing the latter to gather information useful for the prevention of such attacks. The ANSSI will also have the option, in certain circumstances, to install its own probes on the networks and servers of operators and online services providers.

GS Mag: where is the MPL lacking in terms of cybersecurity?

Olivier Cadic: The main weakness of the MPL is that it only gives a partial vision of cyber defence. Besides the measures put in place by the military, the ANSSI and the Interior Ministry also come into play in terms of prevention, resilience, reaction and suppression in the civilian sector. A Strategic Review of Cyber Defence was published in February 2018 by the SGDSN (Secretariat-General for National Defence and Security). We're still waiting for the budget needed to put it into action to be allocated.
Finally, on the 'defence' side, the MPL has failed to get the full measure of the threat that information warfare represents in the open cyberspace we operate in.

GS Mag: what amendments to this law do you propose?

Olivier Cadic: We went in two directions. First, we introduced an amendment to the annexed report with the goal of making information warfare part of the MPL. In concrete terms, we've obtained that the 'manipulation of public opinion through the massive use of digital media and social networks, with the aim of altering the normal operation of democratic institutions' be entered into the MPL's annexed report.
Second, we introduced several amendments intending to strengthen legally the cyber-attack prevention system and extend it to operators of essential services, as defined by the European directive adopted by France last February.

"FAKE NEWS" ARE THE BIGGEST THREAT IN TERMS OF HYBRID WAR

GS Mag: what sort of risks could 'fake news' pose?

Olivier Cadic: A 'war' is being waged against democracies by authoritarian regimes. Our opponents make massive use of information warfare meant to undermine the foundations of our societies and values. They have 'troll factories' working around the clock to generate millions of targeted messages on social media; we've witnessed their effectiveness during the Brexit campaign and the American presidential election. Their techniques aim to sow chaos and paralyse our public services. That has driven the Pentagon to declare 'fake news' to be the biggest threat in terms of hybrid warfare.

GS Mag: your communications department is making proposals on that topic. Could you share your thoughts with us?

Olivier Cadic: I believe that with information warfare introduced into the MPL by the Senate, we now have to shift into high gear, by adopting a strategy that ranges from resilience to offensive responses. However, that implies a European or transatlantic dimension, as protecting our cyberspace is something we must do together. It would be ridiculous – and penalising – to protect our cyberspace at the sole level of our own country. Close cooperation with our partners and allies in this domain is absolutely necessary.

GS Mag: as part of your duties, you were invited to the Pentagon in the USA. What were the main lessons you learned from that visit?

Olivier Cadic: Last May I met at the Pentagon Theresa Whelan, Principal Deputy Assistant, Secretary of Defence for Homeland Defence and Global Security.
We discussed in turn the fight against fake information (a subject addressed by the United States Congress), the organisation of the cyber chain of command, dissuasion strategy and budgetary planning. The 1st Amendment of the American Constitution complicates their ability to fight against 'fake news'. I was grateful they decided to share their expertise with me, thus allowing me to enrich my own work.

GS Mag: you were similarly invited to the NATO Cyber Centre in Riga. What conclusions did you draw from that meeting?

Olivier Cadic: Janis Sarts, director of the NATO Strategic Communication Centre of Excellence – StratCom – reminded me of two facts that show how favourable the field is to cyber-aggressors. First, the average reading time for a given piece of information on the internet is seven seconds. Second, four out of five individuals react emotionally. Consequently, only one in five will make a rational decision … Now you see why populists currently have the wind behind them!

What one computer can create, another can destroy utterly. We discussed my idea to create an 'electronic vaccine' against fake news, in order to combat the manipulation of public opinion in our democracies.
Janis Sarts should be heard by our Commission at the senate in September.

NATIONAL POLICY

A Europe of cyberdefense and cybersecurity is work in progress

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

Senator Olivier Cadic is currently producing a report on all cyberdefense provisions. For him a number of issues need to be worked on. First of all it is necessary that greater account should be taken of the threat of information warfare in the Military Planning Law. It appears that a Europe of cyberdefense and cybersecurity is work in progress.

EUROPEAN CYBER DEFENCE HAVE YET TO BE BUILT

GS Mag: in your opinion, what are the efforts that France and Europe must make in terms of cyber security?

Olivier Cadic: If I were president (smile), I would appoint a general for cyber defence who would have equal status with the chiefs of staff of the three branches (Army, Air Force, Navy) to report to the Parliament. I would encourage EU countries to name out loud, if they are able to, the pirates by whom they are targeted. European cyber defence and cyber security have yet to be built. On that subject the European Commission is perfectly realistic, calling for an increased sharing of intelligence and noting that 'the absence of a secure, common communication network between European institutions is a sizable shortcoming.'
We must create an airtight European network. Let's not wait until we have to experience a cyber 9/11 to offer a common answer to those who want to undermine our democracies from the inside.

GS Mag: Finally, what actions do you intend to lead in terms of cyber security in the coming months?

Olivier Cadic: I am planning to propose a bill to simultaneously ban all Chinese investments in sensitive sectors, and the use of Chinese equipment and components in anything that comes under national security – such as cyber security.
Then, as part of the PACTE Law (Plan of Action for the Growth and Transformation of Businesses), I will make sure that no new mandatory regulations are introduced for businesses in matters of cyber security that would only serve to feed certificate-producing experts. I propose that small and medium businesses be encouraged to consider cyber security within the scope of a quality assurance toolkit built by our industrialists.
I've scheduled several trips through France to inspect our operational cyber defence system prior to the drafting of the 2019 budget reviews. ■■■

* Olivier CADIC, Senator for French citizens living abroad
Member of the Foreign Affairs, Defence and Armed Forces Committee (and cyber security questions rapporteur)
Vice-president of the Senate's Business Delegation
President of the France-Democratic People's Republic of Korea Study and Contact Group
Member of the Monitoring Group for the Withdrawal of the United Kingdom and the Rebuilding of the European Union
Member of the Monitoring Group for the Lancaster House Defence Treaty