

Interview: France warns of risk of war in cyberspace

June 1 2017, by John Leicester



The director general of the cyber defense agency known in France by its acronym, ANSSI, Guillaume Poupard, poses for a photographer during an interview with the Associated Press at his office in Paris, France, Thursday, June 1, 2017. The head of the French government's cyber security agency that was called in to investigate the hack of President Emmanuel Macron's election campaign says they have found no trace of a notorious Russian hacking group behind the attack. (AP Photo/John Leicester)

Cyberspace faces an approaching risk of "permanent war" between

states and criminal or extremist organizations because of increasingly destructive hacking attacks, the head of the French government's cybersecurity agency warned Thursday.

In a wide-ranging interview in his office with The Associated Press, Guillaume Poupard lamented a lack of commonly agreed rules to govern cyberspace and said: "We must work collectively, not just with two or three Western countries, but on a global scale."

"With what we see today—attacks that are criminal, from states, often for espionage or fraud but also more and more for sabotage or destruction—we are getting closer, clearly, to a state of war, a state of war that could be more complicated, probably, than those we've known until now," he said.

His comments echoed testimony from the head of the U.S. National Security Agency, Adm. Michael Rogers, to the Senate Armed Services Committee on May 9. Rogers spoke of "cyber effects" being used by states "to maintain the initiative just short of war" and said: "'Cyber war' is not some future concept or cinematic spectacle, it is real and here to stay."

Poupard said "the most nightmare scenario, the point of view that Rogers expressed and which I share" would be "a sort of permanent war—between states, between states and other organizations, which can be criminal and terrorist organizations—where everyone will attack each other, without really knowing who did what. A sort of generalized chaos that could affect all of cyberspace."

Poupard is director general of the government cyber-defense agency known in France by its acronym, ANSSI. Its agents were immediately called to deal with the aftermath of a hack and massive document leak that hit the election campaign of President Emmanuel Macron just two

days before his May 7 victory.

Contrary to Rogers, who said the U.S. warned France of "Russian activity" before Macron's win, Poupard didn't point the finger at Russia. He told the AP that ANSSI's investigation found no trace behind the Macron hack of the notorious hacking group APT28—identified by the U.S. government as a Russian intelligence outfit and blamed for hacks of the U.S. election campaign, anti-doping agencies and other targets. The group also is known by other names, including "Fancy Bear."

Poupard described the Macron campaign hack as "not very technological" and said: "The attack was so generic and simple that it could have been practically anyone."

Without ruling out the possibility that a state might have been involved, he said the attack's simplicity "means that we can imagine that it was a person who did this alone. They could be in any country."

"It really could be anyone. It could even be an isolated individual," he said.

Poupard contrasted the "Macron Leaks" hack with another far more sophisticated attack that took French broadcaster TV5 Monde off the air in 2015. There, "very specific tools were used to destroy the equipment" in the attack that "resembles a lot what we call collectively APT28," he said.

"To say 'Macron Leaks' was APT28, I'm absolutely incapable today of doing that," he said. "I have absolutely no element to say whether it is true or false."

Rogers, the NSA director, said in his Senate Armed Services hearing that U.S. authorities gave their French counterparts "a heads-up" before the

Macron documents leaked that: "We are watching the Russians. We are seeing them penetrate some of your infrastructure. Here is what we have seen. What can we do to try to assist?"

Poupard said Rogers' comments left him perplexed and that the French had long been on alert about potential threats to their presidential election.

"Why did Admiral Rogers say that, like that, at that time? It really surprised me. It really surprised my European allies. And to be totally frank, when I spoke about it to my NSA counterparts and asked why did he say that, they didn't really know how to reply either," he said.

"Perhaps he went further than what he really wanted to say."

Still, Poupard said the attack highlighted the cyber-threat to democratic processes. "Unfortunately, we now know the reality that we are going to live with forever, probably," he said.

Poupard said France suffers "about 20" very serious attacks each year—"very serious means that they shouldn't have happened and the impacts were very serious for the entire nation."

The attack on TV5 was a rare public example. In 2016, others targeted government administrations and big companies quoted on the benchmark French stock market index, the CAC-40, he said.

Pointing fingers at suspected authors is fraught with risk, because sophisticated attackers can mask their activities with false trails, he said.

"We suffered attacks that were attributed to China, that we think came from China. Among them, some came from China. China is big, I don't know if it was the state, criminals," he said. "What I am certain of is that among these attacks, some strangely resembled Chinese attacks but in

fact didn't come from China."

"If you start to accuse one country when in fact it was another country ... we'll get international chaos," he said. "We'll get what we all fear, which is to say a sort of permanent conflict where everyone is attacking everyone else."

© 2017 The Associated Press. All rights reserved.

Citation: Interview: France warns of risk of war in cyberspace (2017, June 1) retrieved 25 April 2024 from <https://phys.org/news/2017-06-france-war-cyberspace.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.