Article

11-06-2018 - 15:05
Reference No: 20180601STO04823

European Parliament

Cyber defence: "If one member state is weak, it could harm the others"

With Europe facing the risk of cyber attacks on civilian and military targets, MEPs are calling for more cooperation on cyber defence. We talked to Urmas Paet, the MEP in charge.

Cyber attacks can target a wide range of things, from our devices and e-wallets, to hospitals, power plants, air traffic control systems and the military. On 13 June MEPs adopted an own-initiative report calling on member states to step up their cyber defence capabilities and work together more closely.

Ahead of the plenary vote, we talked about why more needs to be done about cyber defence with report author Urmas Paet, an Estonian member of the ALDE group:

If you were to rate the EU's cyber defence on a scale from one to five, with one being excellent and five being a failure, how would the EU do and why?

Being a little bit optimistic, I would say two. The situation is not bad, but we can do better. The crucial issue is that cyber defence is the responsibility of member states. What the EU can do is to push them to cooperate better, to have more unified structures to combat cybercrime and cyber-attacks, to be prepared to act if needed; and to provide a platform for cooperation with Nato and third countries. Cybersecurity is international and interlinked so, if one member state is very weak, it could unfortunately harm all the others.

What role can the EU do regarding cyber defence?

The role of the EU is to encourage member states to establish similar structures - this would facilitate cooperation - and to encourage them to share knowledge and information, to look at the overall picture for Europe. For example, we are missing 100,000 or more experts or specialists who can deal with cyber-attacks.

Cyber defence is a natural part of European defence cooperation and a European defence union. Cyberspace has joined the classic military domains like air, sea and land.

When people talk about cyber threats, they usually think about misuse of their personal data or security of online payments. Your report focuses more on the military aspects of cyber defence. Are there crossovers for civilian use?

This report is mainly about cyber defence, but there is no clear-cut difference between cyber defence and cybersecurity. All modern systems in Europe use IT and computers. If there was a successful cyber-attack, for example, against a nuclear power plant, we all understand that there might be lethal consequences. We are at the boundaries between military and civilian, public and private. Last summer, British hospitals were hit and it was simply luck that nobody died. Possible cyber-attacks against air traffic control or rail systems are a serious risk.

We have to be ready to go on the offensive. It is not enough to simply defend, sometimes it's important to get active, for example, when you know where the attacks come from.

Should we expect cyber-attacks to become more common and do people need training in how to react?

The short answer is yes. On a personal level, everybody should think about their own IT or cyber "hygiene", how they behave on the internet. Governments and politicians have to admit the possible consequences of cyber-related risks. I really hope that awareness on all levels will increase.

Find out more

Press release on the plenary vote
Press release on the committee vote
Briefing: cyber attacks

Urmas Paet