CENTRE FOR EUROPEAN REFORM

Press release

Game over? Europe's cyber problem

by Camino Mortera-Martinez

9 July 2018

The European Union has woken up to the threat of cyber attacks, but it's coming late to the party. The longer it takes for the bloc to scale up its security efforts in this domain, the greater the risk it could face a cyber attack that could endanger not only the EU's economy but the physical security of its citizens. That's the conclusion of a new research paper 'Game over? Europe's cyber problem' by the Centre for European Reform which examines the EU's cyber vulnerabilities and how it could better tackle the online threat.

The EU's cyber security has been in focus since a series of high profile attacks hit Europe in 2017. The bloc has passed laws to update its capabilities for tackling cyber crime, such as online fraud. But its ability to counter disruptive and costly cyber attacks lags behind the capabilities of adversaries in places like Russia and North Korea. Obtaining evidence in cross-border cases is difficult. The EU is also unclear about which institutions should handle the cyber threat and where the resources should come from. The EU, NATO and US have also yet to agree on a strategy to deal with cyber attacks from state and non-state actors. NATO, which is likely to discuss cyber at its annual summit on July 11-12, recognised cyber space as a domain of operations akin to air, land and sea where it must defend itself in 2016.

While the EU cannot be expected to take responsibility for responding directly to cyber attacks, it could take some modest steps to boost security. The EU should improve how it shares electronic evidence, perhaps with a more efficient EU-US treaty, and also work more closely with technology companies to define and attribute cyber attacks. It should also encourage member-states to invest more in cyber security and better coordinate their responses, while the European Commission should consider setting up a dedicated task force to advise on cyber issues.

"*The EU knows that a cyber war is already happening, but does not know how to fight it. If it wants to be up to speed with the likes of Russia, China and the US, the EU needs to begin by understanding what a cyber threat is – and deciding what role it wants to play in countering it. Otherwise, the next major cyber attack could damage much more than a few hundred computers*," said Camino Mortera-Martinez, senior research fellow at the CER, who authored the policy brief.

Note to editors:
This paper is the second in a series for a Centre for European Reform/Open Society European Policy Institute commission on EU justice and home affairs policy, which is being led by former Italian prime minister Giuliano Amato. Its purpose is not to argue for particular policies, which the commissioners will do themselves in their final report, but rather to provide an overview of the state of the debate, and evidence for the commissioners to consider in their deliberations.

For further information on the policy brief and to request an interview with Camino Mortera-Martinez, please contact Nick Winning in the CER press office on pressoffice@cer.eu or + 44 (0) 20 7233 1199. The Centre for European Reform is a think-tank devoted to making the EU work better and strengthening its role in the world. The CER is pro-European but not uncritical. Follow us on: @CER_EU and the author on @CaminoMortera.