CENTRE FOR EUROPEAN REFORM

Europe's cyber problem

by Camino Mortera-Martinez

Cyber has become a buzzword in Europe. Just as both the migration crisis and the terrorist threat seem to have abated, a series of high profile cyber attacks in 2017, allegedly from both state and non-state actors, struck targets including national health systems, banks and electoral campaigns. These attacks have raised big questions about the European Union's attitude towards cyber security and its ability to deal with security breaches. The increasing incidence of online crime and the aggressive cyber tactics of countries like Russia and North Korea mean the bloc must raise its game in this area.

The EU's cyber security plans cover three different things: cyber crimes (like child pornography or online fraud); cyber attacks (like disrupting a city's transport network); and disinformation campaigns. Cyber crimes and cyber attacks sometimes overlap – like the 'Wannacry' ransomware attack attributed to North Korea, which blocked computers at large private companies and national service providers like the UK's National Health Service. All three cyber threats can come from both state and non-state actors. Russia was allegedly behind a major cyber attack in 2017 ('NotPetya'). Russian nationals have been indicted for meddling in the 2016 US presidential election. Drug dealers and other criminals make extensive use of the darkweb – websites which conceal users' identities. Terrorists are also using the internet to wage their own online jihad.

The EU has done well in dealing with more traditional cyber crimes, like identity theft. A 2013 directive harmonised national laws and penalties for cyber crimes and the EU will approve rules to tackle online fraud later this year. But obtaining digital evidence in cross-border cases is still difficult: member-states struggle to gain quick access to information stored in another EU country. This is even more problematic when evidence sits outside Europe. US tech companies like Facebook or Microsoft receive an average of 100,000 direct requests per year from EU governments. There is no law governing such requests so the whole system works on the assumption that internet companies will simply hand over information to law enforcement authorities. Such requests put firms in a difficult position, because they are also required to protect their customers' privacy.

This legal gap has already caused problems on both sides of the Atlantic. The US government is sueing Microsoft, which has refused to provide evidence stored on a server located in Ireland.

The EU is looking at ways to work around similar problems. The Commission is due to present a proposal on obtaining cross-border evidence within the EU in the spring. The EU is also considering options to make access to evidence in data form, stored outside the Union, easier for member-states. But better international co-operation is still needed, not only with the US but also with less obvious partners such as China or India – many large companies have outsourced their IT services there and co-operation with these countries is still patchy.

But Europe has a more urgent problem to solve: as state-sponsored cyber attacks increase all over the world, there is a gap between the EU's ambitions and its capabilities in cyber defence. Europe understands that a cyber war is already happening, but it does not know how to fight it. The EU's efforts to date have been few and far between. This is because there is little understanding in Brussels of what cyber attacks really are and how to deal with them, and, crucially, there is no consensus on who should be responsible for responding. Is it NATO, the EU, the national capitals, or a combination of the three?

Cyber security is a cross-border issue where the EU can certainly add value. The EU should find a common answer to the thorny question of what to do when a country launches a cyber attack against European interests. But, for now, the EU should focus on acquiring the knowledge and resources to build a robust cyber security strategy. At the moment, those resources are confined to a few member-states (like Estonia, France, the Netherlands and the UK). To deal with state-sponsored cyber attacks, the EU must begin by understanding what cyber is and what impact it has on all its policies – from trade, to crime, to the rule of law. Hackers have begun to exploit weaknesses for the purpose of insider trading; cross-border networks of paedophiles have been active in Europe for years; and disinformation campaigns targeting elections threaten European democracies and the rule of law. A good place to start understanding the impact of cyber in Europe would be for the next European Commission to set up a task force from all the relevant Commission departments and EU agencies to advise on cyber issues. The Council of Ministers already has a similar group. ENISA, the EU's cyber agency, located on the Greek island of Crete, is supposed to support member-states, but is too under-resourced and too far removed to play that role.

The cyber world, like the real world, is full of bad actors. The EU is currently at a disadvantage because these actors – unlike the Union – know what they are doing. The challenge for the EU is to learn how to beat these international cyber villains. Otherwise, a major cyber attack could endanger not only the EU's economy but also its democratic foundations.

Camino Mortera-Martinez
Research fellow, CER @CaminoMortera

CER in the press

Voice of America
13th March 2018
Expectations are growing for a tough response from Theresa May, said Ian Bond of the **CER**. "I think she'll be under a lot of pressure to show that the UK takes this very seriously. And that's partly because when she was home secretary, the British reaction to the murder of [Russian defector] Alexander Litvinenko in London was seen as rather weak."

The Irish Times
4th March 2018
Sam Lowe of the **CER** said that it would make sense for the UK to keep its focus on European links. "I'd question the logic of running into a trade deal with a [US] president who sees trade less as a means of achieving mutual prosperity and more an instrument of war."

The Financial Times
23rd February 2018
The centre-right coalition, including Silvio Berlusconi's Forza Italia and Matteo Salvini's Northern League, has been able to "ride a wave of discontent over the migration crisis", according to Luigi Scazzieri of the **CER**.

The Guardian
17th February 2018
"Theresa May is right to warn against letting ideology get in the way of security," said Sophia Besch of the **CER**. "But her message should be directed not just at the EU: she needs to say the same to Brexiters at home who categorically oppose the ECJ on ideological grounds."

The Guardian
7th February 2018
Jacob Rees-Mogg asked Steve Baker to "confirm that he heard from Charles Grant, director of the **CER**, that officials in the Treasury have deliberately developed a model to show that all options other than staying in the customs union are bad, and that officials intend to use the model to influence policy." Baker agreed with Rees-Mogg, although their effort to renew their attack on Treasury officials backfired when a recording emerged to show that supposed source Grant had not said the Treasury had developed such a model, instead making the more basic claim that the Treasury was determined to stay in the customs union.

The Express
6th February 2018
John Springford of the **CER** warned Britain may not have a clean break from the EU. Speaking on Channel 4 News, he said: "I think it is very likely that Britain will remain in the customs union for longer than the two years of transition, which everybody is talking about."