Global Counsel

Cyber-attacks: testing the EU's defences

Blog post by Senior Associate Franck Thomas, 3 August 2018

British retailer Dixons Carphone reported on Tuesday that ten million customers may have been affected by a cyber-attack. This is yet another example of the privacy breaches that are affecting every day operations of European companies. The Dixons Carphone incident follows other major cyber-attacks. The WannaCry and NotPetya attacks led to substantial financial losses for firms across France, Germany, Italy, Poland, Portugal, Spain and the UK.

Every new major cyber-attack demonstrates both the significant risks to the European economy and the borderless nature of the threat. The European Commission is understood to be planning to intervene after the summer break to address cybersecurity concerns over Chinese IT providers. But there are a number of things that suggest the Berlaymont will continue to struggle to make progress on this, and cybersecurity in general.

The first is the way cyber-attacks have blurred the line between law enforcement and national security with member states reluctant to cede sovereignty as a result. An example is the EU Agency for Network and Information Security (ENISA), created within the framework of the EU's Cybersecurity Act. In its negotiating position, the council jealously guarded its competences by setting clear limits on the role of ENISA to complement national agencies' activities. This is a sign of a wider problem.

Second is the way that fragmentation reduces access to innovative cybersecurity products in accordance with EU policy priorities such as privacy. Member states have developed their own certification schemes for cybersecurity products and services, creating a myriad of national markets. This not only has implications for the EU's single market but it makes it difficult for European companies to compete in the global cybersecurity market and take advantage of its rapid annual growth.

Third are member states' sometimes conflicted interests on China. Huawei has become a major provider in member states such as the UK, Germany and Spain. As pressure increases for 5G investment, major telcos across Europe have been signing commercial arrangements with Huawei to pilot 5G projects. Security concerns have been raised, most recently by the Huawei Cyber Security Evaluation Centre Oversight Board in the UK, but attempts by the commission to intervene will be frustrated by the patchwork of national policies and interests.

Since 2013, the commission has been taking incremental legislative steps to try and navigate some of these challenges. The Directive on Security of Network and Information Systems (NIS) in 2016 and the proposed EU's "Cyber Act" are important milestones. But the latter in particular bears the marks of constraints imposed by member states that are unlikely to disappear. Even where the commission has made progress, national governments are still moving slowly. In July, the commission triggered the first stage of an infringement procedure against 17 national governments which have not yet fully transposed the new EU rules into national law.

For telecoms operators and hardware providers assessing their political risk in Europe, it is clear that scrutiny of Chinese investment in telecoms networks is moving up the political agenda in the EU. For Huawei's competitors this may present an opportunity, but for many network operators it constitutes a growing risk. One of the consequences of the current uneven approach is that regulatory or political intervention – if it materialises – remains more likely to emerge from national authorities than the EU itself.

Coming back to Dixons Carphone, for the wider digital economy the concern persists that the EU's cyber defences remain a patchwork and that gaps remain which can be exploited by hostile states, terrorist groups and criminals. For now, the apparent urgency of this threat won't and probably can't be matched by a similar urgency in at the EU level.