How coherent is EU cybersecurity policy?


Recent security breaches at major companies and cyber-attacks such as the WannaCry ransomware attack have put cybersecurity firmly on the EU's political agenda. But how coherent an actor is the EU in the field of cybersecurity? Drawing on a recent study, **Andre Barrinha** *and* **Helena Farrand-Carrapico** *write that there remains a lack of cohesion in EU cybersecurity policy, with the main responsibilities in cybersecurity governance remaining with the member states. It remains to be seen whether recent events will encourage EU states to cooperate more closely on the issue or whether stronger responses will be pursued by individual states at the national level.*

Credit: ibmphoto24 (CC BY-NC-ND 2.0)

Cybersecurity is one of the European Union's top policy priorities. The EU 2016 Global Strategy – adopted by the European Council five days after the Brexit referendum – and, more recently, Jean-Claude Juncker's 2017 State of the Union address, clearly highlight the centrality that Europe's information networks and its critical infrastructures assume for the future of the Union.

In recent years, the panoply of objects and processes that have incorporated advanced computerised elements has grown rapidly to include not only laptops, tablets and smartphones, but also watches, cars, fridges, toys, classrooms and musical instruments – the so-called 'internet of things'. By 2021, the number of objects connected to the Internet is projected to be over 20 billion. The more connected we are, the more vulnerable to cyber-attacks we become.

Brussels has been very active in trying to develop an adequate response to cyber-attacks in the last few years. In 2013 it adopted its first EU Cybersecurity Strategy and, since then, it has invested in developing resilience, deterring cyber-attacks and increasing cooperation at national, European and international levels. An example of such investment is the adoption of the much-needed Network and Information Security Directive, which focuses on improving coordination and communication between the private sector, member states and EU institutions in case of cyber-crime attacks. In September 2017, the Commission also proposed a new set of measures, which among other initiatives, suggests the transformation of the European Network and Information Security Agency (ENISA) into the new permanent EU Cybersecurity Agency, with added competences in terms of training and certification.

Date originally posted: 2018-01-16

Permalink: http://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/

Blog homepage: http://blogs.lse.ac.uk/europpblog/

There are multiple motivations pushing the EU in this direction: the implementation of its Digital Single Market strategy, the progressive centrality of hybrid threats (another area of significant recent activity within the EU) and the increasing rise in cyber-crime, just to name a few. Among the most recent and concerning attacks, there is the Uber data breach where the email addresses and phone numbers of 2.7 million Uber clients and drivers were stolen, and the hacking of 3 billion Yahoo accounts. To this we can add recent high profile cyber-attacks such as WannaCry and NotPetya, alongside the increasing use of cyber-tools by nation-states to disrupt or attempt to disrupt elections and other electoral processes. These incidents have contributed to the approval of the above-mentioned EU-led initiatives.

The coherence conundrum

Addressing cybersecurity issues demands the institutional flexibility that to a large extent goes against the EU's bureaucratically heavy and institutionally sedimented default *modus operandi*. Dealing with cyberspace means that multiple agencies, institutions and even countries may be called to intervene to address a single incident. Furthermore, the divide between internal and external security or between the public and private sector are not always clear in cyberspace, and that is no different with the EU.

As we argue in a recent study, similar to other security fields, the EU equates policy success with increased levels of coherence: coherence across EU institutions (horizontal) and between them and member states (vertical). That can be seen from an institutional perspective – institutional coordination – but also from a deeper shared understanding of what cybersecurity is and how it should be approached. This need for coherence is recognised by the EU in multiple instances, from European Commission communications to the EU Global Strategy.

Within cybersecurity, the fact that the EU's 2013 strategy was drafted as a combined effort between DG Home Affairs, DG Connect, and the European External Action Service (with an active contribution from DG JUST) is quite revealing of this need for a coherent cross-sector approach. However, in practice its implementation has been broadly divided along three main lines – cybercrime, critical information infrastructure protection, and cyberdefence – each with its own budgets, set of policies and agencies.

The major paradox in the EU's cybersecurity architecture, and the main cause for its lack of cohesion, results from the mismatch between needs and responses in the relationship between Brussels and its member states. Although the EU recognises the transnational character of cyber-related threats, it also acknowledges that the main responsibilities in cybersecurity governance should remain with member states, giving itself more of a light-touch coordination role. The measures adopted since then do not really address that balance.

At the centre of this mismatch are issues of trust (both vertical and horizontal) and divergent policy priorities between member states (in 2017 there are still member states without a cybersecurity strategy). States are often afraid of sharing information that could compromise the economic interests of their companies or, given the significant secrecy that still surrounds cybersecurity operations, of sharing too much operational information. It is also the case that certain countries, particularly the smaller member states, have neither the know-how nor the interest in the field, whereas larger member states do not want to be controlled by Brussels when it comes to setting their own cybersecurity priorities.

The EU cybersecurity architecture is – as in many other areas – complex and multi-layered. It is also a still largely incipient area in which actors and institutions are still shaping their practices and priorities. The Cybersecurity Package that was presented last September is, in that regard, a sign of some maturation by the European Union in this field. If the notion of cybersecurity as a progressively important policy area has been maintained since 2013, it is now more visible than it was four years ago, due to the damaging consequences that cyber-attacks can have on our way of life, be it ransomware attacks on hospitals or the attempt to use information networks to influence electoral processes. Whether this will lead to additional coherence in terms of the way the EU approaches cybersecurity, or, on the contrary, to more ad hoc, nation-based responses, remains to be seen.

Please read our comments policy before commenting.

Note: This article draws on the authors' recent paper in the Journal of Common Market Studies. The article gives the views of the authors, not the position of EUROPP – European Politics and Policy or the London School of Economics.

Date originally posted: 2018-01-16

Permalink: http://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/

Blog homepage: http://blogs.lse.ac.uk/europpblog/

About the authors

André Barrinha – *University of Bath*
André Barrinha is a Lecturer in International Security in the Department of Politics, Languages and International Studies at the University of Bath.

Helena Farrand-Carrapico – *Aston University*
Helena Farrand-Carrapico is a Senior Lecturer in Politics and International Relations, and Co-Director of the Aston Centre for Europe at Aston University.

Date originally posted: 2018-01-16

Permalink: http://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/

Blog homepage: http://blogs.lse.ac.uk/europpblog/