EPRS
European Parliamentary Research Service

At a glance
31/03/2014

EU approach to cyber-security

Fighting cross-border crime affecting information and communications networks (cybercrime) is a priority in the EU's internal security strategy. To counter so-called cyber-attacks in a borderless space, the European Union and the Council of Europe have drawn up common strategies, operational measures and legislation.

Crimes beyond national borders

National security issues

The internet has opened up information flows, but has also made possible a range of new transnational crimes. Criminals can threaten the security of nation states and/or the civil liberties of their citizens. Organised criminals exploit cyberspace to steal money or to commit fraud. They also break into computer networks in order to steal data or business secrets or simply to destroy documents. Cybercrime can damage essential infrastructure on which society depends, affecting health, safety, or security, but also infrastructure vital for economic or social well-being (such as power plants, transport networks and government networks).

International protection

The first global instrument aimed at deterring action directed against the confidentiality, integrity and availability of computer systems, networks and computer data was the 2001 Budapest Convention promoted by the Council of Europe. This legal instrument aims to facilitate detection, investigation, criminalisation and prosecution of such activities at both domestic and international levels. This Convention has been supplemented by a Protocol on acts of xenophobia and racism committed through computer systems.

The EU strategic and operational approach

The EU has set out its approach against cybercrime with actions developed at strategic, legislative and operational levels.

At strategic level, the 2009 Stockholm Programme includes a number of measures to counteract cybercrime. Europol's 2013 Serious and Organised Crime Threat Assessment (SOCTA) considers cybercrime to be an ever-increasing threat to the EU in the form of large-scale data breaches, online fraud and child sexual exploitation, while profit-driven cybercrime is becoming an enabler for other types of criminal activity.

The Justice and Home Affairs Council of 6-7 June 2013 designated cybercrime as one of nine EU priorities in the fight against serious and organised crime between 2014 and 2017. The Council Conclusions of 25 June 2013 on the EU Cybersecurity Strategy help to shape the EU's general strategy in this domain.

At operational level, the creation of the European Network and Information Security Agency (ENISA) in 2004 was followed more recently with the creation of the European Cybercrime Centre (EC3). Hosted by Europol, EC3 is intended to become the main point in the EU's fight against cybercrime, by supporting Member States and the European Union's institutions. It started its activities in January 2013. Cybercrime has also become one of the priorities of the EU mutual evaluation mechanism on fighting organised crime: all Member States' capabilities in this field will be examined in the seventh round of evaluations, starting in late 2014.

The "Cyber-attacks" Directive

At legislative level, several measures against cybercrime have been adopted, such as the 2011 Directive on combating the sexual abuse and sexual exploitation of children and child pornography (to have been transposed into national law in the Member States by 18 December 2013). Particularly relevant is the 2013 Directive on attacks against information systems, which replaces a 2005 Council Framework Decision and has

Author: Francesca Ferraro, Members' Research Service
European Parliamentary Research Service
140775REV1

to be transposed before 4 September 2015. This Directive sets out minimum rules concerning definitions of criminal offences in this field and sanctions for those found guilty of them.

The main crimes defined in the Directive are illegal access to information systems, illegal interference with systems or data, and illegal interception of data transmissions. In particular, stricter criminal sanctions are required for so-called "botnet" attacks, in which a large number of computers are infected in order to control them remotely, performing tasks automatically without users' knowledge. Large-scale cyber-attacks can thus spread rapidly over the internet. Penalties can also be imposed on legal persons, such as companies, in case of criminal acts from which they benefit. The Directive, however, aims to take a balanced approach in order to prevent possible over-criminalisation.

Operational cooperation and legislation

The Directive also improves operational cooperation between Member States' national law enforcement services and relevant EU agencies (Eurojust, Europol and its European Cybercrime Centre, as well as ENISA). Member States have to respond within eight hours to an urgent request related to a cyber-attack. EU agencies will conduct threat assessments and strategic analyses of cybercrime on the basis of the information submitted by Member States. All such activities have also to comply with existing EU legislation on privacy and electronic communication and data protection, which is an essential part of the comprehensive approach to effectively counteracting cybercrime.

The "NIS" directive

With the goal of shaping a new EU cybercrime strategy, the European Commission proposed, in February 2013, a directive concerning measures to ensure a high common level of network and information security (NIS) across the Union. Due to the interconnectedness of network and information systems, significant disruptions of these in one Member State can affect other Member States and the Union as a whole. The resilience and stability of network and information systems as well as the continuity of major services are essential for the smooth functioning of the internal market, in particular for further development of the digital single market. This directive would require all Member States to set up Computer Emergency Response Teams (CERTs) and to adopt national NIS strategies and cooperation plans. As a major innovation, the proposed directive requires obligatory notification by market operators of incidents which have a significant impact on the security of core services.

The European Parliament voted in March 2014 on amendments to the proposed directive, based on the report of the Committee on Internal Market and Consumer Protection (rapporteur Andreas Schwab, EPP, Germany). The new legislature will then have the task of securing agreement with the Council on the final shape of the directive.

Cybercrime and the impact of the Snowden revelations

The EU strategy on cyber-security will also be influenced by the outcome of the European Parliament's inquiry into the revelations in the wake of the Edward Snowden affair. According to the report adopted in plenary in March 2014 based on the inquiry of the Committee on Civil Liberties, Justice and Home Affairs (rapporteur Claude Moraes, S&D, United Kingdom), the EU's cyber strategy should be extended to cover malicious state behaviour and to strengthen IT security and resilience of IT systems. According to the Committee's report, Europol's mandate should be enhanced in order to allow it to launch its own investigations following suspicions of a malicious attack on network and information systems. The EU should, however, avoid amendments to Article 32 of the Council of Europe's Cybercrime Convention. The latter makes trans-border access by law enforcement authorities to servers and computers located in other jurisdictions legally possible without recourse to multilateral agreements and other instruments of judicial cooperation. Moreover, by December 2014, the Commission, ENISA and Europe's standardisation bodies should develop minimum security and privacy standards and guidelines for IT systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data and the integrity of all IT systems. It encourages the United States to accede to the Council of Europe's Convention for the protection of individuals with regard to Automatic Processing of Personal Data (Convention 108), as it has acceded to the 2001 Convention on Cybercrime, thus strengthening the shared legal basis for transatlantic relations in this field.