At a glance
April 2016

European Parliament

Cyber-attacks: Visible danger, invisible enemy

The advance of information and communication technologies (ICT) has created numerous opportunities for human development, and reshaped the ways in which our societies communicate, work or learn. However, our reliance on internet-based platforms can also be a source of vulnerability, exploited by criminal networks for financial or political aims.

Landscape of cyber threats

Research into the cost of cybercrime and threat assessments reveals a gloomy picture. In 2013, the number of victims of cybercrime reached 1 million per day – ten times more than can fit into Wembley stadium – with almost 12 people falling victim to cybercrime every second. According to Europol estimates, victims of cybercrime lose around €290 billion each year worldwide, making internet crime more profitable than the global trade in marijuana, cocaine and heroin combined, while cybercrime is becoming more aggressive and confrontational. The analysis of the scope of existing threats, allows to distinguish three main categories of cyber threats: cybercrimes (i.e. computers used to commit crime, or targeted for crimes such as theft of money or intellectual property), cyber espionage (i.e. cases of intrusion into networks of other countries or companies, whereby computers are used to extract large amounts of information for military, governmental or economic gains), and cyber conflict (i.e. computers used for military purposes).

Cyber strategy of the European Union

To ensure that EU citizens can fully enjoy the benefits stemming from new internet technologies, the Member States agreed in 2013 on the Cybersecurity Strategy of the European Union. The document – a cornerstone of the EU's actions in this area – focuses on five strategic priorities: achieving cyber resilience by developing better prevention and response capabilities, drastically reducing cybercrime, developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP), developing industrial and technological resources for cyber security, and establishing a coherent international cyber-space policy. The aims of the strategy were addressed further in policy-specific documents, including the renewed Internal Security Strategy, the Digital Single Market Strategy, the Cyber Defence Policy Framework and Council conclusions on Cyber Diplomacy. Implementation of the strategy is distributed among the EU institutions, agencies, and the Member States, who bear primary responsibility for the security of citizens.

Building cyber-resilience

In the context of the Digital Agenda for Europe, the EU focuses, among other things, on strengthening the resilience of its systems and internal capacities. As the delivery of public services (e.g. transport, financial, healthcare and energy systems) increasingly depends on internet-based platforms, the need to ensure their secure functioning is growing too. To minimise the risk of organised criminal groups or foreign governments exploiting their vulnerabilities, and to strengthen citizens' trust in the online environment, the Network and Information Security (NIS) Directive aims to improve Member States' national cybersecurity capabilities and enhance cooperation between public and private sectors. To achieve this objective, the Directive requires critical sectors and key internet service providers to adopt risk management practices and report major incidents to the national authorities. It also contains a set of government-specific requirements, including the establishment of Computer Emergency Response Teams – equivalent to a combination of ambulance and fire brigade operating in cyberspace – and strengthening cooperation among a network of round-the-clock contact points. Several Member States have also developed and started implementing national security strategies, with guidance and support from the EU Agency for Network Information Security (ENISA).

This note has been prepared for the European Youth Event, taking place in Strasbourg in May 2016.

EPRS | European Parliamentary Research Service
Author: Patryk Pawlak, **Members' Research Service**
PE 581.964

Fighting cybercrime

The European Union differentiates between three major groups of cybercrime: crimes specific to the internet (e.g. attacks against information systems), online fraud and forgery (e.g. identity theft, phishing, spam and malicious code), and illegal online content (e.g. child sexual abuse material, incitement to racial hatred, incitement to terrorist acts). To deal with these challenges, the EU has set up the European Cybercrime Centre (EC3) as a part of Europol in The Hague. The EU also strongly supports the principles for fighting online crime as set out in the Council of Europe's Budapest Convention on Cybercrime, and engages in capacity-building by providing funding for projects designed for law enforcement. In December 2015, the European Commission launched the EU Internet Forum to counter terrorist content and hate speech online through, among other things, further engagement with internet companies. Currently, the international response to cyber jihadism is organised around three main pillars: constraining the use of the internet by jihadi organisations, strengthening de-radicalisation efforts and limiting access to funding.

Strengthening cyber-partnerships

Recognising the importance of engagement with key international partners as a way to promote EU political, economic and strategic interests, the EU adopted Council conclusions on Cyber Diplomacy in February 2015. They elaborate several priority areas for the EU’s cyber diplomacy: ensuring that citizens receive the same level of protection of their human rights in cyberspace as they do in the physical space; preventing international conflicts by developing norms of behaviour and application of existing international law in cyberspace; promoting internet-governance mechanisms ensuring that the internet remains an open, secure and safe space for all; as well as building capacities in developing countries in order to ensure that they also benefit from new technologies. The EU pursues these priorities through engagement with international organisations (e.g. United Nations, Council of Europe, Organization for Security and Co-operation in Europe) and bilateral cyber dialogues with China, India, Japan, South Korea, and the United States.

Developing cyber defence

One of the most contested elements in the discussion about cyberspace is the issue of cyber conflict or cyber war, and the applicability of existing international law. The concept of cyber defence itself is very often misused by the public and media to describe instances of a high-profile cyber-attack. The EU's own Cyber-Defence Policy Framework focuses on: supporting the development of Member States' cyber-defence capabilities related to CSDP; enhancing the protection of CSDP communication networks used by EU entities; promoting civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector; improving training, education and exercise opportunities; and enhancing cooperation with relevant international partners. With regard to the ongoing processes, the issues that require further discussion concern developing a joint EU response against coercive cyber operations, the practicalities of applying existing international law to cyber conflicts, and development of Confidence-Building Measures in cyberspace.

Existing and future challenges

Despite the fact that governments and the private sector have made progress in threat analysis and intelligence, and improved their capabilities to counter threats posed by online criminal networks or third countries, there are still a large number of challenges that need to be overcome with regard to:

- Implementation of policies, including Member States' own capabilities and cooperation with the private sector and other stakeholders;
- Mainstreaming cybersecurity-related issues into debates at high political levels in order to generate additional political energy and to ensure that cybersecurity concerns are taken on board across all areas, in line with the 'whole-of-government' approach;
- Raising awareness about cyber threats and responses among citizens and other stakeholders; and
- Ensuring the right balance between security and civil liberties concerns. Whether this objective is achieved, will partly depend on the outcome of the ongoing debate about the use of encryption tools. The ban on encryption and its implications for the privacy of over 3 billion Internet users worldwide have galvanised privacy advocates.