

Brussels, 30th September 2010

Commission to boost Europe's defences against cyber-attacks

The European Commission today unveiled two new measures to ensure that Europe can defend itself from attacks against its key information (IT) systems. A proposal for a Directive to deal with new cyber crimes, such as large-scale cyber attacks, is complemented by a proposal for a Regulation to strengthen and modernise the European Network and Information Security Agency (ENISA). The two initiatives are foreseen by the [Digital Agenda for Europe](#) and the Stockholm Programme to boost trust and network security (see [IP/10/581](#), [MEMO/10/199](#) and [MEMO/10/200](#)). Under the proposed Directive, the perpetrators of cyber attacks and the producers of related and malicious software could be prosecuted, and would face heavier criminal sanctions. Member States would be also obliged to quickly respond to urgent requests for help in the case of cyber-attacks, rendering European justice and police cooperation in this area more effective. Strengthening and modernising ENISA would also help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber-security challenges. Both proposals will be forwarded to the European Parliament and the EU's Council of Ministers for adoption.

Commissioner Cecilia Malmström, in charge of Home Affairs, said: "Crime is finding new ways. With the help of malicious software, it is possible to take control over a large number of computers and steal credit card numbers, find sensitive information or launch large-scale attacks. It is time for us to step up our efforts against cyber crime, also often used by organised crime. The proposals we are putting forward today are one important step, as we criminalise the creation and selling of malicious software and improve European police cooperation".

Commission Vice-President for the Digital Agenda, Neelie Kroes, said "Making every European digital will only happen if citizens feel confident and safe on-line. Cyber threats know no borders. A modernised European Network and Information Security Agency will bring new expertise and foster exchanges of best practice in Europe. Our EU institutions and governments must work ever closely together, to help us understand the nature and scale of the new cyber-threats. We need ENISA's advice and support to help design efficient response mechanisms to protect our citizens and businesses online".

While Europe is engaged in taking full advantage of the potential of network and information systems, it should not become more vulnerable to disruptions caused by accidental or natural events (like submarine cable breaks) or through malicious actions (like hacking or other cyber-attacks). These could be based on, for example, increasingly sophisticated tools which hijack large numbers of computers and manipulate them simultaneously as an army of robots on the internet ("botnets") without their owners' knowledge. These infected computers can later be used to carry out devastating cyber-attacks against public and private IT systems, as happened in Estonia in 2007 where most online public services, as well as government, parliament and police servers were made temporarily inoperative. The number of attacks against information systems has risen steadily since the EU first adopted rules on [attacks against information](#) systems in February 2005. In March 2009, the computer systems of government and private organizations in more than 100 countries were attacked by a network of compromised computers which extracted sensitive and classified documents. In this instance again, malicious software created 'botnets', networks of infected computers that can be remotely controlled to stage a coordinated attack.

The package proposed by the Commission today will strengthen Europe's response to cyber disruptions. The Commission's proposal on cybercrime builds on rules that have been in force since 2005, and introduces new aggravating circumstances and higher criminal sanctions that are necessary to fight more effectively the growing threat and occurrence of large scale attacks against information systems.

Moreover, it would pave the way for an improvement of cooperation between the judiciary and the police of the Member States, introducing the obligation for Member States to make better use of the existing 24/7 network of contact points by treating urgent requests in a specified timeframe.

Finally, the proposed Directive would provide for the establishment of a system to record and trace cyber attacks.

Reinforced cooperation across countries and industrial sectors

To help co-ordinate Europe's response, the Commission is proposing a new Regulation to strengthen and modernise the European Network and Information Security Agency ([ENISA](#)), which was first established in 2004. This would reinforce cooperation across EU Member States, law enforcement authorities and the industrial sector. ENISA will play an important role in boosting trust, which underpins the development of the Information Society, by enhancing the security and privacy of users.

Under its new mandate, ENISA would engage EU Member States and private sector stakeholders in joint activities across Europe, such as cyber security exercises, public private partnerships for network resilience, economic analyses and risk assessment and awareness campaigns.

A modernised ENISA would have greater flexibility and adaptability and would be available to providing EU countries and institutions with assistance and advice on regulatory matters.

Finally, to respond to the increased intensity of cyber security challenges, the proposed Regulation would extend ENISA's mandate for five years and gradually increase its financial and human resources. The Commission proposes that ENISA's governance structure would also be strengthened with a stronger supervisory role of the Management Board, in which the EU Member States and the European Commission are represented.

Background

The proposed Directive on attacks against information systems repeals the Council Framework Decision 2005/222/JHA. Member States would have an obligation to comply with the new Directive on cyber crime, and transpose it into national legislation within two years from its adoption at the latest.

ENISA was created in 2004 and its current mandate expires in March 2012. It is now proposed to extend it by 5 years. This proposal for a Regulation was preceded by a broad process that included an evaluation of the Agency, recommendations by its Management Board, two public consultations and an impact assessment including a cost/benefit analysis

For further information

Homepage of Cecilia Malmström, EU Commissioner for Home Affairs:

http://ec.europa.eu/commission_2010-2014/malmstrom/index_en.htm

Homepage of Neelie Kroes, Commission Vice-President for the Digital Agenda

http://ec.europa.eu/commission_2010-2014/kroes/index_en.htm

Information Society Newsroom

http://ec.europa.eu/information_society/newsroom/cf/menu.cfm

[MEMO/10/459](#)

[MEMO/10/463](#)