SUMMARY  As modern economies have embraced information and communication technologies, they have become vulnerable to cyber attacks. Such attacks are mounted by a wide variety of actors, some state-affiliated or enjoying state support. The methods and tools used are however largely the same.

Cyberspace is an open environment, which poses a serious challenge to policy-makers. Its governance is shared by governments, the private sector and civil society. Cyber security efforts thus require the involvement of various stakeholders, in particular since the private sector owns the vast majority of hardware, software and information infrastructure.

Despite limits to its competence, the EU has sought to become a platform for common cyber security efforts by the Member States. It has tackled network security issues and set up procedures for the protection of critical infrastructure in Europe. Moreover, the EU has established minimum rules concerning criminal offences and facilitated law enforcement cooperation through Europol, including with the newly established European Cybercrime Centre.

The Parliament has closely followed the Commission’s actions and commented in depth on its major policy documents. In 2013, it co-decided the Directive on attacks against information systems.

In this briefing:
- A growing space for cyber attacks
- A challenge to governments
- Cyber attacks: who and what
- EU laws and policies
- European Parliament position
- Main references

A growing space for cyber attacks

Over the past few decades, the digital revolution has brought global connectivity to an entirely new level. Every day, around 294 billion e-mails are sent and 5 billion phone messages exchanged. By the end of 2013, an estimated 2.7 billion people will be using the internet, i.e. more than one-third of the world’s population.1 Information and communication technologies (ICT) are crucial for virtually all modern services, both civilian and military. Electrical grids, transport and logistics are but a few networks for which the digital infrastructure is just as important as the physical one.

Convenient as it is, such growing reliance on ICT entails an increasing risk of cyber attacks. These attacks may target individuals or businesses, or even a country’s critical infrastructure – such as energy or water supply. The consequent disruption may have a serious impact on the health, security or economic well-being of citizens, and/or the functioning of government.

The number of incidents covered under the broad umbrella term ‘cybercrime’2 has been increasing constantly around the world. Whereas, at any time, an estimated 150 000 computer viruses are in circulation, almost as many computers are infected each day. As the popularity of smartphones and tablets is growing, so is the number of viruses designed specifically for them.
Cybercrime "victimisation" surveys in 21 countries have revealed that the number of both individual and institutional victims is significantly higher than that for "conventional" forms of crime.3

The internet is very important in the daily life of European households. According to Eurostat, around half of its users in the EU buy goods or services online (53%), use social networking sites (52%), or bank online (48%). Such widespread use of the web exposes them to cybercrime. Indeed, 12% of internet users across the Union have experienced online fraud, and 8% – identity theft. Moreover, 13% have been unable to access online services due to cyber attacks.

Eurostat data shows that such incidents do have an impact on consumers' behaviour online. In addition, they entail considerable costs for EU citizens, businesses and governments (see table 1).

Table 1: Global cost estimates for cybercrime infrastructure

<table>
<thead>
<tr>
<th>Costs</th>
<th>US$ million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus software*</td>
<td>3 400</td>
</tr>
<tr>
<td>Software patching</td>
<td>1 000</td>
</tr>
<tr>
<td>Clean-up by internet service providers</td>
<td>40</td>
</tr>
<tr>
<td>Clean-up by users*</td>
<td>10 000</td>
</tr>
<tr>
<td>Generic cyber-defences of firms</td>
<td>10 000</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>400</td>
</tr>
</tbody>
</table>

Source: Measuring the Cost of Cybercrime / Anderson et al.

NB The authors of this study for the UK Ministry of Defence emphasise the need to treat the estimates with great caution; Figures in bold are scaled up from estimates for the UK alone. Figures are for 2010, except those marked * which are for 2012.

According to the study from which the estimates in the table are taken, expenditure on defences against cybercrime is significantly more than society’s losses to it, and many times more than criminals gain from it, thus imposing a disproportionate burden on society.

A challenge to governments

Governments tackling cyber threats meet with numerous challenges which derive from the nature of the worldwide web. The anonymity and freedom of movement in the virtual world are unparalleled. Websites can easily be moved outside a given jurisdiction to a location with different laws or unwilling to cooperate in law enforcement. While cybercrime knows no borders, governments certainly do.

Moreover, the internet has been set up as an open system, resistant to external attempts at control and not designed to be secure.4 Whereas governments have been trying to increase their role in cyberspace, the web remains largely unregulated or self-regulated. Public authorities share internet governance with the private sector and civil society (in a model known as "multi-stakeholder governance"). In addition, almost all software and hardware, entire networks and, in many cases, even critical infrastructure, are owned by private firms. When cyber incidents occur, the contribution of informal expert networks is often more important than top-down state-governed processes.5

When the EU addresses cyber threats, it has to face these challenges, as well as some specific limitations of its own. While Member States (MS) rely heavily on computer technology and interconnected networks, they differ considerably in terms of security and defence capacities. They are not equally willing to cooperate on these issues, which could create serious problems in case of a large-scale attack targeting more than one of them. The EU's options for action are limited, with MS eager to retain competence in areas such as criminal law, and, even more so, in national security and defence. Despite this, efforts have been made at EU level to enhance the protection of individuals, networks and systems through better prevention, preparedness and response to cyber attacks.
Cyber attacks: who and what

Forms of cyber attacks
Whereas cyber attacks may be perpetrated by various (often non-identifiable) actors, the means used are largely the same. The following methods and tools are among the most common:

- "Hacking": illegally accessing systems by exploiting software vulnerabilities,
- "Phishing": deceiving internet users so as to lead them into divulging personal information (so-called "spoof sites" may be used for this which imitate legitimate websites of, e.g. banks), and
- The use of "malware" – unintentionally installed software which collects and transmits personal information. They include Trojans (programs which steal information or provide access), viruses (which replicate and contaminate other programs), and worms (able to replicate and move between systems).

These means are used not only to attack individual computers, but also in large-scale attacks. To this end a so-called "botnet" may be set up, which is a group of infected and remotely controlled computers. Botnets serve to spread malware, spam or to conduct a Distributed Denial of Service (DDoS) attack whereby a stream of requests is sent to a specific web server, leading to its serious slowdown or blockage. Various estimates point to millions of computers tied up in botnets around the world.

The cyber black market
Malware, personal information and credit card details are offered on cybercriminal fora (websites or internet relay chat (IRC) channels). Skilled hackers identify vulnerabilities. This knowledge is used to create "toolkits", which are then sold to, or stolen by, the actual perpetrators of cyber attacks who may not have equivalent skills. In 2011, IT security company Bitdefender reported that China and Russia produced over half of the world's malware (see figure 1).

Perpetrators
Little is known of those who carry out cyber attacks. Depending on their motivation, different categories may be identified, such as hackers, criminals, terrorists, foreign intelligence or the military. Such clear-cut typology however ignores the real nature of the cyber-criminal world, which is composed of loosely connected networks and alliances of actors shifting identities. It is further complicated by speculation about states tolerating the illegal activities of organised crime and non-affiliated hackers, and making use of them to mount easily deniable attacks against other states. Moreover, qualifying an attack as an act of war or terrorism, a crime or civil disobedience may be a matter of interpretation or political stance, as illustrated by the varied perceptions of the activities of the hacker group Anonymous.

Given the intricacies of the cyber world, it may be argued that improving resilience of systems and networks against all kinds of cyber attacks is more important than acting against specific categories of attacker. The EU cyber security policy seems to follow such an "all-hazards" approach.

EU laws and policies
At first, the EU perceived cyber security to be a secondary issue related to the growing dependence on ICT. That situation changed in the aftermath of major terrorist attacks in...
the US and EU and, even more so, following a major cyber attack on Estonia in 2007.

The two strands of EU cyber security
Whereas the relevant EU legal and policy framework has been fragmented, two main policy areas in the field of cyber security may be identified. On the one hand, actions have been taken to enhance network resilience to potential attacks and incident response capacities. Relevant measures go under headings such as Network and Information Security (NIS), Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP). On the other hand, the EU has addressed cybercrime and cyber terrorism from the law enforcement perspective.

It is important to note that these two policy areas tend to overlap with numerous policy documents including elements of both.

Cyber war and cyber defence have, on the contrary, rarely been addressed at EU level, arguably due to limits of competence in Common Foreign and Security Policy (CFSP). MS tend to cooperate within NATO instead, to improve their cyber-defence capacities. It is argued that such a "division of labour", with NATO working on military and the EU on civilian aspects of cyber security, is the only approach likely to be successful.7

Strategy documents
Raising the level of cyber security in the EU was one objective of the Internal Security Strategy adopted in 2010. The Strategy provided for setting up an EU cybercrime centre by 2013. Moreover, it stated that every MS and EU institution should have a well-functioning Computer Emergency Response Team (CERT). Reporting cybercrime incidents was considered crucial, as well as creating alert platforms and networks of contact points. In this regard the need to develop the European Information and Alert System (EISAS) was stressed. Furthermore, the Strategy promoted exercises in cyber incident response at EU level.

The 2010 Digital Agenda for Europe – a flagship initiative under the Europe 2020 Strategy – stressed the need for trust and security in the digital society. It promoted widening the network of CERTs in the EU, including setting up a CERT for the EU institutions.

The 2013 Cyber Security Strategy of the EU was built on the premise that when enhancing cyber security, web access for all as well as its multi-stakeholder governance should be preserved. The Strategy set the following strategic priorities:

- Achieving cyber resilience (including further development of the European Public-Private Partnership for Resilience)
- Drastically reducing cybercrime
- Developing cyber defence policy and capabilities, while avoiding duplication with NATO activities
- Developing the industrial and technological resources for cyber security, including promoting a Single Market for cyber security products
- Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

Enhancing network resilience
Network and information security
The concept of Network and Information Security (NIS) was born out of security considerations in the process of building the Information Society. It has been developed as part of the EU’s economic agenda, with
the stated objective of contributing to the smooth functioning of the Internal Market. In 2004, the European Network and Information Security Agency (ENISA) was set up; its mandate was redefined by a new basic Regulation in 2013. ENISA’s role is to contribute to a high level of NIS across the EU through supporting MS, EU institutions and the business community. This includes preparatory work for EU legislation in the field.

At present cooperation between MS on NIS issues is on a voluntary basis, with no mechanism to guarantee effective information sharing at EU level. This is regarded as a major disadvantage especially since MS vary considerably in terms of NIS capabilities. The Commission intends to address this issue through its proposal for a directive on a high common level of NIS – an Internal Market measure based on Article 114 TFEU. The proposal would establish NIS-related obligations for MS, new cooperation mechanisms, and security requirements for market operators and public administrations.

Critical Infrastructure Protection (CIP)
CIP was first discussed in the context of the fight against terrorism. The European Programme for Critical Infrastructure Protection (EPCIP) was set up, leading to the adoption of a 2008 Directive. This established a procedure for identification by MS of infrastructure to be designated as European critical infrastructure. However, the Directive stressed that the primary and ultimate responsibility for protecting such infrastructure remains with MS and its owners and operators. The Directive focused on the energy and transport sector.

The 2007 cyber attack on Estonia created a momentum for advancing CIP, and in particular Critical Information Infrastructure Protection (CIIP), as a general security issue. The Commission's 2009 Communication on Critical Information Infrastructure Protection – promoting a European multi-stakeholder governance framework coordinated by the EU – set up a detailed CIIP Action Plan. The Commission's approach was broadly endorsed by the Council. In 2011 the Commission assessed the Action Plan's implementation. While the conclusions were mostly positive, the need to improve global coordination of cyber security efforts was stressed.

Combating crime
While many cyber threats go beyond the reach of law enforcement, the EU has attempted to promote a common approach to cybercrime. Its limited competence in this area allows for the approximation of national criminal law, and enhancing operational cooperation amongst MS.

Tackling attacks against information systems
In 2013 a Directive was adopted under Article 83 TFEU to replace the 2005 Council Framework Decision on attacks against information systems. Its aim is to establish minimum rules on the definition of criminal offences and sanctions with respect to attacks against information systems. The main crimes defined in the Directive are illegal access to information systems, illegal system interference, illegal data interference, and illegal interception. Harsher penalties have been provided for crimes committed within the framework of a criminal organisation, causing serious damage (which includes the use of botnets) and committed against a CIIP system. Furthermore, the text aims at facilitating the prevention of such offences and improving cooperation between national authorities.

The European Cybercrime Centre
The European Cybercrime Centre (EC3) hosted by Europol was launched in January 2013. The EC3 is supposed to become a focal point in the fight against cybercrime in the EU. Its role consists of supporting operational cooperation between MS (including joint cybercrime investigations) and analysing cyber-threats in the EU. EC3’s mandate covers cybercrime:

- committed by organised criminal groups
- causing serious harm to its victims (e.g. sexual exploitation of children)
Cyber security in the European Union

- affecting critical infrastructure and information systems in the EU.

European Parliament position

In recent years the Parliament and individual Members have shown avid interest in cyber security issues, as illustrated by numerous parliamentary questions and a series of resolutions.

In its 2012 resolution on the ISS, the EP welcomed the prioritisation of the fight against cybercrime, and stressed the importance of prevention. Moreover, it urged MS to ratify the Budapest Convention.

Another 2012 resolution included numerous proposals for the development of CIP. The EP called, among other things, for an expansion of the scope of the 2008 Directive on European critical infrastructure, to include the ICT sector and financial services.

In yet another 2012 resolution on a digital freedom strategy in EU foreign policy, the EP took a stance on the more general issue of Internet governance. It defended its open and participatory nature and advocated the inclusion of all stakeholders in any debate on internet regulations. Moreover, the Parliament called for the EU to play a leading role in the development of norms of behaviour in cyberspace. For the EP, digital security and digital freedom are both essential and cannot replace one another.

The Parliament co-decided the 2013 Directive on attacks against information systems and is currently discussing the Commission proposal for a directive on a high common level of NIS across the Union.

Main references


Disclaimer and Copyright

This briefing is a summary of published information and does not necessarily represent the views of the author or the European Parliament. The document is exclusively addressed to the Members and staff of the European Parliament for their parliamentary work. Links to information sources within this document may be inaccessible from locations outside the European Parliament network. © European Union, 2013. All rights reserved.

http://library.europarl.wordpress.com

Endnotes


2 There are various definitions of cybercrime which differ in scope. In most cases however, the term seems to be used in its broad sense to cover crimes unique to electronic networks, i.e. attacks against information systems, traditional forms of crime, such as fraud committed online, content-related offences (e.g. electronic dissemination of child pornography or incitement to racial hatred), and copyright offences. This briefing focuses on cyber security measures addressing actions falling under the first two categories. The term “cyber security” is used broadly to cover not only technical and organisational measures used to protect networks and systems (e.g. firewalls and incident reporting), but also relevant criminal laws and law enforcement. Issues such as cyber war, cyber weapons and cyber espionage are not addressed in the briefing, and the related problem of cyber defence only to the extent necessary to understand the main lines of EU laws and policies concerning cyberspace.

3 Comprehensive study on cybercrime / UNODC, 2013, p 28.


