European Commission

Citizen's summary

Cybersecurity in the European Digital Single Market

What is cybersecurity and why does it matter?

The internet and web have made many activities simpler, cheaper and more convenient: banking and shopping; staying in touch with friends and family and organising our social lives; and doing everyday administration. They have also enabled an explosion of innovative new businesses and services. However, this on-line and connected world is not without risks, including identity theft, data fraud, and other types of cybercrime as well as the misuse of digital information across geographical and jurisdictional boundaries.

Cybersecurity refers to the degree to which the networks, computers and programs we use, and the data contained therein, are protected against unauthorised access and use, and the measures taken to achieve this. Breaches of cybersecurity cost money and can result in reputational damage, psychological trauma, frustration, and a loss of privacy. Beyond these private risks, there are also risks to national security, which is increasingly dependent on a safe and resilient cyberspace. Cybersecurity is therefore a priority for business and political leaders around the world, as well as for citizens.

What is the link between cybersecurity and the Digital Single Market?

The European Commission's Digital Single Market priority is intended to remove barriers which prevent citizens and businesses from benefitting from all of the opportunities presented by the internet and digital technologies. But it can only succeed in delivering these benefits if organisations and individuals have confidence that these technologies are secure.

Why did the Commission consult the High Level Group of Scientific Advisors?

European Commission Vice President Andrus Ansip asked the SAM High Level Group of Scientific Advisors (SAM HLG), January 2016, to provide scientific advice that would inform the revision of the EU's cybersecurity strategy, as well as the further development of the Digital Single Market strategy. The SAM scientific opinion is acknowledged as an important input substantiating the approaches set out in the recently published (September

2017) *Communication from the European Commission to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"*.

On what does SAM base its scientific opinion?

The advice in this Scientific Opinion is based on a detailed analysis of publicly-available scientific literature as well as close consultation with the scientific community and a wide range of stakeholders representing industry, consumers, NGOs and so on. The High Level Group of scientific advisors also placed at the centre of their opinion the need to uphold important principles in the Charter of Fundamental Rights of the European Union and others which are particularly pertinent to cybersecurity including transparency, duty-of-care towards customers and shared responsibility.

What are the main elements of the SAM Scientific Opinion?

The Scientific Opinion makes the following recommendations for policy actions to make it easier and safer for people and businesses to operate online in the EU:

- **Maintain state-of-the-art cryptographic standards** and avoid 'backdoors' that bypass normal security processes. The opinion also recommends establishing a duty of care principle towards consumers that would help to ensure that systems (in their electronic hardware and software) are well maintained and have fewer technical vulnerabilities
- **Empower citizens** through 'context tailored' digital identities so that: each of us is only asked for the data necessary to secure an online transaction; we are given more choice and control over our personal data; and we are sufficiently aware and equipped to act responsibly and to take protect ourselves online. Also, promote citizens' data-literacy and engagement in shaping the future of the digital world.
- **Strengthen Europe's strategically important cybersecurity industry**, and ensure an adequate supply of well-trained cybersecurity professionals
- **Improve coordination and information-sharing across Europe** on cyber-incidents and responses, and ensure adequate technical expertise in European bodies. The Opinion also calls for a global cybersecurity governance framework, in which the EU would play a leading role.

The Opinion also makes a number of important observations on issues pertinent to cybersecurity policy but on which there was no clear expert consensus. These included highlighting the complex nature of cybersecurity, a scarcity of reliable scientific studies in an otherwise large body of academic literature, the need to ensure that EU legislation can keep abreast of the latest threats and opportunities in cybersecurity.

Contact for further questions: ec-sam@ec.europa.eu
Website of the Scientific Advice Mechanism: ec.europa.eu/research/sam

Download of the report:
http://www.test.ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf#view=fit&pagemode=none

Research and Innovation