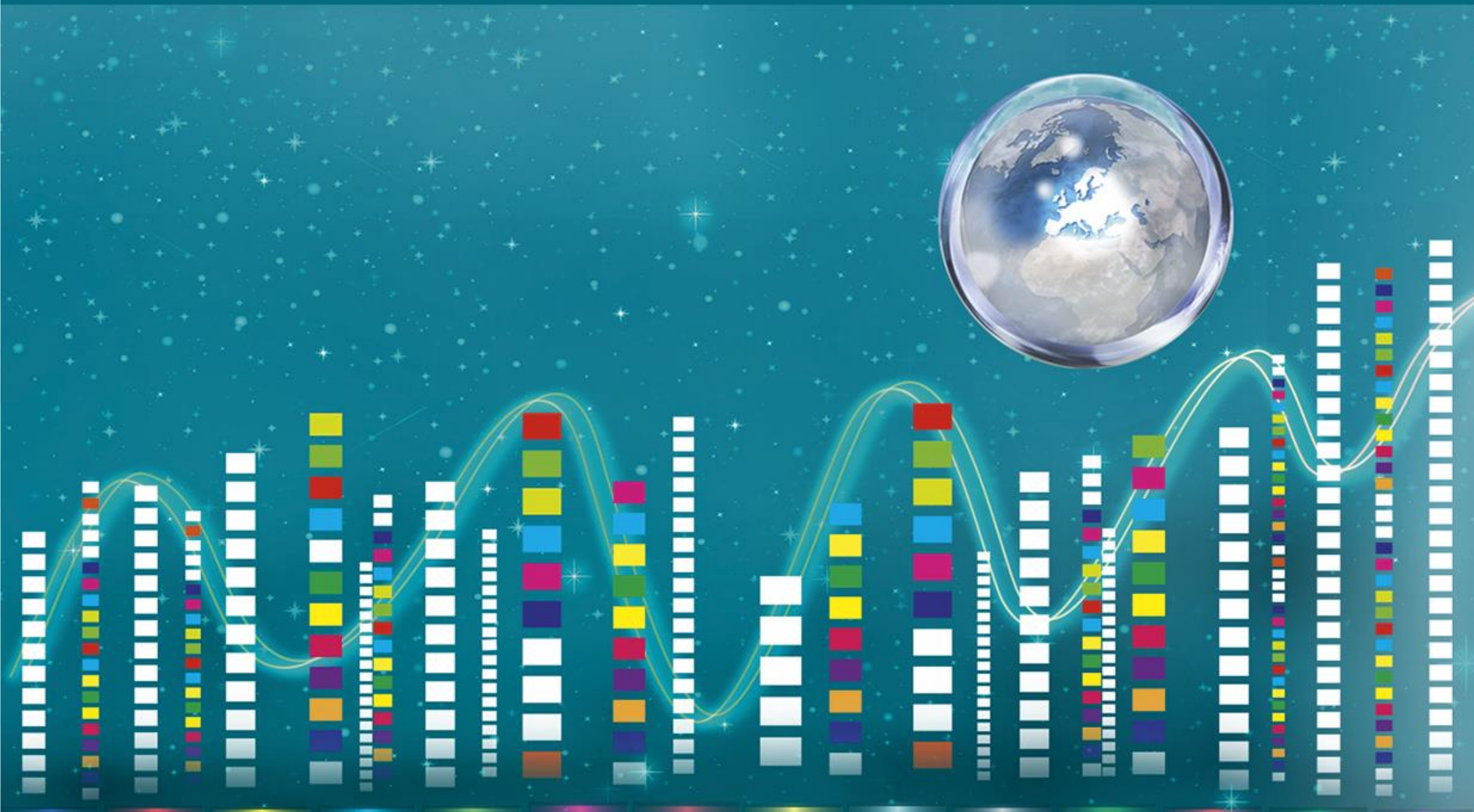
European Commission

Foresight

Continuous Cyberwar

Targeted scenario N°4

Glimpses of the future from the BOHEMIA study



[

Research and Innovation

EN

Continuous Cyberwar **- Targeted scenario N°4**

European Commission
Directorate-General for Research and Innovation
Directorate A Policy Development and Coordination
Unit A.3 Horizon 2020 Policy and Foresight
Contact   Nikolaos Kastrinos
E-mail   nikolaos.kastrinos@*ec.europa.eu*
RTD-PUBLICATIONS@ec.europa.eu
European Commission
B-1049 Brussels

Manuscript completed in March 2018

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2018

PDF   ISBN 978-92-79-81126-5   Doi 10.2777/512174   KI-KI-02-18-406-EN-N

Cover page image: © Lonely # 46246900, ag visuell #16440826, Sean Gladwell #6018533, LwRedStorm #3348265, 2011; kras99 #43746830, 2012. Source: Fotolia.com.
Icons: © UN Sustainable Development Goals Source: http://www.un.org/sustainabledevelopment/news/communications-material/

EUROPEAN COMMISSION

Continuous Cyberwar
Targeted scenario N°4

Glimpses of the future from the BOHEMIA study

Directorate-General for Research and Innovation

2018

About BOHEMIA

BOHEMIA is a foresight study (contract N° Contract PP-03021-2015) designed specifically to support the preparation of the next framework programme.

The study put forward policy recommendations for the next framework programme, based on a foresight processes involving scenario development, a Delphi survey and an online consultation.

As part of its recommendations, the study identified 19 likely future scenarios with disruptive implications and associated priority directions for EU research and innovation.

The full range of the results of the study is available at https://ec.europa.eu/research/foresight

Targeted scenario N° 4

Continuous Cyberwar

Summary

With the rapid growth of Internet of Things, cybersecurity hacks proliferate, putting citizens and infrastructures at risk. EU governments strengthen collaboration with citizens and industries to build up a response based on both social participation and cutting-edge technologies.

UN Sustainable Development Goals (SDGs) most relevant to this scenario:

16
PEACE, JUSTICE AND STRONG INSTITUTIONS

The scenario

It is now 2040. Technology devices connected to internet are central to EU economy and permeate citizens’ daily live. Energy facilities (power grid, nuclear facilities), transport networks, banks, public administrations, hospitals, production facilities, and security and defence systems are dependent on digital technologies. Given the huge amount of interconnections on which EU citizens’ and governments rely, cyber security is an area of major policy concern.

EU governments collaborate and work closely with citizens and industries to develop innovative data security solutions, implement cutting edge technologies and design backup plans to protect systems and data from cyber-attacks from both home and abroad. Some EU cities have suffered major disruption of services due to cyberattacks on critical infrastructures, and cyber-attacks on satellites have caused major disruption to communication and banking services. All EU governments have adopted advanced and differentiated Cyber Incident Response Plans since many years. To support structures under attack, a Cyber-Security Emergency Response Fund is now available at EU level.

Quantum computing has made major contributions to security but it has not managed to quench on-line fraud and cybercrime. Quantum encryption, even if theoretically unbreakable, does not protect against manipulative social engineering techniques. And of course there is quantum decryption. There is a one-in-two chance that some fundamental public- crypto key is broken by quantum-computing.

Important societal strategies have been developed to increase cybersecurity and strengthen resilience to cyberattacks. People's awareness, knowledge and motivation to be secure online have been strengthened as media have been drawing attention to the issue. Community initiatives to promote security by design in local infrastructures and systems have flourished, and companies and public administrations have been developing protocols and implementing training programmes. Social cooperation and effective warning mechanisms that rely on users’ feedback help in identifying fake news and quickly spot fraudulent websites and new forms of cybercrime. Users know the degree of confidentiality of everything they share online, can assess the level of security of websites, their devices and passwords of their virtual accounts, and respect clear behavioural guidelines when navigating social networks, chatting or paying online.

Relevance for Europe

The internet is so critical to so many functions in the social, economic and political spheres that it needs to be assured as a safe space.

Fast developing internet and ICT provide an infrastructure to new crime that is difficult but urgent to detect and tackle. For example “Crime as a Service (CaaS)” on-line platforms serve new organized crime syndicates but also challenge ‘traditional’ organised crime organisations by commodifying crime.

As the Internet grows, it is expanding not only to new users but to entirely new devices: the “Internet of Everything” means an increased risk of “cyber attacking everything”. Tens of billions of “Internet of Things” devices are expected to be connected to the internet by 2020, but cyber security is not yet fully prioritised in their design. The cybersecurity market is on the rise: research reports valued the global cybersecurity market at $64 billion in 2011, $78 billion in 2015 and $120 billion in 2017.

Contribution towards the UN Sustainable Development Goals (SDGs)

As the internet is a key infrastructure for societies, safeguarding against cyber-attacks will make an important contribution to SDG 16 to promote just, peaceful and inclusive societies, as they rely on ICT and web-connections. Better management and control of the cyber world are crucial for reaching the target of “significantly reducing illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime”.

Implications for EU policy

Cybersecurity combines the interests of a number of EU policies: security policy, justice and home affairs; telecommunications, networks and the digital single market are but some of the most relevant. Cyberattack is a specific priority crime threat for Europol. Potential policy actions to foster cybersecurity range from fostering cyber education and training, encouraging attention on data protection, fighting against disinformation campaigns and fake news, to promoting agreements for secure-by-design devices.

Cybersecurity calls for the collaboration across all sectors and actors. Cyber resilience can be enhanced through design improvements and certification (e.g. cybersecurity certification schemes, with EU-level standards), and the promotion of skills for cyber hygiene and awareness[1] in the public.

It is equally important to create a legal framework to detect, trace and prosecute cyber criminals and elaborate effective mitigation. While such legal framework should be provided at national level, it is important that the EU foster information exchange and cooperation among cyber-police services in different member states, supported by common standards, infrastructures, databases and harmonised response plans.

Future Directions for EU R&I policy recommended by the public consultation

- **Tools for monitoring, evaluating and responding to threats**
- **Methods and practices, including co-design approaches, for awareness raising on cybersecurity and cyber hygiene.**
- **Research for thorough understanding of the evolving cyber-threats**
- **Research on blockchains and quantum based solutions**
- **Regulations, agreements and partnerships for monitoring, evaluating and responding to threats**
- **Developing a common cybersecurity certification framework for technological devices and web-services**
- **Research to decrease digital exposure of critical infrastructure**
- **Understanding links between internal and external security**

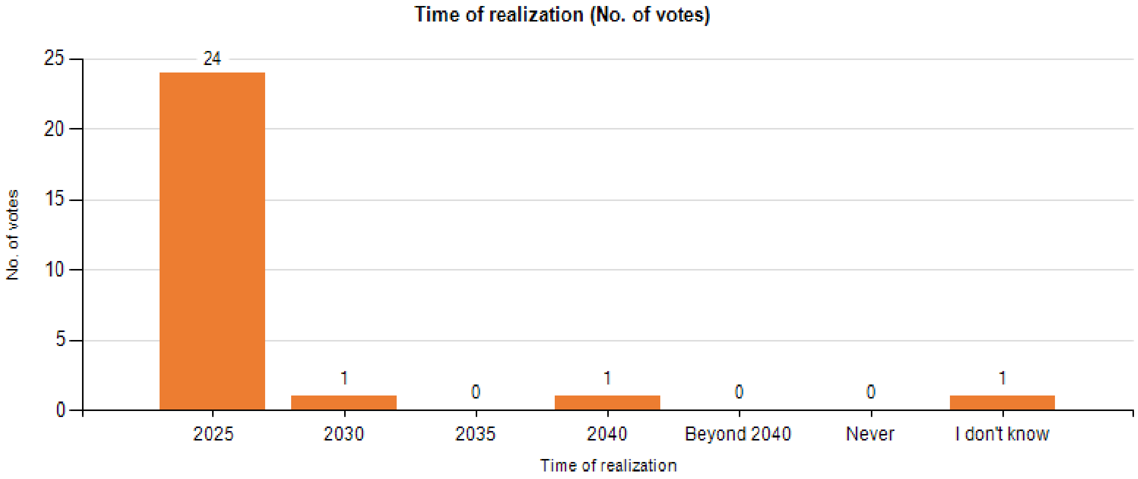
[1] Joint Communication to the EP and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN/2017/0450 final

Annex: Relevant Data from the Delphi Survey

The Delphi survey of the BOHEMIA study asked experts about the time of realization of 143 statements about the future, and about the relevance of Research and Innovation for that realization, or about the relevance of the realization for Research and Innovation policy. The experts were asked to justify their judgements with arguments. The whole data set has been published and can be found at: https://ec.europa.eu/research/foresight

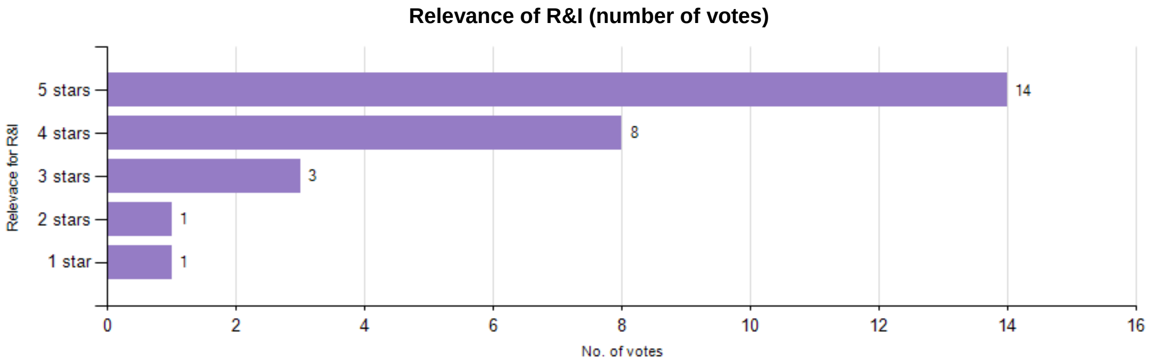
This annex includes the parts of the data set that are relevant to this scenario.

A large EU city (population greater than 500 000) sees a major, prolonged disruption of services (longer than 48 hours) due to cyberattacks on critical infrastructures



Number of respondents: 28

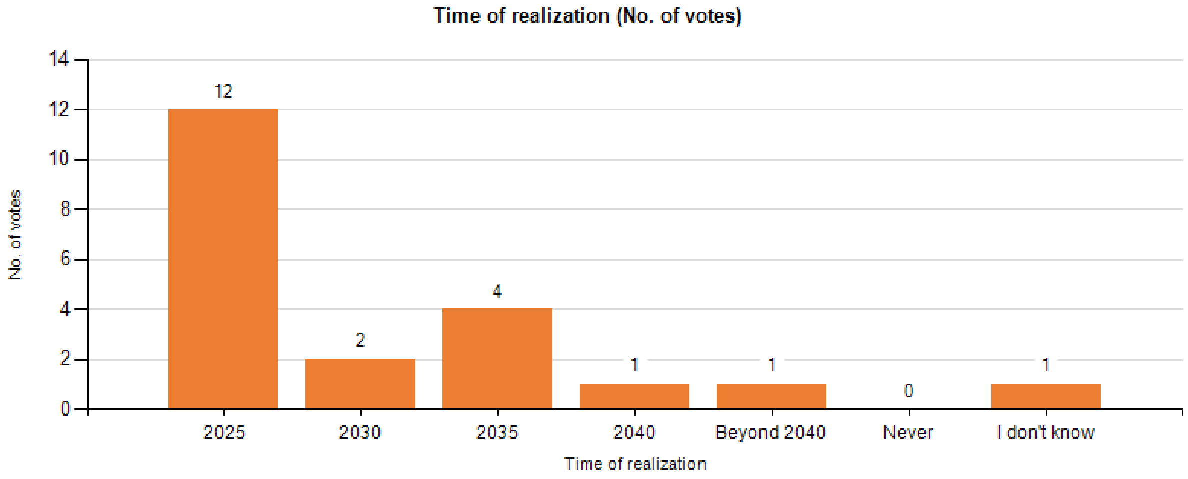
Arguments regarding the time of realization	**No. of votes**
Cyber crime is on the rise. Power supply is a major single point of failure in modern societies and will thus be the primary target in hybrid warfare.	23
US National Security Agency chief said in 2016 that cyberattacks on critical infrastructures are a matter of when, not if.	18
In December 2015, a presumed Russian cyber-attacker left an important city in Ukraine without power for 6 hours, but the attack could have rendered the system permanently inoperable.	8
Sleeper threats need to be addressed that can be autonomously initiated at specified times or conditions.	5
In May 2017, the NHS of the UK was hobbled. Too many people w/power to do MUCH more to prevent and respond effectively to attacks continue to exercise 'wilful blindness' of their vulnerabilities	5
There are lots of cyberattacks, but most of them do not cause that much harm.	2



Average: 4.22 **Dispersion:** 1.08

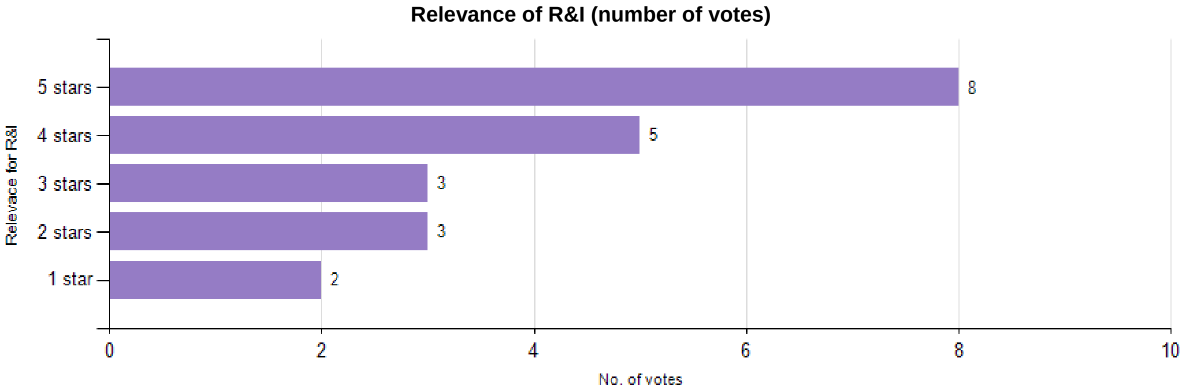
Arguments regarding the relevance of R&I	**No. of votes**
Cyber security and infrastructure security need joint (policy) approaches and a lot of knowledge.	24
There must be experiments, scenarios and risk management on EU and on city level to be prepared.	19
We need more research and foresight on the changing nature of power relations in the world (nations, networks, criminal groups, new great powers, international structures, etc.).	10
A "security" culture should be introduced in the workplace, in addition to safety.	9
Research into resilience at various levels (e.g. critical infrastructure, social) is needed to deal with cyber attacks, as a successful attack is inevitable.	2

A successful physical or digital attack on low orbital space satellites causes one major system (global positioning systems, telecom, security) to fail completely for an extended period of time



Number of respondents: 22

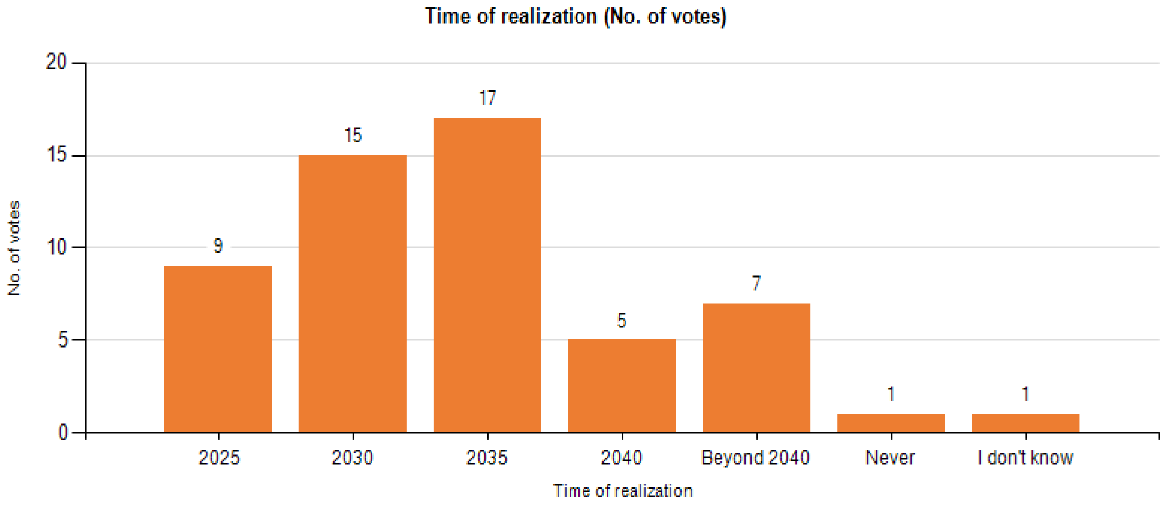
Arguments regarding the time of realization	**No. of votes**
Digital attacks have already taken place, but the failures of these systems have not been made public.	10
Open or subtle threats to space satellites and major IT systems - rather than direct attacks - may well become a part of the security repertoire of hostile states.	9
Physical attacks are not very feasible, as there are only a few states with the capabilities to attack in low orbital space now. But, in the future, there might be private actors with these capabilities, too.	7
Space related infrastructure is a vital part of the Critical Infrastructures in the EU. They are a primary target for digital attacks.	6
Killer CubeSats are thinkable that can disable other satellites and become increasingly likely as launch costs decrease and fall within reach of non-state actors.	5
A rogue state or non-state actor or a crime cartel in command of $billions could blackmail major states with demands that can be readily met if anti-sat technologies have been deployed, demonstrated.	4
A 'Ransomware' scenario is highly probable.	3
The most damaging North Korean threat would be the capacity to destroy key satellites that could not be rapidly replaced.	2



Average: 3.67 **Dispersion:** 1.82

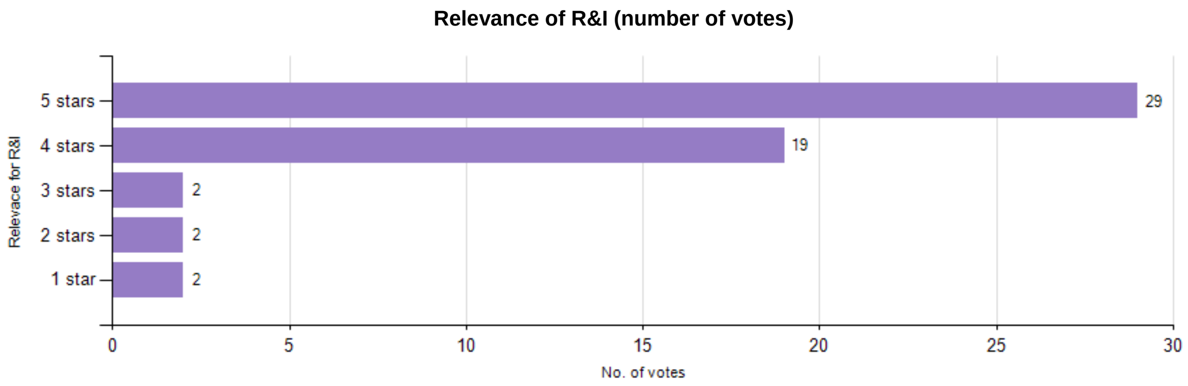
Arguments regarding the relevance of R&I	**No. of votes**
The EU needs coherent and integrated risk identification, analysis and assessment tools and procedures in order to monitor evolving threats.	20
Experiments on response to such an event have to be performed and international reactions have to be tested in order to be prepared. Political coordination is necessary.	11
RI policy in this area must be guided by an understanding of the fundamental uncertainty, both political and technological, that we face. Mitigating evident risks is only a part of the picture.	8
The prospect of very large constellations of small satellites multiplies the threat level dramatically. Precise tracking of these objects and knowing that threats may exist among them requires R&D.	3
AND risk definition. A risk for some is an opportunity for others (good and bad)	1

Quantum cryptography is used by three-quarters of EU corporations for secure digital communication



Number of respondents: 55

Arguments regarding the time of realization	No. of votes
So far, 'quantum speed-up' has not been unambiguously achieved with any prototype quantum computer.	29
Timing is difficult to predict but it is quite likely that quantum computing will one day ignite the major and fast transition in cryptography.	25
Quantum computing endangers the current public-key cryptographic systems, which raises issues about wide-scale adoption.	20
Post-quantum mathematical cryptography will persist for less-demanding applications. Quantum cryptography will co-exist with it, will improve, become cheap and ubiquitous, but slowly.	11
Quantum cryptography is just a beginning for other quantum applications.	9
Quantum cryptography exists for key distribution. Post-quantum crypto will address key management and keep systems secure.	9
Basic quantum computing security technologies exist today, so it should not take too long.	2



Average: 4.31 **Dispersion:** 1.00

Arguments regarding the relevance of R&I	**No. of votes**
Develop quantum-resistant cryptography to deal with the advent of quantum computers.	43
Increase the efficiency of information exchange in quantum key distribution.	34
Investing in R&I is important. Limited availability of these new capabilities create a major imbalance in global market.	14
Critical and ground-breaking advances in strong cryptography usually happen in academia. Investment in research is therefore important.	13
China, U.S., S. Korea, Japan, UK, EU as well as Google, Microsoft, IBM and others are making major investments in quantum computing. Accelerating research results with industry academia partnerships	6
In parallel work on possible impacts should be done	5

With the rapid growth of Internet of Things, cybersecurity hacks proliferate, putting citizens and infrastructures at risk. EU governments strengthen collaboration with citizens and industries to build up a response based on both social participation and cutting-edge technologies

Studies and reports

Publications Office