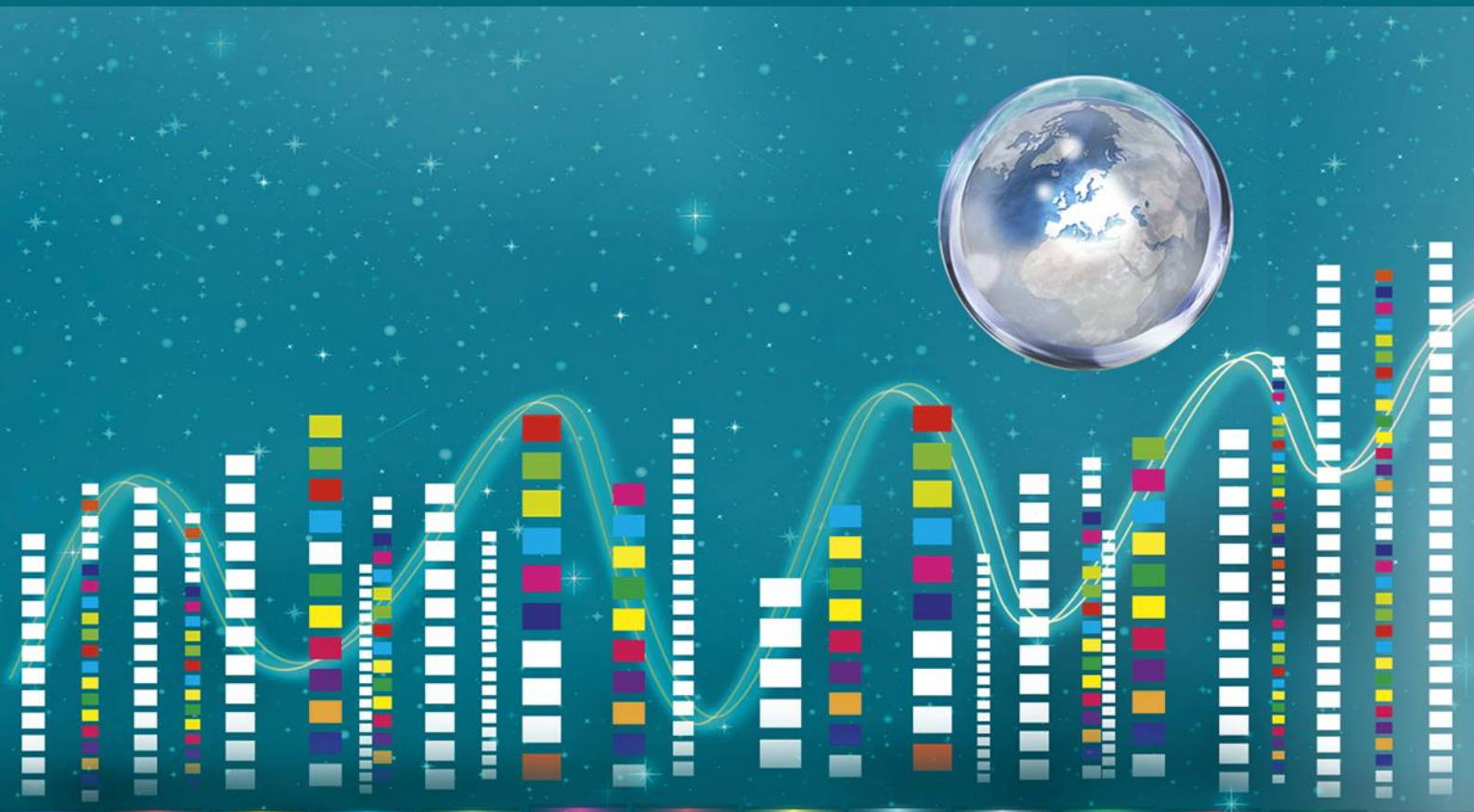
European Commission

Foresight

ICT-based Security Defence

Targeted scenario N°9

Glimpses of the future from the BOHEMIA study



[

Research and Innovation

EN

***ICT-based Security Defence* - Targeted scenario N°9**

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

Luxembourg: Publications Office of the European Union, 2018

PDF ISBN 978-92-79-81127-2 doi: 10.2777/383920 KI-02-18-407-EN-N

EUROPEAN COMMISSION

ICT-based Security Defence
Targeted scenario N°9

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° 9

ICT-based Security Defence

Summary

It is 2040. Globalisation and ICT solutions have changed the nature of threats faced by the EU. A combination of preventive and response measures is implemented in coordination by security and defence forces with the aid of computers. The role of the anticipatory crime units is rising, together with the diffusion of unmanned aerial vehicles and military robots with Artificial Intelligence features. These are used in external military actions as well as to secure national territories in cooperation with security units.

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

The scenario

It is 2040. Security and defence forces have strengthened their cooperation and share intelligence and technological solutions. ”Asymmetric” risks such as terrorism, weapons of mass destruction, state failure and organised crime dominate the security debate. The virtual world has joined the physical as a playground for conflict. Attackers and criminals – both state and private actors – move easily across territories and use technologies to do harm and amass profits. In this new landscape, access to communication data, artificial intelligence and robotics are crucial to protect the EU. Data collected through smart devices is used for crime prevention as well as for international investigations. Security and defence forces cooperate and exchange data and technologies, facilitating investigations and law enforcement across the Union and beyond.

Anticipatory crime units are now active in every city. They use data analytics to prevent crimes and direct police operations. These units also track criminals often outside their territory in missions organised jointly with armed forces. The role of unmanned aerial vehicles and robots with Artificial Intelligence features is increasing in military external actions as well as in securing national territories, in cooperation with security units. These semi-autonomous defensive systems are used to defend critical infrastructures from new threats such as swarm attacks by unmanned drones. Such systems monitor and secure more than half of the EU’s land, sea, and air borders, sensitive places.

The United Nations Convention on Conventional Weapons had been debating a possible ban on autonomous weapons since 2017, but no agreement has been reached. In Europe, human decision-making is mandatory when it comes to the use of weapons. European countries apply the EU framework on privacy protection which regulates data gathering and analysis by the police and private actors. The tension between liberty and security is high, and EU citizens have built movements and networks to improve the data-related regulations and management.

Most advanced cities combine the deployment of continuous surveillance and defence robots in public spaces with inclusive policies directed to reinforce the sense of community and the access to social and cultural services. Participatory and transparent decision-making process related to security has proved to be key for promoting the acceptance of the measures and the collaboration of citizens protecting their community.

Relevance for Europe

Geopolitical uncertainty combined with globalization and technological trends call for ensuring security at international level, which is increasingly interlinked with internal security. The global scale of organised crime, including terrorist organisations, facilitated by ICT, requires innovative security measures and policies. Predictive policing, artificial intelligent and autonomous weapons are domains where solutions are sought. These are likely to form the fields of technological competition, but also raise important ethical concerns.

ICT-based security measures, both for internal policing and external defence, can inspire a sense of safety in citizens, strengthening the Union. However, as ICT advances, it will be available also to criminals and ‘enemies’, so that it remains uncertain whether developing these technologies for policing and military purposes increases security in reality. Addressing the root causes of security threats remains a major challenge. Questions will arise on whether a de-humanisation of security pursued through autonomous weapons and robots is in line with the EU’s foundations related to its peace-building mission.

Contribution towards the UN Sustainable Development Goals (SDGs)

Addressing the security issue is key to ensure that the developments contribute, rather than undermine, the achievement of SDG 16, to promote just, peaceful and inclusive societies. Better management and control of the data to increase security can help reach 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". In addition, it could contribute to "substantially reducing corruption and bribery in all their forms", with the ultimate aim of "reducing all forms of violence and related death rates everywhere". However, depending on how ICT based security is applied, it could also threaten the achievement of SDG 16, making war easier and crueller.

Implications for EU policy

EU home affairs, justice, and security and defence policies are closely relevant to this scenario. Better cooperation across Commission departments and among EU member states authorities is challenging as well as much it is needed. Of particular importance are the EU cooperation on security (CFSP), the regulation on data to secure privacy protection along with the establishment of a clear framework for enforcement of related laws, and the standardisation of data, data mining and utilisation protocols around the EU. There is a strong need for technology assessment, including questions of decommissioning autonomous weapons, and an important industry policy agenda too. However, also ethical considerations and social acceptance on autonomous weapons, defence robots and in general about replacing humans with Artificial Intelligence when it comes to security measures are crucial to define a consistent policy at the EU level. Along with technological developments, policy can focus also on inclusion, social affection and social awareness to mitigate security risks.

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

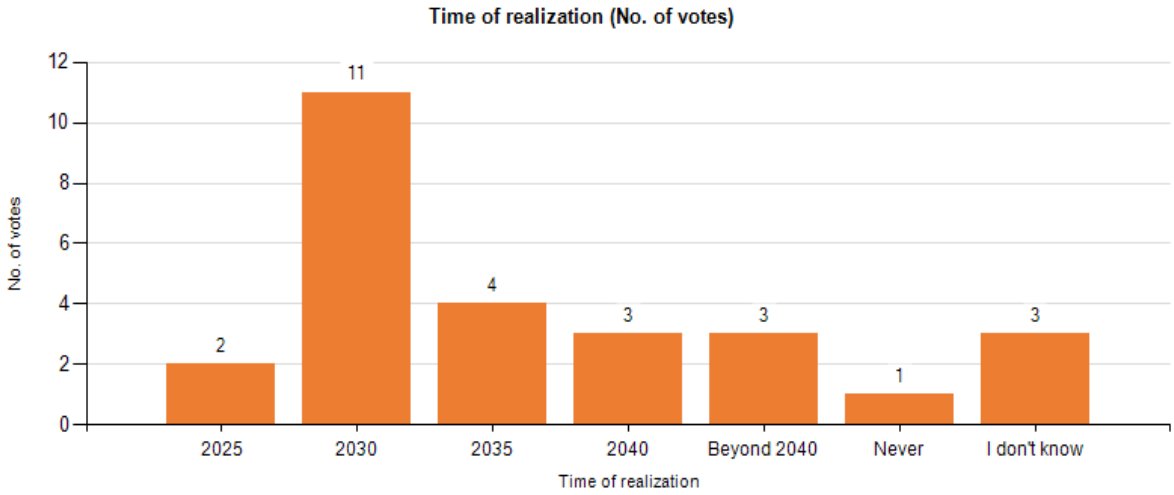
- **Understanding the roots causes of security challenges**
- **Agreement on common decision rules to be applied for autonomous security systems and new war codes, norms and ethical rules**
- **Methodologies and technologies for media and data analytics to predict security problems**
- **Research on automation of security systems**
- **Developing passive security techniques**
- **Deepening knowledge on man-machine interaction for semi-autonomous security technology**
- **Methods and practices for inclusive governance of security**
- **Research on socio-cultural and political consequences of a security-based society with new weapons**
- **Regulations for data and privacy protection**

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

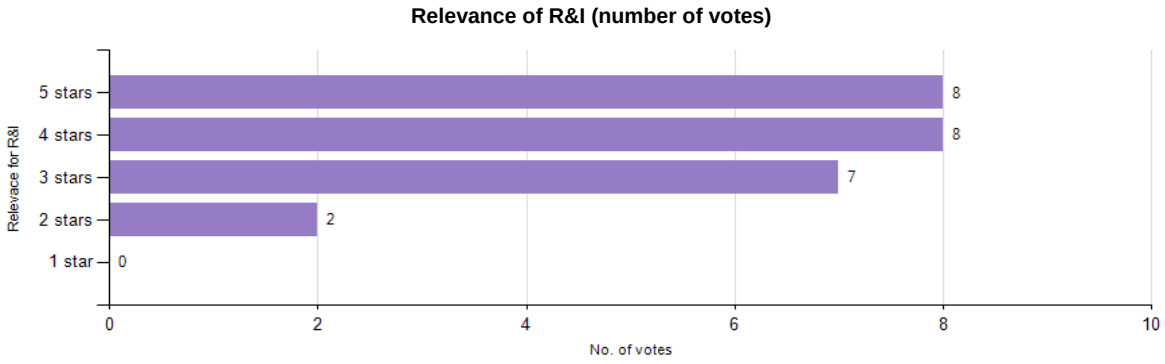
This annex includes the parts of the data set that are relevant to this scenario.

Autonomous weapons and robots are deployed to monitor and secure at least 50% of the EU's land, sea, and air borders, sensitive places and infrastructures



Number of respondents: 27

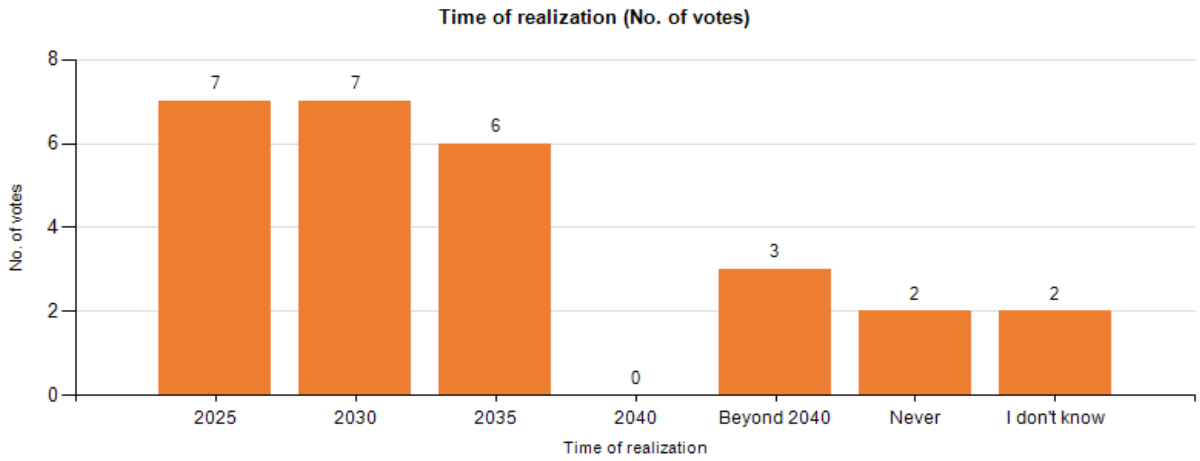
Arguments regarding the time of realization	**No. of votes**
As many as 40 nations are currently developing military robotics. Some weapons already in use may be considered "autonomous".	16
Autonomous machines will be available earlier; however, development of weapon systems takes a long time (usually 10-15 years).	13
The United Nations Convention on Conventional Weapons has been already debating a possible ban on Autonomous Weapons.	9
EU bureaucracy and national uneveness will hold up deployment of systems that will be perceived as reducing sovereignty (especially of small-geography EU states).	7
Autonomous defensive systems are needed to secure critical infrastructure that must be protected 24/7/365 particularly from swarm attacks by autonomous drones where human action may be too slow.	7
The prospect of "autonomous" weapons and systems could revive interest in Confidence and Security-Building Measures in Europe (CSBM) and thus dampen and regulate diffusion.	4
Robotic and automatic weapon systems and platforms will profilerate, first by augmenting humans and then becoming autonomous in practice. Cheaper lifetime costs and better performance.	3
Autonomous systems are under development for maritime surveillance where autonomous operation augmented by AI is necessary to identify potential threats 24/7/365.	2



Average: 3.88 **Dispersion:** 0.91

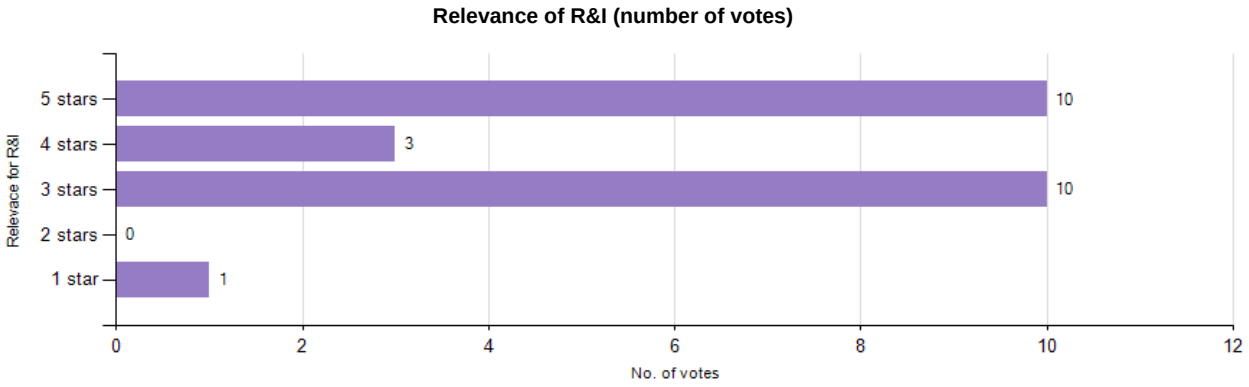
Arguments regarding the relevance of R&I	**No. of votes**
Ethical research needs to address the issues of agency and responsibility of autonomous weapons.	21
We need to have research in parallel for the related legal, ethical and socio-economical issues concerning this technology	14
The key question is what is meant by "autonomous". In mapping and exploring the implications we will need technology foresight (scenarios, etc.) as much as research.	12
It should be assessed how drones and other technologies could be used beneficially for search and rescue mission support.	10
Human - robotic / AI interface is growing in importance as autonomous systems play an increasing role in more activities with a growing concern for security implications of autonomous vehicles, etc.	5
Autonomous technologies are key to industrial activities in space and are necessary for asteroid mining and lunar development. The space economy will be largely autonomous machinery.	3
The key limiting factor is likely to be lack of political & social willingness to adopt the technology, rather than the technology itself.	2
Terrorism will continue as a threat and will employ chemical and biological weapons requiring continual monitoring of water and atmosphere for hazardous agents only possible through autonomous systems	2
((Assuming R&I = Research and Innovation. If I = Investment, position would shift))A/A key factor: positions and activities of the US and, therefore, NATO Nuclear Weapon States may not be keen on this	2

Anticipatory crime units with predictive data analysis exist in every EU capital



Number of respondents: 26

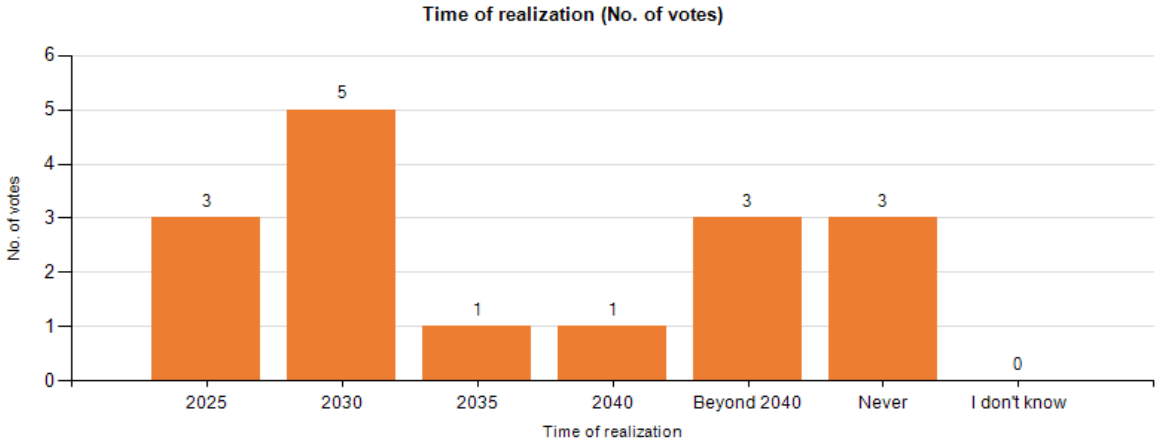
Arguments regarding the time of realization	**No. of votes**
Big Data can enhance knowledge of what is actually going on but is of little use in predicting new developments and discontinuities.	12
Predictive policing is already used in the States, Poland, Israel, Switzerland, and the UK.	12
Since the program is fed only data from offenses that the police registers, it only looks for corresponding patterns and so narrows the view.	10
Predictive policing has not been demonstrated to be effective yet, independent studies do not exist.	8
Privacy concerns need to be addressed prior to reaching this goal.	6
Predictive policing will be attempted to avert terrorism and mass killings. Danger in profiling and misidentification.	6
Smart policing exists in the US with police and probation officers trained to act on identified risk factors. Inaccurate data can result in injustice. Improved data can better identify risk factors.	2
To the term predictive font, it is better to take the anticipation of actions.	1
Predicting what: Crime location? Criminals? Area? Time? "Minority report" is still science fiction in 2040.	1



Average: 3.88 **Dispersion:** 1.15

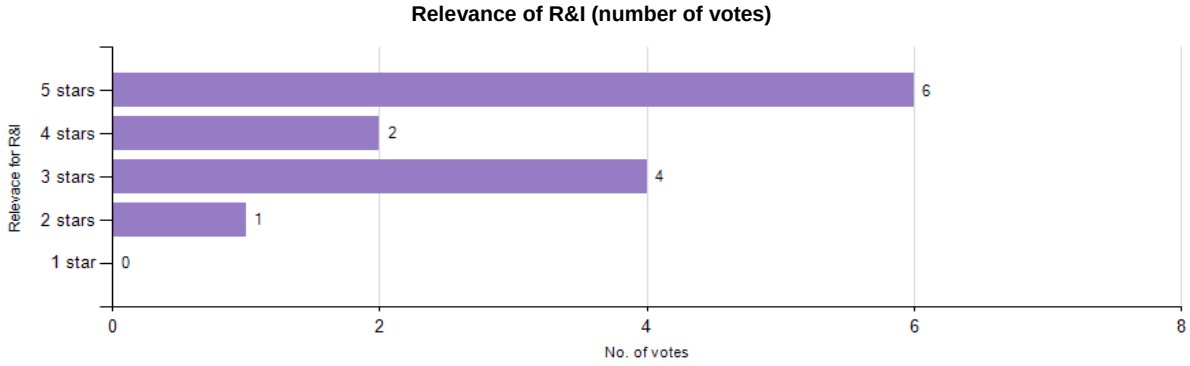
Arguments regarding the relevance of R&I	**No. of votes**
The advantages and disadvantages of combining predictive analytics with crime control should be explored very thoroughly, as this might have an impact on many societal developments.	18
Standardization of data across the EU is needed.	12
Pattern recognition still has to be improved.	9
We must not lose sight of the big picture. Research on population, demography and migration needs to be strengthened, as well as comparative analyses across Europe.	8
Data is very easy to misuse and abuse. Presence of risk factors does not guarantee crime but can be used in crime prevention. Research is needed to prevent abuse and improve effectiveness.	6
Training of police officers and an adjustment in policing doctrines are required	5
We need to make an effort on an operational research mode. This would make it possible to bring research closer to the actors of security.	2

Invisibility inducing metamaterials are deployed for the protection of vulnerable infrastructures for the first time



Number of respondents: 17

Arguments regarding the time of realization	**No. of votes**
Since critical infrastructures are immobile in most cases, invisibility is not an efficient concept in the presence of high precision GNSS services.	9
The demand for invisibility increases in response to improved satellite visual monitoring.	6
Presently metamaterial cloaking operates across a limited range of frequencies making such technology unsuitable to cloak critical infrastructure. Spies could simply use a frequency outside of range.	3
The current technology relies on 3D printing, which promises low cost solutions.	2
In 2016 scientists from Queen Mary University of London have made an object disappear by using a material with nano-size particles.	2
Invisibility of critical infrastructure is a novel kind of "security by obscurity", and unsuitable for civil infrastructure that needs long-term protection.	2
The risk of camouflage is to push the criminal into a spiral of invisibility. Dematerialisation must be measured.	2



Average: 4 **Dispersion:** 1.08

Arguments regarding the relevance of R&I	**No. of votes**
This technology is still in the demonstration phase.	10
Further research is needed regarding its possible use by terrorists.	7
Research is needed to expand range of operable frequencies and object size. Limited value so far.	4

Getting in touch with the EU

IN PERSON
All over the European Union there are hundreds of Europe Direct Information Centres.
You can find the address of the centre nearest you at: http://europa.eu/contact

ON THE PHONE OR BY E-MAIL
Europe Direct is a service that answers your questions about the European Union.
You can contact this service
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by electronic mail via: http://europa.eu/contact

Finding information about the EU

ONLINE
Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU PUBLICATIONS
You can download or order free and priced EU publications from EU Bookshop at: http://bookshop.europa.eu. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact)

EU LAW AND RELATED DOCUMENTS
For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

OPEN DATA FROM THE EU
The EU Open Data Portal (http://data.europa.eu/euodp/en/data) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

It is 2040. Globalisation and ICT solutions have changed the nature of threats faced by the EU. A combination of preventive and response measures are implemented in coordination by security and defence forces with the aid of computers. The role of the anticipatory crime units is rising, together with the diffusion of unmanned aerial vehicles and military robots with Artificial Intelligence features. These are used in external military actions as well as to secure national territories in cooperation with security units.

Studies and reports