



Европейски парламент Parlamento Europeo Evropský parlament Europa-Parlamentet Europäisches Parlament  
Euroopa Parlament Ευρωπαϊκό Κοινοβούλιο European Parliament Parlement européen Parlaimint na hEorpa  
Europskí parlament Parlamento europeo Eiropas Parlaments Europos Parlamentas Európai Parlament  
Parlament Ewropew Europees Parlement Parlament Europejski Parlamento Europeu Parlamentul European  
Európsky parlament Evropski parlament Europan parlamentti Europaparlamentet

## EP Ideju laboratorijas publikāciju saraksts

<https://www.europarl.europa.eu/thinktank>

Saraksta izveidei izmantotie meklēšanas kritēriji :

Sakārtot Sakārtot rezultātus pēc datuma  
Atslēgvārds "spiegošana"

22 Rezultāts(-i)

Izveides datums : 19-03-2024

## [The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware](#)

Publikācijas veids [Pētījums](#)

Datums [05-12-2022](#)

Ārējais autors LIGER Quentin, GUTHEILMirja

Politikas joma Brīvības, drošības un tiesiskuma telpa | ES demokrātija, institucionālās un parlamentārās tiesības | ES tiesības: tiesību sistēma un akti

Atslēgvārds aizsardzība | datu aizsardzība | informācija un informācijas apstrāde | informācijas drošība | informācijas tehnoloģija | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | komunikācijas | privātās dzīves aizsardzība | programmatūra | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | TIESĪBAS | tiesības un brīvības

Kopsavilkums This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA), provides a description of the legal framework (including oversight and redress mechanisms) governing the use of Pegasus and equivalent spyware in a selection of Member States.

[Pētījums EN](#)

Kopsavilkums [DE](#), [EL](#), [EN](#), [ES](#), [FR](#), [HU](#), [IT](#), [PL](#)

## [Greece's Predatorgate: The latest chapter in Europe's spyware scandal?](#)

Publikācijas veids [Pārskats](#)

Datums [08-09-2022](#)

Autors MILDEBRATH Hendrik Alexander

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds administratīvā caurredzamība | aizsardzība | Eiropa | ekonomiskā ģeogrāfija | Grieķija | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | izpildvara un valsts dienests | komunikācijas | komunikācijas vadība | POLITIKA | politika un sabiedrības drošība | politiskā opozīcija | politiskā ģeogrāfija | prese | programmatūra | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | GEOGRĀFIJA

Kopsavilkums After Hungary, Poland and Spain, Greece is the latest Member State accused of spying on journalists and opposition politicians. While the opposition is seeking transparency and is steadily increasing the pressure, the Greek government has acknowledged select surveillance operations but insists on their legality and categorically denies purchasing or using the commercial Predator spyware. This EPRI paper synthesises the fast-paced and highly politicised developments at national level and contextualises the European Union's responses. It refers to the EPRI study 'Europe's PegasusGate' for more information and possible ways forward.

[Pārskats EN](#)

## [Europe's PegasusGate: Countering spyware abuse](#)

Publikācijas veids [Pētījums](#)

Datums [06-07-2022](#)

Autors MILDEBRATH Hendrik Alexander

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds aizsardzība | brīvības, drošības un tiesiskuma telpa | dabaszinātnes un eksaktās zinātnes | datu aizsardzība | EIROPAS SAVIENĪBA | Eiropas struktūra | informācija un informācijas apstrāde | informācijas drošība | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | kibernetika | komunikācijas | plašsaziņas līdzekļi | saziņas aizsardzība | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | TIESĪBAS | tiesības un brīvības | ZINĀTNĒ

Kopsavilkums As civil society and media organisations expose EU Member States for using the Pegasus commercial spyware, one of the most high-profile spying scandals of recent years is coming to light in Europe. Member States' intelligence agencies have been accused of abusing highly sophisticated spyware to surveil opposition figures, journalists, lawyers, and high-ranking state officials. 'Having regard to the European Union's attachment to the values and principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law', the European Parliament has set up a committee of inquiry. This study (i) introduces the Pegasus product's features and trading practices, (ii) surveys Pegasus operations and reactions, (iii) identifies transversal and country-specific legal concerns, and (iv) sketches possible ways forward in the public and private sectors.

[Pētījums EN](#)

## Strategic communications as a key factor in countering hybrid threats

Publikācijas veids Pētījums

Datums 10-03-2021

Ārējais autors DG, EPERS\_ This study has been written by Juan Pablo Villar García, Carlota Tarín Quirós and Julio Blázquez Soria of Iclaves S.L., Carlos Galán Pascual of the University Carlos III of Madrid, and Carlos Galán Cordero of the Universitat Oberta de Catalunya at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

Politikas joma Brīvības, drošības un tiesiskuma telpa | Demokrātija | Ārlietas

Atslēgvārds aizsardzība | datornoziegums | demokrātija | dezinformācija | Eiropas Savienība | Eiropas struktūra | humanitārās zinātnes | informācija un informācijas apstrāde | informācijas apmaiņa | informācijas karš | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | komunikācijas | kopējā ārpolitika un drošības politika | POLITIKA | politika un sabiedrības drošība | politiskā propaganda | politiskā sistēma | sabiedrības informēšanas kampaņa | sociālie mediji | spiegošana | starptautiskā drošība | STARPTAUTISKĀS ATTIECĪBAS | terorisms | ZINĀTNE | ģeopolitika

Kopsavilkums This report describes the key features, technologies and processes of strategic communications to counter hybrid threats and their components. The theoretical description of hybrid threats is complemented by the analysis of diverse case studies, describing the geopolitical context in which the hybrid threat took place, its main features, the mechanisms related to strategic communications used by the victim to counter the hybrid threat and its impact and consequences. A comprehensive set of policy options aimed at improving the EU response to hybrid threats is also provided.

Pētījums [EN](#)

Pielikums 1 [EN](#)

## EU cyber sanctions: Moving beyond words

Publikācijas veids Pārskats

Datums 25-09-2020

Autors LATICI Tania

Politikas joma Drošība un aizsardzība | Globālā pārvadība | Ārlietas

Atslēgvārds aizsardzība | dezinformācija | Eiropas Savienība | Eiropas struktūra | ES ierobežojošs pasākums | informācijas drošība | informācijas karš | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | komunikācijas | POLITIKA | politika un sabiedrības drošība | politiskā propaganda | RAŽOŠANA, TEHNOLOGIJA UN PĒTNIECĪBA | rūpnieciskā spiegošana | spiegošana | starptautiskā drošība | STARPTAUTISKĀS ATTIECĪBĀS | tehnoloģija un tehniskā reglamentācija | Jaunprogrammatūra

Kopsavilkums The EU recognises that cybersecurity and cyber-defence are critical for its prosperity, security and global ambitions. Offensive cyber-attacks by malicious actors show no sign of slowing down (not even during the coronavirus pandemic) and thus require concrete dissuasive measures. In July 2020, the EU Member States decided for the first time to use the 'teeth' rooted in the EU cyber-diplomacy framework and to 'bite cyber perpetrators back' by placing sanctions on them. This precedent has helped reinforce the EU's cyber policy action.

Pārskats [EN](#)

## 5G in the EU and Chinese telecoms suppliers

Publikācijas veids Pārskats

Datums 08-04-2019

Autors GRIEGER Gisela

Politikas joma Pētniecības politika | Rūpniecība | Ārlietas

Atslēgvārds aizsardzība | autoritārais režīms | ekonomiskā ģeogrāfija | informācijas drošība | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | komunikācijas | krimināltiesības | POLITIKA | politiskā sistēma | publiskais iepirkums | pārraides tīkls | RAŽOŠANA, TEHNOLOGIJA UN PĒTNIECĪBA | rūpnieciskā spiegošana | saziņas aizsardzība | spiegošana | STARPTAUTISKĀS ATTIECĪBĀS | tehnoloģija un tehniskā reglamentācija | tehnoloģijas nodošana | TIESTĪBAS | tiesības un brīvības | TIRDZNIECĪBA | tirdzniecības politika | valsts drošības apdraudējums | Āzija un Okeānija | GEOGRAFIJA | Ķīna

Kopsavilkums The spectrum auctions of fifth-generation (5G) mobile telecoms networks planned in 17 EU Member States for 2019 or 2020 have sparked a highly politicised debate in the EU about whether the use of Chinese 5G equipment in critical EU infrastructure poses a threat to security. While Australia, Japan, and New Zealand have followed the United States (US) in imposing a (partial) ban on Chinese telecom vendors, EU Member States appear to privilege EU-coordinated national risk-mitigating measures over a ban.

Pārskats [EN](#)

## What if your emotions were tracked to spy on you?

Publikācijas veids Pārskats

Datums 13-03-2019

Autors VAN WOENSEL Lieve

Politikas joma Brīvības, drošības un tiesiskuma telpa | Cilvēktiesības | Drošība un aizsardzība | Dzimumu līdztiesības jautājumi, līdztiesība un daudzveidība | Ex ante ietekmes novērtēšana | Iepriekšēja plānošana | Izglītība | Nodarbinātība | Patēriņtāju aizsardzība | Starptautiskās privātiesības un tiesu iestāžu sadarbība civilīietās

Atslēgvārds aizsardzība | biometrija | dabaszīnātnes un eksaktās zinātnes | datu aizsardzība | datu apstrādes likums | Eiropas Savienība | Eiropas Savienības tiesību akti | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | informācijas tehnoloģijas ietekme | Izglītība un komunikācijas | komunikācijas | personas dati | policijas uzraudzība | privātās dzīves aizsardzība | regula (ES) | spiegošana | Starptautiskās attiecības | tiesvedība | TIESĪBAS | tiesības un brīvības | video novērošana | ZINĀTNE

Kopsavilkums Recent reports of celebrity singer, Taylor Swift, deploying facial recognition technology to spot stalkers at her concerts raised many eyebrows. What started out as a tool to unlock your smartphone or tag photos for you on social media is surreptitiously becoming a means of monitoring people in their daily lives without their consent. What impact and implications are facial recognition technology applications likely to have, and what can be done to ensure the fair engagement of this technology with its users and the public at large?

Pārskats [EN](#)

## Russia in the Western Balkans

Publikācijas veids Pārskats

Datums 06-07-2017

Autors RUSSELL Martin

Politikas joma Ārlietas

Atslēgvārds aizsardzība | ANO rezolūcija | Eiropa | Eiropas Savienība | Eiropas struktūra | ekonomiskā ģeogrāfija | energoapgāde | ENERĢĒTIKA | humanitārās zinātnes | kopējā ārpoliтика un drošības politika | Krievija | militārā sadarbība | nacionālisms | pievienošanās Kopienai | POLITIKA | politika enerģētikas jomā | politika un sabiedrības drošība | politiskā propaganda | politiskā sistēma | politiskā ģeogrāfija | Rietumbalkāni | sadarbības politika | spiegošana | starptautiskā drošība | starptautiskā politika | Starptautiskās attiecības | ZINĀTNE | ārpoliтика | ĢEOGRAFIJA | geopolitika

Kopsavilkums The Western Balkans have emerged as a front in Russia's geopolitical confrontation with the West. Building on close historical ties, Moscow is taking advantage of the political and economic difficulties to expand its influence, potentially undermining the region's stability.

Pārskats [EN](#)

## Transatlantic data flows

Publikācijas veids Pārskats

Datums 23-05-2016

Autors MONTELEONE Shara

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | datu aizsardzība | datu apstrādes likums | datu vākšana | Eiropas Komisija | Eiropas Savienība | Eiropas Savienības iestādes un Eiropas civildienests | ekonomiskā ģeogrāfija | iespēja griezties tiesā | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | Izglītība un komunikācijas | komunikācijas | POLITIKA | politiskā sistēma | politiskā ģeogrāfija | privātās dzīves aizsardzība | pārrobežu datu plūsmu | spiegošana | Starptautiskās attiecības | Tiesa (ES) | tiesvedība | TIESĪBAS | tiesības un brīvības | uzraudzības pilnvaras | ĢEOGRAFIJA

Kopsavilkums Privacy Shield is a new framework for transatlantic exchanges of personal data, agreed between the European Commission and the US government. Although it has significant improvements compared to its predecessor, Safe Harbour, concerns remain to be addressed before its finalisation.

Pārskats [EN](#)

## EYE 2016 – We are not afraid!

Publikācijas veids Pārskats

Datums 28-04-2016

Autors ORAV Anita

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds aizsardzība | diskriminācija etniskās piederības dēļ | Eiropas drošība | Eiropas Savienība | Eiropas struktūra | ES ārejo robežu aizsardzība | Izglītība un komunikācijas | komunikācijas vadība | kopējā ārpoliтика un drošības politika | personiskais ierocis | POLITIKA | politika un sabiedrības drošība | politiskā propaganda | privātās dzīves aizsardzība | robežkontrole | spiegošana | starptautiskā drošība | Starptautiskās attiecības | starptautiskās tiesības | terorisms | TIESĪBAS | tiesības un brīvības | vārda brīvība | Šengenas Informācijas sistēma

Kopsavilkums The year 2015 confirmed once again that terrorism is a serious threat to international security. The EU plays an active role in supporting Member States' measures to ensure security, be it through strengthening the control of firearms, securing borders or using new technologies. Security, however, needs to be balanced with the respect for fundamental rights. Communities also have an important part to play in preventing terrorism. This note has been prepared for the European Youth Event, taking place in Strasbourg in May 2016. Please click here for the full publication in PDF format

Pārskats [EN](#)

## [Foreign fighters – Member State responses and EU action](#)

Publikācijas veids Briefing

Datums 09-03-2016

Autors BAKOWSKI Piotr | PUCCIO Laura

Politikas joma Brīvības, drošības un tiesiskuma telpa | Ārlietas

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | ANO rezolūcija | datu izpaušana | EIROPAS SAVIENĪBA | Eiropas struktūra | ekonomiskā ģeogrāfija | eksteritoriālā jurisdikcija | ekstrēmisms | ES dalībvalsts | ES tiesu iestāžu sadarbība kriminālīetās | ES ārejo robežu aizsardzība | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | krimināllikums | krimināltiesības | kultūra un reliģija | policijas sadarbība | POLITIKA | politika un sabiedrības drošība | politiskā ģeogrāfija | reliģiskais fundamentālisms | robežkontrole | sadarbības politika | SOCIĀLIE JAUTĀJUMI | sociālā rehabilitācija | sociālās lietas | spiegošana | starptautiskā politika | STARPTAUTISKĀS ATTIECĪBAS | starptautiskās tiesības | terorisms | TIESĪBAS | tiesību sistēmas struktūra | valstspiederība | GEOGRAFIJA

Kopsavilkums As the hostilities in Syria and Iraq continue, and terrorist activities worldwide appear to be on the rise, EU Member States are increasingly confronted with the problem of aspiring and returning 'foreign fighters'. Whereas the phenomenon is not new, its scale certainly is, explaining the wide perception that these individuals are a serious threat to the security of both individual Member States and the EU as a whole.

International fora, including the United Nations, have addressed the problem, with the UN adopting a binding resolution in 2014 specifically addressing the issue of foreign fighters. The EU is actively engaged in international initiatives to counter the threat.

Within the EU, security in general, and counter-terrorism in particular, have traditionally remained within the Member States' remit. The EU has, however, coordinated Member State activities regarding the prevention of radicalisation, the detection of travel for suspicious purposes, the criminal justice response, and cooperation with third countries. The EU is seeking to strengthen its role, given the public feeling of insecurity in the wake of recent terrorist attacks. The EU's role as a forum to discuss security issues has consequently grown during 2015.

Individual Member States have stepped up their efforts to address the problem, using various tools including criminal law, administrative measures and 'soft tools', such as counter-radicalisation campaigns. The Member States most affected have also cooperated with each other outside the EU framework.

The United States has a particularly developed counter-terrorism framework, now used to deal with foreign fighters. Since 9/11, the EU and the USA cooperate on counter-terrorism, despite differing philosophies on issues such as data protection.

This briefing substantially updates an earlier one, PE 548.980, from February 2015.

Briefing [EN](#)

## [EU-Brazil cooperation on internet governance and ICT issues](#)

Publikācijas veids Briefing

Datums 30-10-2015

Autors LAZAROU Eleni

Politikas joma Brīvības, drošības un tiesiskuma telpa | Drošība un aizsardzība | Globālā pārvaldība | Ārlietas

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | Brazīlija | datu aizsardzība | ekonomiskā ģeogrāfija | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | internets | IZGLĪTĪBA UN KOMUNIKĀCIJAS | izpildvara un valsts dienests | komunikācijas | personas dati | POLITIKA | politiskā ģeogrāfija | pārraides tīkls | pārrobežu datu plūsma | sadarbības politika | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | tehniskā sadarbība | telekomunikācijas iekārta | telekomunikācijas noteikumi | valdišana | valsts-privātuzņēmumu partnerība | GEOGRAFIJA

Kopsavilkums Following revelations of large-scale Internet surveillance Brazil and the EU have become actively involved in the global debate on internet governance. Since early 2014 cyber policy has become part of the agenda of the EU-Brazil Strategic Partnership. The two have agreed on the need for support for inclusive and transparent internet governance based on a multistakeholder governance model, and are moving forward on a number of related bilateral initiatives in the 2015-2017 Joint Action Plan. In 2014, Brazil hosted the Global Multistakeholder Meeting on Future Internet Governance (NETMundial) which established principles on internet governance endorsed by both the EU and Brazil. These encompass inclusiveness, legitimacy, accountability, and global public interest. As a move towards greater independence of digital flows between Latin America and the Europe, the Brazilian government and the EU are developing a project to establish a public-private partnership to lay a submarine fibre-optic cable across the Atlantic Ocean, from Fortaleza (Ceará, Brazil) to Lisbon (Portugal). Please click here for the full publication in PDF format

Briefing [EN](#)

## [The CJEU's Schrems ruling on the Safe Harbour Decision](#)

Publikācijas veids Pārskats

Datums 26-10-2015

Autors MONTELEONE Shara | PUCCIO Laura

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | datu aizsardzība | datu izpaušana | EIROPAS SAVIENĪBA | Eiropas Savienības tiesību akti | Eiropas struktūra | ekonomiskā ģeogrāfija | ES attiecības | ES Pamattiesību harta | informācija un informācijas apstrāde | informācijas apmaiņa | informācijas tehnoloģija un datu apstrāde | IZGLITĪBA UN KOMUNIKĀCIJAS | personas dati | POLITIKA | politiskā sistēma | politiskā ģeogrāfija | privātās dzīves aizsardzība | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | Tiesas spriedums (ES) | TIESĪBAS | tiesības un brīvības | tiesību aktu iztulkošana | tiesību avoti un nozares | uzraudzības pilnvaras | GEOGRAFIJA

Kopsavilkums On 6 October 2015, the Court of Justice of the EU (CJEU) declared invalid the European Commission's decision on the adequacy of the US data protection system (Safe Harbour Decision). In this judgment, regarding the transfer of personal data from the EU to the USA, the Court also clarified that national supervisory authorities are always allowed to investigate the lawfulness of data transfers and, if necessary, to suspend them. The case underlines the requirement for ensuring high-level protection when EU citizens' data are transferred to third countries. The implications for businesses, governments and EU institutions, as well as for EU-US relations, remain to be clarified.

Pārskats [EN](#)

## [The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens](#)

Publikācijas veids Pētījums

Datums 15-05-2015

Ārējais autors Francesca Bignami (George Washington University Law School, Washington, USA)

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | datu aizsardzība | datu izpaušana | datu vākšana | ekonomiskā ģeogrāfija | ES pilsoni | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | IZGLITĪBA UN KOMUNIKĀCIJAS | krimināltiesības | politiskā ģeogrāfija | privātās dzīves aizsardzība | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | starptautiskās tiesības | tiesas izmeklēšana | tiesvedība | TIESĪBAS | tiesības un brīvības | tiesību avoti un nozares | tiesību avots | tiesību sistēma | tiesību sistēmas struktūra | valsts drošības apdraudējums | GEOGRAFIJA

Kopsavilkums Upon request by the LIBE Committee, this study surveys the US legal system of data protection in the field of federal law enforcement. It reviews two principal sources of US data protection law, the Fourth Amendment to the US Constitution and the Privacy Act of 1974. It also considers the legally prescribed methods of data collection, together with their associated data protection guarantees, in ordinary criminal investigations and national security investigations. Throughout, the study pays special attention to the rights afforded to EU citizens.

Pētījums [EN](#)

## [Mass Surveillance - Part 2: Technology foresight, options for longer term security and privacy improvements](#)

Publikācijas veids Pētījums

Datums 13-01-2015

Ārējais autors Company:  
Capgemini Consulting

Authors:  
M. van den Berg  
P. de Graaf (editor)  
P.O. Kwant  
T. Slewe

Politikas joma Iepriekšēja plānošana | Pētniecības politika

Atslēgvārds aizsardzība | atklātā pirmkoda programmatūra | brīvības, drošības un tiesiskuma telpa | datornoziegums | datu aizsardzība | EIROPAS SAVIENĪBA | Eiropas struktūra | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | informācijas tehnoloģijas ietekme | internets | IZGLITĪBA UN KOMUNIKĀCIJAS | komunikācijas | kriptogrāfija | personas dati | RAZOŠANA, TEHNOLOGIJA UN PĒTNIECĪBA | sazinās aizsardzība | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | tehnoloģija un tehniskā reglamentācija | tehnoloģijas perspektīvu izpēte | TIESĪBAS | tiesības un brīvības

Kopsavilkums The main objective of part two of this study is to provide the European Parliament with policy options, based on technology foresight, with regard to the protection of the European Information Society against mass surveillance from a perspective of technology and organisational foresight. Four scenarios with two to four technology options each were developed in this study, leading to twenty-three policy options.

Pētījums [EN](#)

Pielikums 1 [EN](#)

Pielikums 2 [EN](#)

Multivide [Mass surveillance and citizen rights in the EU part 2](#)

## [Mass Surveillance - Part 1: Risks and opportunities raised by the current generation of network services and applications](#)

Publikācijas veids Pētījums

Datums 12-01-2015

Ārējais autors Company:  
TECNALIA Research and Investigation

Authors:

Arkaitz Gamino Garcia  
Concepción Cortes Velasco  
Eider Iturbe Zamalloa  
Erkuden Rios Velasco  
Iñaki Eguíua Elejabarrieta  
Javier Herrera Lotero  
Jason Mansell (Linguistic Review)  
José Javier Larrañeta Ibañez  
Stefan Schuster (Editor)

Politikas joma lepriekšēja plānošana | Pētniecības politika

Atslēgvārds aizsardzība | brīvības, drošības un tiesiskuma telpa | datornoziegums | datu aizsardzība | EIROPAS SAVIENĪBA | Eiropas struktūra | elektroniskais pasts | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | informācijas tehnoloģijas ietekme | internets | IZGLĪTĪBA UN KOMUNIKĀCIJAS | komunikācijas | kriptogrāfija | personas dati | saziņas aizsardzība | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | TIESIBAS | tiesības un brīvības | Jaunprogrammatūra

Kopsavilkums This document identifies the risks of data breaches for users of publicly available Internet services such as email, social networks and cloud computing, and the possible impacts for them and the European Information Society. It presents the latest technology advances allowing the analysis of user data and their meta-data on a mass scale for surveillance reasons. It identifies technological and organisational measures and the key stakeholders for reducing the risks identified. Finally the study proposes possible policy options, in support of the risk reduction measures identified by the study.

Pētījums [EN](#)

Pielikums 1 [EN](#)

Pielikums 2 [EN](#)

Multivide [Mass surveillance and citizen rights in the EU part 1](#)

## [The Echelon Affair: The EP and the global interception system 1998 - 2002](#)

Publikācijas veids Pētījums

Datums 04-11-2014

Autors MOMBELLI Iolanda | PIODI Franco

Politikas joma Brīvības, drošības un tiesiskuma telpa | Drošība un aizsardzība | Globālā pārvadība | Ārlietas

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | Apvienotā Karaliste | daļība Eiropas Savienībā | Eiropa | EIROPAS SAVIENĪBA | Eiropas Savienības iestādes un Eiropas civildienests | Eiropas struktūra | ekonomiskā ģeogrāfija | ES attiecības | iestāžu savstarpējās attiecības (ES) | institucionālās pilnvaras (ES) | konkurence | parlamenta komiteja | parlamenta procedūra | parlamenta procedūras | parlaments | POLITIKA | politiskā ģeogrāfija | RĀZOŠANA, TEHNOLOGIJA UN PĒTNIECĪBA | rūpnieciskā spiegošana | saziņas aizsardzība | spiegošana | starptautiska konkurence | STARPTAUTISKĀS ATTIECĪBAS | tehnoloģija un tehniskā reglamentācija | tehnoloģijas novērtējums | TIESIBAS | tiesības un brīvības | UZŅEMEJDARBĪBA UN KONKURENCE | GEOGRAFIJA

Kopsavilkums During the second half of the 1990s press and media reports revealed the existence of the Echelon network. This system for intercepting private and economic communications was developed and managed by the states that had signed the UKUSA and was characterised by its powers and the range of communications targeted: surveillance was directed against not only military organisations and installations but also governments, international organisations and companies throughout the world.

This study recounts the uncovering of the network, notably through the STOA investigations, questions by MEPs, debates in plenary, the setting up of a temporary committee and the final position adopted by the European Parliament. It also takes account of statements by researchers and journalists on the technical aspects and legal implications of the Echelon network. Finally, it considers the views of the political groups in the European Parliament and of the Commission and Council.

Fifteen years after the events, The Echelon Affair draws on the European Parliament's archives to describe and analyse a worldwide scandal which had an impact on the history of Parliament and which today is echoed in the revelations of Edward Snowden and Julian Assange and in other cases of spying on a grand scale.

Pētījums [EN, FR](#)

## Evaluation of EU Measures to Combat Terrorist Financing

Publikācijas veids Pētījums

Datums 11-04-2014

Ārējais autors Mara WESSELING (Centre de Sociologie des Organisations, Sciences-Po Paris/CNRS, France)  
Foreword by: Marieke DE GOEDE (Universiteit van Amsterdam, the Netherlands)

Politikas joma Brīvības, drošības un tiesiskuma telpa | Finanšu un banku jautājumi

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | banku uzraudzība | cīņa pret noziedzību | datu aizsardzība | datu izpaušana | ekonomiskā ģeogrāfija | FINANSES | finanšu tiesību akti | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | kapitāla brīva kustība | kreditiestādes un finanšu iestādes | naudas atmazgāšana | personas dati | POLITIKA | politika un sabiedrības drošība | politiskā ģeogrāfija | privātās dzīves aizsardzība | SOCIĀLIE JAUTĀJUMI | sociālās lietas | spiegošana | STARPTAUTISKĀS ATTIECĪBAS | terorisms | TIESĪBAS | tiesības un brīvības | ĢEOGRĀFIJA

Kopsavilkums Upon request by the LIBE Committee, this note evaluates the EU's measures to combat terrorist financing and their societal and political impact. In response to the renewed politicization of the EU-US Terrorist Finance Tracking Programme (TFTP) and taking into account that the European Commission has announced in November 2013 its intention not to present at this stage a proposal for a European Terrorist Finance Tracking System (EU TFTS), and in the light of the development of a 4th Directive on anti-money laundering and combatting terrorist financing (AML/CFT Directive), the note proposes a set of recommendations concerning possible measures to combat terrorist financing.

Pētījums [EN](#)

## Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013

Publikācijas veids Pētījums

Datums 11-04-2014

Ārējais autors Didier BIGO (CCLS – King's College London, United-Kingdom), Julien JEANDESBOZ (CCLS – University of Amsterdam, Netherlands), Médéric MARTIN-MAZE (CCLS) and Francesco RAGAZZI (CCLS – University of Leiden, Netherlands)

Politikas joma Brīvības, drošības un tiesiskuma telpa | Drošība un aizsardzība

Atslēgvārds aizsardzība | civilā aizsardzība | Eiropas drošība | ES pētniecības politika | ES rūpniecības politika | humanitārās zinātnes | informācijas tehnoloģija un datu apstrāde | informācijas tehnoloģijas ietekme | informācijas tehnoloģijas lietojums | IZGLĪTĪBA UN KOMUNIKĀCIJAS | izpildvara un valsts dienests | POLITIKA | politika un sabiedrības drošība | privātās dzīves aizsardzība | PTI pamatprogramma | pētniecība un intelektuālais īpašums | RAŽOŠANA, TEHNOLOGIJA UN PĒTNIECĪBA | RŪPNIECĪBA | rūpniecības struktūras un politika | sociālās zinātnes | spiegošana | starptautiskā drošība | STARPTAUTISKĀS ATTIECĪBAS | TIESĪBAS | tiesības un brīvības | valsts-privātuzņēmumu partnerība | ZINĀTNE

Kopsavilkums Upon request by the LIBE Committee, this study analyses how the public-private dialogue has been framed and shaped and examines the priorities set up in calls and projects that have received funding from the European Commission under the security theme of the 7th Research Framework Programme (FP7 2007-2013). In particular, this study addresses two main questions: to what extent is security research placed at the service of citizens? To what extent does it contribute to the development of a single area of fundamental rights and freedoms? The study finds that security research has only partly addressed the concerns of EU citizens and that security research has been mainly put at the service of industry rather than society.

Pētījums [EN](#)

## EU approach to cyber-security

Publikācijas veids Pārskats

Datums 31-03-2014

Autors FERRARO Francesca

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds administratīvā sadarbība | aizsardzība | brīvības, drošības un tiesiskuma telpa | cīņa pret noziedzību | datornoziegums | datu aizsardzība | direktīva (ES) | Eiropas konvencija | EIROPAS SAVIENĪBA | Eiropas Savienības iestādes un Eiropas civildienestu | Eiropas Savienības Kiberdrošības aģentūra | Eiropas Savienības tiesību akti | Eiropas struktūra | Eiropols | ES programma | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | izpildvara un valsts dienests | POLITIKA | SOCIĀLIE JAUTĀJUMI | sociālās lietas | spiegošana | starptautiskā politika | STARPTAUTISKĀS ATTIECĪBAS

Kopsavilkums Fighting cross-border crime affecting information and communications networks (cybercrime) is a priority in the EU's internal security strategy. To counter so-called cyber-attacks in a borderless space, the European Union and the Council of Europe have drawn up common strategies, operational measures and legislation.

Pārskats [EN](#)

## The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights

Publikācijas veids Pētījums

Datums 16-09-2013

Ārējais autors Caspar BOWDEN (Independent Privacy Researcher),  
Introduction by Didier BIGO (King's College London / Centre d'Etudes sur les Conflits, Liberté et Sécurité – CCLS,  
Paris, France)

Politikas joma Brīvības, drošības un tiesiskuma telpa

Atslēgvārds aizsardzība | Amerika | Amerikas Savienotās Valstis | datu aizsardzība | datu ieraksts | datu vākšana | ekonomiskā  
ģeogrāfija | informācija un informācijas apstrāde | informācijas tehnoloģija un datu apstrāde | internets | IZGLĪTĪBA UN  
KOMUNIKĀCIJAS | Komunikācijas | pamattiesības | personas dati | politiskā ģeogrāfija | spiegošana |  
STARPTAUTISKĀS ATTIECĪBAS | TIESĪBAS | tiesības un brīvības | ĢEOGRĀFIJA

Kopsavilkums In light of the recent PRISM-related revelations, this briefing note analyzes the impact of US surveillance programmes  
on European citizens' rights. The note explores the scope of surveillance that can be carried out under the US FISA  
Amendment Act 2008, and related practices of the US authorities which have very strong implications for EU data  
sovereignty and the protection of European citizens' rights.

Pētījums [DE](#), [EN](#), [FR](#)

Kopsavilkums [ES](#), [IT](#), [PL](#)

## Space and Security : The Use of Space in the Context of the CSDP

Publikācijas veids Padziļināta analīze

Datums 30-11-2011

Ārējais autors DARNIS, Jean-Pierre (ISTITUTO AFFARI INTERNAZIONALI, ITALY) and VECLANI, Anna (ISTITUTO AFFARI  
INTERNAZIONALI, ITALY)

Politikas joma Drošība un aizsardzība | Pētniecības politika

Atslēgvārds aizsardzība | attālā uzrāde | Eiropas Aizsardzības aģentūra | EIROPAS SAVIENĪBA | Eiropas struktūra | informācijas  
tehnoloģija un datu apstrāde | IZGLĪTĪBA UN KOMUNIKĀCIJAS | komunikācijas | kopejā āropolitika un drošības politika  
| kosmosa militarizācija | kosmosa politika | militārs gaisa kuģis | militārā sadarbība | pētniecība un intelektuālais  
īpašums | RĀZOŠANA, TEHNOLOGIJA UN PĒTNIECĪBA | sadarbības politika | satelītkomunikācija | spiegošana |  
starptautiskā drošība | STARPTAUTISKĀS ATTIECĪBAS

Kopsavilkums Space applications are best suited for dealing with an increasingly expanding concept of security. If, on the one hand,  
traditional customers are military users, on the other, a wider security and civilian community benefits from space  
services which are being developed in Europe in line with the evolution of Common Security and Defence Policy  
(CSDP) civilian and military missions.

The study includes a twofold analysis. First, an analysis of CSDP missions and their operational context to be matched  
with the main space-based applications. Of course, the EU flagship programmes GMES and Galileo are taken into  
consideration.

Second, an overview of the state-of-the-art of the different space programmes in Europe based on their compatibility  
with CSDP missions is provided. Building on this analysis, conclusions on the use of space in the context CSDP are  
drawn, focusing on strengths and weaknesses emerged. Finally, some recommendations addressed to the European  
Parliament are provided.

Padziļināta analīze [EN](#)