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

Seznam publikacij Think Tanka Evropskega parlamenta

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

Iskalna merila, uporabljena za izdelavo seznama :

Razvrsti Razvrsti po datumu
Ključna beseda "računalniška kriminaliteta"

98 Rezultati

Datum nastanka : 19-04-2024

Cyber solidarity act

Vrsta publikacije Briefing

Datum 13-02-2024

Avtor CAR POLONA

Politično področje Sprejemanje zakonodaje s strani Evropskega parlamenta in Sveta

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | enotni digitalni trg | EVROPSKA UNIJA | evropska varnost | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | POLITIKA | politika in javna varnost | pravo Evropske unije | predlog (EU) | računalniška kriminaliteta | varnost kritične infrastrukture | varovanje tajnosti podatkov | zbiranje podatkov

Povzetek Russia's war against Ukraine has revealed the extent of our dependency on digital technology and the fragility of the digital space. It has triggered a surge in cyberattacks that have been particularly disruptive when targeting critical infrastructure – such as energy, health or finance – because of the increasing reliance on information technology, rendering this infrastructure all the more vulnerable. Against this backdrop, the Commission has proposed a regulation on a cyber solidarity act that would address the urgent need to strengthen solidarity and EU capacities to detect, prepare for and respond to cybersecurity threats and incidents. The proposed regulation envisages the establishment of a framework based on three pillars. The first is a European cyber shield – a platform of national and cross-border security operations centres. The second is a cybersecurity emergency mechanism that would support – including financially – preparedness, response and mutual assistance actions among Member States by creating a European cybersecurity reserve of trusted providers. The third is a cybersecurity incident review mechanism to assess and review significant or large-scale incidents. In Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE), where Lina Gálvez Muñoz (S&D, Spain) was appointed rapporteur. The Council and the Parliament are currently in negotiations to finalise the text. Second edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Briefing EN

EU cyber-resilience act

Vrsta publikacije Briefing

Datum 28-11-2023

Avtor CAR POLONA | DE LUCA Stefano

Politično področje Notranji trg in carinska unija | Varstvo potrošnikov

Ključna beseda digitalna tehnologija | dovoljenje za prodajo | EVROPSKA UNIJA | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | nadzor trga | oznaka skladnosti CE | pravo Evropske unije | predlog (EU) | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | računalniška oprema | tehnologija in tehnični predpisi | TRGOVINA | trgovinska politika | trženje | varovanje tajnosti podatkov

Povzetek New technologies come with new risks, and the impact of cyber-attacks through digital products has increased dramatically in recent years. Consumers are increasingly falling victim to security flaws linked to digital products such as baby monitors, robo-vacuum cleaners, Wi-Fi routers and alarm systems. For businesses, the importance of ensuring that digital products in the supply chain are secure has become pivotal, considering three in five vendors have already lost money owing to product security gaps. The European Commission's proposal for a regulation, the 'cyber-resilience act', therefore aims to impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network. The proposal introduces cybersecurity by design and by default principles and imposes a duty of care for the lifecycle of products. The Council and the Parliament are currently in negotiations to finalise the text. Third edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Briefing EN

European Day on the Protection of Children against Sexual Exploitation and Sexual Abuse

Vrsta publikacije Na kratko

Datum 17-11-2023

Avtor ODINK Ingeborg

Politično področje Območje svobode, varnosti in pravice | Vprašanje spola, enakost in različnost

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | otrokove pravice | otroška pornografija | ozaveščanje javnosti | pedofilija | POLITIKA | politika in javna varnost | pomoč žrtvam | pravice in svoboščine | PRAVO | računalniška kriminaliteta | spolno nasilje | varstvo otrok

Povzetek Child sexual exploitation and sexual abuse are among the worst forms of violence against children, and are crimes that know no borders. The constant rise of these crimes, exacerbated by the pandemic, underscores the importance of harmonised national legislation and international cooperation to improve prevention, protect the victims and prosecute the perpetrators. The European Day helps to raise awareness to this end.

Na kratko EN

High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

Vrsta publikacije Briefing

Datum 05-10-2023

Avtor NEGREIRO ACHIAGA Maria Del Mar

Politično področje Varnost in obramba

Ključna beseda delovanje institucij | EVROPSKA UNIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijski sistem | informacijsko vojskovanje | institucija EU | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | obvladovanje tveganja | organ EU | POSLOVANJE IN KONKURENCA | poslovodenje | pravo Evropske unije | predlog (EU) | računalniška kriminaliteta | urad ali agencija EU | varovanje tajnosti podatkov

Povzetek The digital transformation is making the EU institutions and administration more vulnerable to cyber-threats and incidents. Their number has surged dramatically in recent years: there were as many incidents during the first half of 2021 as in the whole of 2020, for instance. Yet an analysis of 20 Union institutions, bodies and agencies showed that their governance, preparedness, cybersecurity capability and maturity vary substantially, weakening the system. This proposal for a regulation would establish a common framework to ensure that similar cybersecurity rules and measures are applied within all Union institutions, bodies, offices and agencies, to improve their resilience and incident-response capacities and rapidly improve the existing situation. In the European Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE). The report was adopted unanimously in the ITRE meeting on 9 March 2023. The committee's decision to enter into interinstitutional negotiations was confirmed by the plenary on 15 March 2023. A provisional agreement was reached during the trilogue on 26 June 2023. ITRE confirmed the political agreement at its meeting on 18 September 2023 and Parliament is expected to adopt the text as agreed during its plenary session in November 2023. Third edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Briefing EN

The NIS2 Directive: A high common level of cybersecurity in the EU

Vrsta publikacije Briefing

Datum 08-02-2023

Avtor NEGREIRO ACHIAGA Maria Del Mar

Ključna beseda ekonomske analize | GOSPODARSTVO | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | računalniška kriminaliteta | varovanje tajnosti podatkov | študija učinkov

Povzetek The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law. Fourth edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Briefing EN

Qualified certificates for website authentication

Vrsta publikacije Na kratko

Datum 11-01-2023

Avtor Niestadt Maria

Politično področje Varstvo potrošnikov

Ključna beseda brskalnik | digitalna tehnologija | elektronski podpis | EVROPSKA UNIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | internetni naslov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | območje svobode, varnosti in pravice | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | spletna stran | tehnologija in tehnični predpisi | TRGOVINA | trženje | varovanje tajnosti podatkov

Povzetek Qualified certificates for website authentication (QWACs) allow users to identify who is behind a website. Aiming to increase QWAC uptake, the Commission has proposed an obligation for web-browsers to recognise them and make them more visible. The proposal has prompted fierce debate. While the Council agrees with the Commission and the Parliament is still debating its position, many stakeholders have raised concerns.

Na kratko EN

Strengthening cyber resilience

Vrsta publikacije Briefing

Datum 14-12-2022

Avtor VIKOLAINEN Vera

Politično področje Predhodna ocena učinka

Ključna beseda digitalna vsebina | EVROPSKA UNIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kibernetika | naravoslovne in uporabne vede | območje svobode, varnosti in pravice | pravo Evropske unije | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | tehnologija in tehnični predpisi | uredba (EU) | varovanje tajnosti podatkov | ZNANOST

Povzetek The present impact assessment (IA) accompanies the proposal for horizontal cybersecurity requirements for products with digital elements. The IA's strong points include a well-substantiated problem definition, an evidence base that appears to be recent and relevant, and a transparent account of the assumptions and limitations of the analysis. Furthermore, an effort has been made in the IA to quantify the total costs and benefits for the manufacturers of products with digital elements. However, the IA's analysis is predominantly economic, with little focus on environmental or social impacts. In addition to this, the general objectives set in the IA already appear rather prescriptive, leaving only two options that envisage horizontal requirements as real alternatives. Moreover, the IA has only partially reported on the stakeholder consultation activities, has not carried out a proper SME panel consultation, and did not explain why the open public consultation was reduced to 10 weeks.

Briefing EN

Resilience of critical entities

Vrsta publikacije Na kratko

Datum 16-11-2022

Avtor VORONOVA Sofija

Politično področje Območje svobode, varnosti in pravice

Ključna beseda EVROPSKA UNIJA | evropska varnost | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | obvladovanje tveganja | POLITIKA | politika in javna varnost | POSLOVANJE IN KONKURENCA | poslovodenje | pravo Evropske unije | predlog (EU) | računalniška kriminaliteta | strategija EU | varnost kritične infrastrukture | varovanje tajnosti podatkov

Povzetek Protecting critical infrastructure against physical and digital threats is more than ever high on the EU agenda, not least in the light of the recent Nord Stream gas pipelines sabotage. During the November II plenary session, the European Parliament is due to vote on a provisional agreement on rules to enhance critical entities' resilience.

Na kratko DE, EN, ES, FR, IT, PL

A high common level of cybersecurity – NIS2

Vrsta publikacije Na kratko

Datum 07-11-2022

Avtor NEGREIRO ACHIAGA Maria Del Mar

Politično področje Območje svobode, varnosti in pravice

Ključna beseda EVROPSKA UNIJA | evropska varnost | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | opravljanje storitev | POLITIKA | politika in javna varnost | pravo Evropske unije | predlog (EU) | računalniška kriminaliteta | TRGOVINA | trženje | varnost kritične infrastrukture | varovanje tajnosti podatkov | varstvo podatkov

Povzetek Cyber-attacks and cybercrime continue to rise worldwide. The EU is planning to increase its cyber-resilience by updating the Network and Information Security (NIS) Directive. The expansion of the scope to be covered by the proposed NIS2 directive, obliging more entities and sectors to take consistent measures, would help increase the level of cybersecurity in Europe in the longer term. The European Parliament is due to vote in plenary in November on the agreement reached in interinstitutional negotiations.

Na kratko DE, EN, ES, FR, IT, PL

Understanding the EU's response to organised crime

Vrsta publikacije Briefing

Datum 15-09-2022

Avtor LUYTEN KATRIEN

Politično področje Območje svobode, varnosti in pravice

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | Eurojust | Europol | EVROPSKA UNIJA | FINANCE | goljufija | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | migracije | nezakonito priseljevanje | organizirani kriminal | ponarejanje denarja | pranje denarja | PRAVO | prost pretok kapitala | računalniška kriminaliteta | trgovina z ljudmi | umor

Povzetek The EU has made substantial progress in terms of protecting its citizens since the early 1990s. This has often been in response to dramatic incidents, such as murders committed by the mafia or other organised crime groups or big money-laundering scandals, or to negative trends, such as the steep increase in migrant smuggling and trafficking in human beings following the 2015 migration crisis. More recently, it was necessary to respond to the sharp rise in cybercrime, fraud and counterfeiting during the coronavirus pandemic. Criminal organisations continue to pose big risks to the EU's internal security. A rising number of organised crime groups are active in EU territory, often with cross-border reach. Organised crime is furthermore an increasingly dynamic and complex phenomenon, with new criminal markets and modi operandi emerging under the influence of globalisation and new technologies in particular. While the impact of serious and organised crime on the EU economy is considerable, there are also significant political and social costs, as well as negative effects on the wellbeing of EU citizens. As organised crime has become more interconnected, international and digital, Member States – which remain responsible for operational activities in the area of police and judicial cooperation –rely increasingly on cross-border and EU-level cooperation to support their law enforcement authorities on the ground. Recognising the severity of the problem and the need for coordinated action, the EU has initiated several measures to encourage closer cooperation between Member States; it has furthermore adopted common legal, judicial and investigative frameworks to address organised crime. The European Parliament has made fighting organised crime a political priority and helped shape the relevant EU legislation. Future EU action will focus on implementing existing rules, improving operational cooperation – even beyond the EU's boundaries – and information-sharing, while also addressing some of the main criminal activities of organised crime groups. Furthermore, the EU aims to make sure that crime does not pay. This is an updated version of a briefing from September 2020.

Briefing EN

Multimedijske vsebine Understanding the EU response to organised crime

Facts about organised crime in the EU

EU action against serious crime

Russia's war on Ukraine: Timeline of cyber-attacks

Vrsta publikacije Briefing

Datum 21-06-2022

Avtor PRZETACZNIK Jakub

Politično področje Zunanje zadeve

Ključna beseda ekonomska geografija | Evropa | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijsko omrežje | informacijsko vojskovanje | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | omejevalni ukrep EU | POLITIKA | politika in javna varnost | politična geografija | računalniška kriminaliteta | Rusija | skupna varnostna in obrambna politika | Ukrajina | varnost kritične infrastrukture | varovanje tajnosti podatkov

Povzetek Russia launched its war on Ukraine on 24 February 2022, but Russian cyber-attacks against Ukraine have persisted ever since Russia's illegal annexation of Crimea in 2014, intensifying just before the 2022 invasion. Over this period, Ukraine's public, energy, media, financial, business and non-profit sectors have suffered the most. Since 24 February, limited Russian cyber-attacks have undermined the distribution of medicines, food and relief supplies. Their impact has ranged from preventing access to basic services to data theft and disinformation, including through deep fake technology. Other malicious cyber-activity involves sending of phishing emails, distributed denial-of-service attacks, and use of data-wiper malware, backdoors, surveillance software and information stealers. Organisations and governments around the world have not been indifferent to the hybrid risks thus posed. EU-, US- and NATO-led initiatives have been carried out with the aim of neutralising cyber-threats and protecting essential infrastructure. As part of these initiatives, the EU has activated its Cyber Rapid Response Teams (a project under Permanent Structured Cooperation (PESCO) in the area of security and defence policy), to support Ukraine's cyber-defence. Non-government and private players have supported Ukraine through various cyber-resilience activities. Since the beginning of the invasion, a significant number of counter-attacks have been launched by independent hackers, affecting the Russian state, security, banking and media systems. The European Parliament has called for stepping up cybersecurity assistance to Ukraine and for making full use of the EU's cyber-sanctions regimes against individuals, entities and bodies responsible for or involved in the various cyber-attacks targeting Ukraine.

Briefing EN, XL

Organised crime in Europe: Emerging trends and policy challenges

Vrsta publikacije Na kratko

Datum 25-03-2022

Avtor NOONAN EAMONN

Politično področje Območje svobode, varnosti in pravice

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | Europol | EVROPSKA UNIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | korupcija | MEDNARODNI ODNOSI | organizirani kriminal | policijsko sodelovanje | politika sodelovanja | PRAVO | računalniška kriminaliteta | strategija EU | varovanje tajnosti podatkov | čezmejno sodelovanje

Povzetek Serious and organised crime inflict huge costs on both the EU economy and society. Organised crime is an increasingly dynamic and complex phenomenon, as it has become more interconnected, transnational and digital. The Covid-19 pandemic has led to an increase in cybercrime, fraud and counterfeiting. Police and judicial actions and the effective implementation of existing EU instruments are critical in tackling this challenge. New strategies to disrupt the business models and structures of criminal organisations will also benefit from an integrated approach, recognising the socio-economic, technological and geopolitical dimensions of the problem.

Na kratko EN

Combating gender-based cyber-violence

Vrsta publikacije Na kratko

Datum 08-12-2021

Avtor SHREEVES Rosamund

Politično področje Vprašanje spola, enakost in različnost

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | enakost spolov | EVROPSKA UNIJA | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | pravice in svoboščine | PRAVO | pravo Evropske unije | predlog (EU) | računalniška kriminaliteta | spolna diskriminacija | spolno nasilje | varovanje tajnosti podatkov

Povzetek As the world moves online, forms of violence that already affect women and girls disproportionately are following suit, and digital technologies are enabling them to take on new guises. The EU does not have a legislative framework to address this gender-based violence, despite its harmful impacts on individuals, society and democracy. A legislative-initiative report calling for EU legislation to fight gender-based cyber-violence, and provide its victims across the Union with equal protection is expected to be put to the vote during Parliament's December 2021 plenary session.

Na kratko DE, EN, ES, FR, IT, PL

EU cyber-defence capabilities

Vrsta publikacije Na kratko

Datum 30-09-2021

Avtor LATICI Tania

Politično področje Varnost in obramba | Zunanje zadeve

Ključna beseda Agencija Evropske unije za kibernetsko varnost | boj proti kriminalu | dezinformacija | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | EVROPSKA UNIJA | evropska varnost | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | POLITIKA | politika in javna varnost | računalniška kriminaliteta | strategija EU | varnost kritične infrastrukture | varovanje tajnosti podatkov | varstvo podatkov

Povzetek Cyberspace has become the fifth domain of warfare alongside the traditional sea, land, air and space. As societies digitalise and become more technologically connected, cyber risks and vulnerabilities increase. The European Union (EU) has been highly active in strengthening cyber capabilities and coordination frameworks through a collection of initiatives and proposals, notably since 2017. The European Parliament will debate recent as well as future measures during the October I 2021 plenary session, with a focus on cyber-defence capabilities, the subject of a report discussed and voted in the Foreign Affairs (AFET) Committee in July 2021.

Na kratko DE, EN, ES, FR, IT, PL

Artificial intelligence in criminal law

Vrsta publikacije Na kratko

Datum 30-09-2021

Avtor VORONOVA Sofija

Politično področje Območje svobode, varnosti in pravice

Ključna beseda biometrija | boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | enako obravnavanje | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazenski postopek | kazensko pravo | kazensko pravo | naravoslovne in uporabne vede | organizacija pravnega sistema | organizacija sodstva | pravica do sodnega varstva | pravice in svoboščine | PRAVO | računalniška kriminaliteta | sodstvo | temeljne pravice | umetna inteligenca | ZNANOST

Povzetek The use of artificial intelligence (AI) in a broad range of areas is the subject of wide debate at EU level. Establishing an EU approach to AI is one of the European Commission's digital priorities, as illustrated by the proposal on an artificial intelligence act. Despite the great opportunities they offer, AI applications can also entail significant risks to people's fundamental rights. At the October I plenary session, the European Parliament is due to debate an own-initiative report on the use of AI by the police and judicial authorities in criminal matters.

Na kratko DE, EN, ES, FR, IT, PL

Internal Security Fund 2021-2027

Vrsta publikacije: Na kratko
Datum: 01-07-2021
Avtor: VORONOVA Sofija
Politično področje: Območje svobode, varnosti in pravice
Ključna beseda: boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | EVROPSKA UNIJA | finance EU | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | mednarodno pravo | organizirani kriminal | POLITIKA | politika in javna varnost | pomoč žrtvam | porazdelitev sredstev EU | PRAVO | pravo Evropske unije | predlog (EU) | radikalizacija | računalniška kriminaliteta | sklad (EU) | terorizem | vizumska politika EU | zunanja meja Evropske unije
Povzetek: As part of the 2021-2027 Multiannual Financial Framework (MFF), the European Commission proposed a regulation establishing the Internal Security Fund, with increased budgetary allocation, to ensure a high level of security within the Union. The European Parliament is due to vote at second reading during the July plenary session on the agreed text resulting from interinstitutional negotiations.
Na kratko: DE, EN, ES, FR, IT, PL

Digital transformation - why do some significant banks fall behind?

Vrsta publikacije: Poglobljena analiza
Datum: 25-06-2021
Zunanji avtor: A.C. Bertay, H. Huizinga
Politično področje: Ekonomske in monetarne zadeve | Finančna in bančna vprašanja
Ključna beseda: banka | dokumentacija | Evropska centralna banka | EVROPSKA UNIJA | FINANCE | finančni nadzor | finančno tveganje | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | kreditne in finančne institucije | mednarodna varnost | MEDNARODNI ODNOSI | programska oprema | prost pretok kapitala | raziskovalno poročilo | računalniška kriminaliteta | uporaba informacijske tehnologije | varovanje tajnosti podatkov
Povzetek: This paper shows that larger banks and better capitalised banks invest more in computer software. These findings could reflect that larger banks can attain greater benefits from computer software and that better capitalised banks have more resources to make larger software investments. All the same, smaller and less capitalised banks will also have to make substantial software investments to maintain sustainable businesses, something that supervisors will need to point that out to these banks.
Poglobljena analiza: EN

Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade

Vrsta publikacije: Na kratko
Datum: 02-06-2021
Avtor: NEVILLE ANN
Politično področje: Območje svobode, varnosti in pravice
Ključna beseda: delo parlamenta | dnevni red | dokumentacija | EVROPSKA UNIJA | Evropski parlament | graditev Evrope | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | parlamentarna razprava | POLITIKA | poročilo | računalniška kriminaliteta | strategija EU | uporaba informacijske tehnologije | učinek informacijske tehnologije | varovanje tajnosti podatkov
Povzetek: Increasing digitalisation means that public administration at EU and national levels has come to rely on digital technologies as a means of carrying out their core functions, a process that has been intensified by the pandemic. This growing reliance on digital technologies, while beneficial, has also increased the risk of cyber-attacks, and key institutions at EU and national level have recently been targeted by cyber-attacks. During the June I plenary session, Members of the European Parliament will debate with the Council and the Commission on recent cyber-attacks in the EU, and discuss the European Union's cybersecurity strategy for the digital decade.
Na kratko: DE, EN, ES, FR, IT, PL

Digital Europe programme: Funding digital transformation beyond 2020

Vrsta publikacije Briefing

Datum 26-05-2021

Avtor SZCZEPANSKI Marcin

Politično področje Notranji trg in carinska unija

Ključna beseda digitalizacija | digitalna tehnologija | dokumentacija | ekonomske analize | enotni digitalni trg | EVROPSKA UNIJA | finance EU | GOSPODARSTVO | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | inovacija | IZOBRAŽEVANJE IN KOMUNIKACIJE | obdelava podatkov | porazdelitev sredstev EU | pravo Evropske unije | predlog (EU) | program EU | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | računalniška pismenost | tehnologija in tehnični predpisi | umetna inteligenca | uporaba informacijske tehnologije | varovanje tajnosti podatkov | študija učinkov

Povzetek The Digital Europe Programme is a new financial support tool for the 2021-2027 period, aimed at bolstering the digital transformation of society, the economy and public administrations in the EU. With a financial envelope of €7.6 billion (in current prices), a figure 17.5 % lower than the initial Commission proposal, it will build up digital capacity and infrastructure and support a digital single market. The programme will operate mainly through coordinated and strategic co-investments with the Member States in the areas of high-performance computing and data processing, artificial intelligence in the public and private sectors, cybersecurity and trust, advanced digital skills and deployment, best use of digital capacities and interoperability. On 11 May 2021, the regulation establishing the programme entered into force, with retroactive application from 1 January 2021. The programme, dedicated to supporting the digitalisation of Europe and achieving digital sovereignty, is the first-ever such financial instrument at the EU level. Furthermore, in the context of recovery from the pandemic, Member States must allocate at least 20 % of the recovery funds to projects that digitalise their economies and societies. Third edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Briefing EN

Multimedijske vsebine Digital Europe programme

Combating Gender based Violence: Cyber Violence

Vrsta publikacije Študija

Datum 17-03-2021

Avtor FERNANDES MEENAKSHI | LOMBA NIOMBO | NAVARRA Cecilia

Politično področje Evropska dodana vrednost

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomske analize | enakost spolov | gospodarske posledice | GOSPODARSTVO | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | položaj žensk | pomoč žrtvam | pravice in svoboščine | PRAVO | računalniška kriminaliteta | socialni okvir | socialni učinki | spolna diskriminacija | spolno nasilje

Povzetek With the rise of new technology and social media gender-based cyber violence is a constantly growing threat with impacts at individual, social and economic levels, on women and girls and on society as generally. Action taken so far has been inadequate, and the cross-border nature of gender-based cyber violence has yet to be properly addressed either. This European added value assessment (EAVA) complements the European Parliament's own initiative legislative report on Combating Gender based Violence: Cyber Violence (2020/2035(INL)). The costs to individuals and society are substantial and shown to be in the order of €49.0 to €89.3 billion. A combination of legal and non-legal policy options would generate the greatest European added value, promote the fundamental rights of victims, reduce costs imposed on individuals and society, and support law enforcement and people working with victims.

Študija EN

Multimedijske vsebine Combating gender-based violence at EU level

Strategic communications as a key factor in countering hybrid threats

Vrsta publikacije Študija

Datum 10-03-2021

Zunanji avtor DG, EPRS_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.

Politično področje Demokracija | Območje svobode, varnosti in pravice | Zunanje zadeve

Ključna beseda demokracija | dezinformacija | družbeni mediji | družboslovne vede | EVROPSKA UNIJA | geopolitika | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | obramba | ozaveščanje javnosti | POLITIKA | politika in javna varnost | politična propaganda | politični okvir | računalniška kriminaliteta | skupna zunanja in varnostna politika | terorizem | vohunjenje | ZNANOST

Povzetek 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.

Študija EN

Priloga 1 EN

Improving the common level of cybersecurity across the EU

Vrsta publikacije Briefing

Datum 11-02-2021

Avtor KONONENKO Vadim

Politično področje Varnost in obramba

Ključna beseda ekonomske analize | EVROPSKA UNIJA | evropska varnost | GOSPODARSTVO | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | obvladovanje tveganja | POLITIKA | politika in javna varnost | POSLOVANJE IN KONKURENCA | poslovodenje | pravo Evropske unije | predlog (EU) | računalniška kriminaliteta | umetna inteligenca | varnost kritične infrastrukture | varovanje tajnosti podatkov | varstvo podatkov | študija učinkov

Povzetek Drawing on the findings of an evaluation of the NIS directive, the IA generally seems to provide a clear and relevant analysis of the shortcomings of the existing NIS Directive and the available policy options for their improvement by a new legal act. It appears that the IA's assumptions are based on a thorough stocktaking exercise involving the consultation of a big number of stakeholders. The IA could however have explained in closer detail practical implications of the proposed initiative. It would have been useful if the IA had provided a fuller impact analysis particularly of potential economic costs and fundamental rights implications, as noted in the RSB opinion. Finally, the range of options assessed is limited to two in addition to the baseline. Given that the final outcome of the assessment is a significant revision of the existing legal framework, one might have expected a more granular formulation of policy options in the IA.

Briefing EN

Curbing the surge in online child abuse: The dual role of digital technology in fighting and facilitating its proliferation

Vrsta publikacije Briefing

Datum 23-11-2020

Avtor NEGREIRO ACHIAGA Maria Del Mar

Politično področje Industrija

Ključna beseda boj proti kriminalu | digitalna tehnologija | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | otrokove pravice | otroška pornografija | pedofilija | pravice in svoboščine | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | računalniška pismenost | tehnologija in tehnični predpisi | učinek informacijske tehnologije | varstvo otrok

Povzetek The volume of child abuse materials circulating on the internet has increased dramatically during the pandemic, as both children and child sex offenders spend more time, and interact more, online. Enabled by digital technologies, child sex offenders have tapped into opportunities that were previously unavailable to communicate freely and directly with each other and with children, creating online communities where they share their crimes. Today, they can reach children via webcams, connected devices and chat rooms in social media and video games, while remaining anonymous thanks to technologies such as cloud computing, the dark web, end-to-end encryption and streaming. There has been a rise in grooming and sextortion incidents. Conversely, it is again digital technologies, such as artificial intelligence (AI) and improved online age verification methods or age-appropriate design, which can help to curb the surge of the above crimes. Due to its capacity and speed of analysis, AI could play an important role in tackling the problem and assisting law enforcement in reducing the overwhelming amount of reports that need to be analysed. This is one of two EPRS briefings on the subject of fighting online child abuse. This one looks at technological aspects while the second one will cover legislative and policy issues.

Briefing EN

Directive on security of network and information systems (NIS Directive)

Vrsta publikacije Briefing

Datum 10-11-2020

Avtor ZYGIEREWICZ Anna

Politično področje Notranji trg in carinska unija | Prenos in izvajanje zakonodaje

Ključna beseda direktiva (EU) | EVROPSKA UNIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijski sistem | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvajanje prava EU | osebni podatki | pravo Evropske unije | računalniška kriminaliteta | varovanje tajnosti podatkov | varstvo podatkov

Povzetek Directive on security of network and information systems across the Union (Directive (EU) 2016/1148, NIS Directive) is the first horizontal EU cybersecurity legal act, which will be reviewed in 2020 with the aim to increase cybersecurity in the EU. The NIS Directive entered into force in August 2016 and Members States transposed it into national laws by 9 May 2018. The NIS Directive was designed to improve Member States' cybersecurity capabilities; the cooperation between Member States; and Member States' supervision of critical sectors. The Directive established a culture of risk management and incident reporting among key economic actors - operators providing essential services (OES) and Digital Service Providers (DSPs). The Directive also set out cooperation mechanisms, such as the NIS Cooperation Group and the network of national computer security incident response teams (CSIRTs).

Briefing EN

Online Platforms' Moderation of Illegal Content Online

Vrsta publikacije Na kratko

Datum 15-10-2020

Zunanji avtor Alexandre DE STREEL et al.

Politično področje Notranji trg in carinska unija | Ocena zakonodaje in politik v praksi | Varstvo potrošnikov

Ključna beseda digitalna tehnologija | enotni digitalni trg | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | računalniška pismenost | tehnologija in tehnični predpisi | učinek informacijske tehnologije | varovanje tajnosti podatkov | varstvo podatkov

Povzetek The original full study reviews and assesses the EU regulatory framework on content moderation and current practices by key online platforms. It assesses the regulation in six countries/regions and makes recommendations to improve the EU legal framework on content moderation in the context of the forthcoming Digital Services Act.

Na kratko EN

Regulating digital finance

Vrsta publikacije Na kratko

Datum 30-09-2020

Avtor DELIVORIAS Angelos

Politično področje Finančna in bančna vprašanja

Ključna beseda blokovna veriga | delo parlamenta | denarno poslovanje | FINANCE | finančna tehnologija | finančne storitve | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kreditne in finančne institucije | nova tehnologija | OKOLJE | okoljska politika | POLITIKA | potrošnja | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | tehnologija in tehnični predpisi | TRGOVINA | varovanje tajnosti podatkov | varstvo podatkov | varstvo potrošnikov | virtualna valuta | vpliv na okolje | zakonodajna pobuda

Povzetek The use of new technologies to enable and enhance the activities of the financial sector has the potential to provide significant benefits, including efficiency gains, cost reductions, improved data management and transparency. At the same time, it entails risks in fields such as financial stability, financial crime and consumer protection. These risks may further increase due to the fragmented regulatory landscape in the EU, and uneven global developments in regulating the sector. There is therefore a need for the EU to create a comprehensive and stable regulatory framework in this area. Parliament is expected to debate a legislative-initiative report with recommendations to the European Commission to act in this area during its October I plenary session.

Na kratko DE, EN, ES, FR, IT, PL

Financial Stability in the Euro Area: Assessment of Risks and Policy Options

Vrsta publikacije Študija

Datum 15-01-2020

Zunanji avtor Zsolt DARVAS, Marta DOMÍNGUEZ-JIMÉNEZ, Guntram B. WOLFF, Christopher A. HARTWELL, Salomon FIEDLER, Klaus-Jürgen GERN, Christophe BLOT, Jérôme CREEL, Paul HUBERT

Politično področje Ekonomske in monetarne zadeve

Ključna beseda denarni odnosi | dokumentacija | euroobmočje | EVROPSKA UNIJA | FINANCE | finančna stabilnost | finančno tveganje | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | obremenitve okolja | odbor EP | OKOLJE | prost pretok kapitala | raziskovalno poročilo | računalniška kriminaliteta | sprememba podnebja

Povzetek In November 2019, the ECB published its semi-annual Financial Stability Review that identified a number of risks for the euro area financial system. The Monetary Expert Panel was asked to produce four papers reflecting on these (and other) risks and available policy options.
This publication is provided by Policy Department A at the request of the Committee on Economic and Monetary Affairs (ECON).

Študija EN

ENISA and a new cybersecurity act

Vrsta publikacije Briefing

Datum 05-07-2019

Avtor NEGREIRO ACHIAGA Maria Del Mar

Politično področje Industrija | Notranji trg in carinska unija | Sprejemanje zakonodaje s strani Evropskega parlamenta in Sveta

Ključna beseda Agencija Evropske unije za kibernetsko varnost | delovanje institucij | EVROPSKA UNIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijsko omrežje | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | nacionalni parlament | parlament | POLITIKA | pravo Evropske unije | predlog (EU) | prenosno omrežje | računalniška kriminaliteta | redni zakonodajni postopek | varstvo podatkov

Povzetek In September 2017, the Commission adopted a cybersecurity package with new initiatives to further improve EU cyber-resilience, deterrence and defence. As part of these, the Commission tabled a legislative proposal to strengthen the EU Agency for Network Information Security (ENISA). Following the adoption of the Network Information Security Directive in 2016, ENISA is expected to play a broader role in the EU's cybersecurity landscape but is constrained by its current mandate and resources. The Commission presented an ambitious reform proposal, including a permanent mandate for the agency, to ensure that ENISA can not only provide expert advice, as has been the case until now, but can also perform operational tasks. The proposal also envisaged the creation of the first voluntary EU cybersecurity certification framework for ICT products, where ENISA will also play an important role. Within the European Parliament, the Industry, Research and Energy Committee adopted its report on 10 July 2018. An agreement was reached with the Council during the fifth trilogue meeting, on 10 December 2018. The text was adopted by the European Parliament on 12 March and by the Council on 9 April 2019. The new regulation came into force on 27 June 2019. Fourth edition. The ‘EU Legislation in Progress’ briefings are updated at key stages throughout the legislative procedure. Please note this document has been designed for on-line viewing.

Briefing EN

Police cooperation achievements during the legislative term 2014-2019: the role of the European Parliament

Vrsta publikacije Briefing

Datum 13-05-2019

Avtor MILT Kristiina

Politično področje Območje svobode, varnosti in pravice

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | EVROPSKA UNIJA | Evropski parlament | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | Interpol | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | MEDNARODNE ORGANIZACIJE | MEDNARODNI ODNOSI | organizirani kriminal | policijsko sodelovanje (EU) | POLITIKA | politika in javna varnost | politika sodelovanja | PRAVO | pravo Evropske unije | promet s prepovedanimi drogami | računalniška kriminaliteta | resolucija EP | svetovne organizacije | terorizem | trgovina z ljudmi | uredba (EU) | čezmejno sodelovanje

Povzetek Effective police cooperation is a key step in turning the EU into an area of freedom, security and justice (AFSJ) based on respect for fundamental rights. Cross-border law enforcement cooperation – involving the police, customs and other law enforcement services – is designed to prevent, detect and investigate criminal offences across the EU. In practice, this cooperation mainly concerns serious crime (organised crime, drug trafficking, trafficking in human beings and cybercrime) and terrorism.
Considerable progress in strengthening police cooperation was made during the 2014-2019 legislative term. Most importantly, the new Europol Regulation took effect in May 2017.
In Parliament, the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) is responsible for measures relating to police and judicial cooperation in criminal matters, including terrorism, and substantive and procedural measures relating to the development of a more coherent EU approach to criminal law, in accordance with Parliament’s Rules of Procedure.

Briefing EN

Establishing a cybersecurity competence centre and a network of national coordination centres

Vrsta publikacije Briefing

Datum 19-02-2019

Avtor KONONENKO Vadim

Politično področje Industrija | Varnost in obramba | Varstvo potrošnikov

Ključna beseda Agencija Evropske unije za kibernetsko varnost | ekonomske analize | EVROPSKA UNIJA | GOSPODARSTVO | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvajalska agencija | MEDNARODNI ODNOSI | politika sodelovanja | pravo Evropske unije | predlog (EU) | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | strategija EU | tehnologija | tehnologija in tehnični predpisi | varovanje tajnosti podatkov | varstvo podatkov | čezmejno sodelovanje | študija učinkov

Povzetek The Commission describes logically the significance of cyberdefence and the potential for improvement in this field for the EU. However, the impact assessment accompanying the proposal does not appear to have fully followed the requirements of the better regulation guidelines particularly as no open public consultation was conducted. The impact assessment presents a limited range of options as a result of a number of parameters that were pre-set from the outset and which could have constrained the scope of the impact assessment.

Briefing EN

Harmful internet use - Part II: Impact on culture and society

Vrsta publikacije Študija

Datum 31-01-2019

Zunanji avtor DG, EPRS

Politično področje Izobraževanje | Javno zdravje | Kultura | Socialna politika

Ključna beseda dezinformacija | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | javno zdravje | komunikacije | medčloveški odnosi | računalniška kriminaliteta | socialni okvir | socialni učinki | zdravstvo

Povzetek It is increasingly recognised that the internet, in spite of all its benefits to society, can also be correlated with significant harms to individuals and society. Some of these harms have been studied extensively, particularly harms to privacy, harms associated with security and cybercrime, and harms resulting from digital divides. This report covers less studied but equally important harms: harms associated with internet use that concern the health, well-being a functioning of individuals, and the impact on social structures and institutions. The Part II of the study address the harms of the internet at society level. The harms that are revised are among others: harms to cognitive development, information overload, harmful effects on knowledge and belief and harms to social relationships. The ultimate aim of the study is to develop concrete policy options to be considered by the EU Institutions and Member States, to mitigate harmful effects of the internet for European citizens.

Študija EN

Priloga 1 EN

Cybersecurity [What Think Tanks are thinking]

Vrsta publikacije Briefing

Datum 26-10-2018

Avtor CESLUK-GRAJEWSKI Marcin

Politično področje Varnost in obramba

Ključna beseda dezinformacija | ekonomska geografija | Evropa | evropska varnost | GEOGRAFIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | politična geografija | prenos podatkov | računalniška kriminaliteta | Rusija | varstvo podatkov

Povzetek Cybersecurity was back in the spotlight earlier in October, when several Western countries issued a coordinated denunciation of Russia, accusing it of running a global hacking campaign. Moscow denied the allegations. On 4 October, the UK and the Netherlands accused Moscow of sending agents to The Hague to hack into the Organisation for the Prohibition of Chemical Weapons, while the United States indicted suspected Russian agents for conspiring to hack computers and steal data to delegitimise international anti-doping organisations. They were also accused of trying to hack into Westinghouse Electric, a nuclear power company. Russia and other countries had earlier been accused of cyber-espionage, proliferation of fake news, and misuse of social media in some election campaigns. Cybersecurity can be defined as the protection of computer systems and mobile devices from theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. This note offers links to reports and commentaries from major international think-tanks and research institutes on cyber-security and related issues. More reports on the topic can be found in a previous edition of ‘What Think Tanks are thinking’, published in April 2018.

Briefing EN

Outlook for the meetings of EU Heads of State or Government, 17-18 October 2018

Vrsta publikacije Briefing

Datum 16-10-2018

Avtor ANGHEL Suzana Elena | DRACHENBERG Ralf

Politično področje Ekonomske in monetarne zadeve | Območje svobode, varnosti in pravice | Zunanje zadeve

Ključna beseda denarni odnosi | denarno poslovanje | DRUŽBENA IN SOCIALNA VPRAŠANJA | Ekonomska in monetarna unija | euroobmočje | EVROPSKA UNIJA | evropska varnost | Evropski svet | FINANCE | finance EU | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | mednarodne zadeve | MEDNARODNI ODNOSI | mednarodno pravo | migracije | migracijska politika EU | POLITIKA | politika in javna varnost | politični azil | PRAVO | računalniška kriminaliteta | sklad (EU) | sodelovanje EU-NATO | srečanje na vrhu | terorizem | čezatlantski odnosi

Povzetek As has become the norm with European Council meetings, EU Heads of State or Government will convene on 17 and 18 October 2018 in different formats with varying compositions and levels of formality: a regular meeting of the European Council, and an enlarged Euro Summit of 27 Member States on 18 October, preceded by a European Council (Article 50) meeting on the 17 October over dinner. The agenda of the European Council meeting focuses on migration and internal security. Specific foreign policy issues might also be addressed at this meeting. The Euro Summit will discuss the state of play of negotiations on the deepening of Economic and Monetary Union (EMU), with a view to the next Euro Summit in December. However, the priority issue for Heads of State or Government will be Brexit. At the European Council (Article 50) meeting, EU-27 leaders are expected to discuss the progress that has been achieved in the negotiations so far, and possibly call for an extraordinary summit in November 2018.

Briefing EN

The role of the European Council in internal security policy

Vrsta publikacije Briefing

Datum 11-10-2018

Avtor DRACHENBERG Ralf

Politično področje Območje svobode, varnosti in pravice

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomske analize | EVROPSKA UNIJA | evropska varnost | Evropski svet | GOSPODARSTVO | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | mednarodno pravo | naravna nesreča | nesreča, ki jo povzroči človek | obremenitve okolja | OKOLJE | Pogodba o delovanju EU | Pogodba o Evropski uniji | policijsko sodelovanje (EU) | POLITIKA | politika in javna varnost | PRAVO | pravo Evropske unije | prenos podatkov | računalniška kriminaliteta | Schengenski sporazum | statistika EU | terorizem | zunanja meja Evropske unije

Povzetek Due to the various terrorist attacks across the EU in recent years, internal security and the fight against terrorism have become major concerns for EU citizens as well as for the EU Heads of State or Government. The European Council has a significant Treaty-based role to play in the area of justice and home affairs, including on policy issues such as the fight against terrorism and organised crime, police cooperation and cybersecurity, often subsumed under the concept ‘internal security’. In recent years it has carried out this strategic role on various occasions but sometimes in a more reactive way often in the aftermath of major terrorist attacks. The paper also shows that while the policy fields of internal security and migration were usually clearly separated in European Council discussions, the two areas are now increasingly linked, in particular by the subject of external EU border protection. The Salzburg summit of 20 September 2018 is an example for this and also illustrates a recent trend of EU Presidencies to bring together EU Heads of State or Government in their country to discuss policy topics at the top of their own agendas.

Briefing EN

The right to respect for private life: digital challenges, a comparative-law perspective - The United Kingdom

Vrsta publikacije Študija

Datum 04-10-2018

Zunanji avtor EPRS, Comparative Law

Politično področje Območje svobode, varnosti in pravice | Ocena zakonodaje in politik v praksi

Ključna beseda digitalizacija | dokumentacija | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | dvostranski sporazum | ekonomska geografija | Evropa | GEOGRAFIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | kaznivo dejanje zoper spolno nedotakljivost | komunikacije | mednarodne zadeve | MEDNARODNI ODNOSI | osebni podatki | politična geografija | pornografija | pravice in svoboščine | PRAVO | predpisi o obdelavi podatkov | računalniška kriminaliteta | varstvo otrok | varstvo podatkov | varstvo zasebnosti | Združeno kraljestvo | čezmejni pretok podatkov

Povzetek This study forms part of a wider-ranging project which seeks to lay the groundwork for comparisons between legal frameworks governing the right to respect for private life in different legal systems, and between the ways in which the systems address the challenges that the ‘digital age’ poses to the exercise of that right. It analyses, with reference to the United Kingdom, the legislation in force, the most relevant case law and the nature of the right to respect for private life. Chapter 2 describes the concept of a right to respect for private life as it is recognised in UK legislation. This section of materials is subdivided into two parts. The first part outlines statutory protection for privacy interests, including the recently enacted Data Protection Act 2018 that gives domestic effect to the General Data Protection Regulations. The rest of chapter 2 discusses the most prominent set of statutory restrictions or qualifications upon the right. Privacy interests are thus revealed to be limited in the interests of national security and the prevention, investigation and detection of crime including crimes connected to the sexual abuse of children and young persons. Particular sets of laws authorise interception, examination and retention of digital online communications. Relevant obligations imposed on ISPs and telecommunications companies are described as are safeguards against unlawful forms of intrusion into these communications. Chapter 3 provides an overview of relevant jurisprudence in privacy related matters. A central focus of this chapter is the relatively recently developed tort of misuse of personal information. An evaluation of the overall state of UK law is offered in chapter 4. Finally, the conclusion identifies some privacy-related issues that are likely to arise in the near future.

Študija EN

An assessment of the Commission’s proposals on electronic evidence

Vrsta publikacije Študija

Datum 21-09-2018

Zunanji avtor Prof. Martin BÖSE, Professor, Rheinische Friedrich-Wilhelms-Universität Bonn

Politično področje Območje svobode, varnosti in pravice | Sprejemanje zakonodaje s strani Evropskega parlamenta in Sveta

Ključna beseda Amerika | boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomska geografija | elektronski dokaz | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazenska tožba | komunikacije | MEDNARODNI ODNOSI | organizirani kriminal | pogajanja za sklenitev sporazuma (EU) | politika sodelovanja | politična geografija | PRAVO | pravosodno sodelovanje | računalniška kriminaliteta | računalništvo v oblaku | sodstvo | Združene države | čezmejni pretok podatkov

Povzetek This study, commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs at the request of the LIBE Committee, analyses the added value and the shortcomings of the Commission’s proposals on cross-border access to electronic evidence, with a special focus on the proposals’ implications for territoriality and state sovereignty and fundamental rights of service providers and users.

Študija EN

Cyber violence and hate speech online against women

Vrsta publikacije Študija

Datum 16-08-2018

Zunanji avtor Adriane VAN DER WILK, Monika NATTER, ÖSB Consulting GmbH

Politično področje Vprašanje spola, enakost in različnost

Ključna beseda DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | družbeni mediji | elektronsko poslovanje | enakost spolov | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | ozaveščanje javnosti | POLITIKA | politika in javna varnost | pravice in svoboščine | PRAVO | psihično nasilje | računalniška kriminaliteta | TRGOVINA | trženje | varstvo otrok | varstvo podatkov | zbiranje podatkov

Povzetek This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the FEMM Committee, looks into the phenomenon of cyber violence and hate speech online against women in the European Union. After reviewing existing definitions of the different forms of cyber violence, the study assesses the root causes and impact of online violence on women. It continues by analysing and mapping the prevalence, victims and perpetrators. The document ends with an outline of the existing legal framework and recommendations for action within the EU remit.

Študija EN

Latest on the digital economy [What Think Tanks are thinking]

Vrsta publikacije Briefing

Datum 20-07-2018

Avtor CESLUK-GRAJEWSKI Marcin

Politično področje Ekonomske in monetarne zadeve | Notranji trg in carinska unija

Ključna beseda Azija in Oceanija | dezinformacija | DRUŽBENA IN SOCIALNA VPRAŠANJA | e-zdravje | ekonomska geografija | elektronsko poslovanje | enotni digitalni trg | Evropa | EVROPSKA UNIJA | FINANCE | GEOGRAFIJA | gospodarska struktura | GOSPODARSTVO | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | Kitajska | komunikacije | možganski trust | obdavčenje | obdavčitev digitalnega gospodarstva | POLITIKA | politika in javna varnost | politična geografija | politična propaganda | pravo Evropske unije | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | Rusija | sodelovalno gospodarstvo | TRGOVINA | trženje | uredba ES | varstvo podatkov | zdravstvo

Povzetek The digital revolution, which is reshaping the global economy and societies, offers numerous opportunities, but also poses many challenges, thereby putting governments in a dilemma on how to shape it. While empowering individuals in many ways and spurring impressive inventions, it poses threats of cyber-attacks and privacy abuse. It also raises concern about the future of the labour and social security markets. This note offers links to commentaries and studies on the digital economy by major international think tanks. Earlier papers on the same topic can be found in a previous edition of 'What Think Tanks are Thinking', published in May 2017.

Briefing EN

European production and preservation orders and the appointment of legal representatives for gathering electronic evidence

Vrsta publikacije Briefing

Datum 13-07-2018

Avtor TUOMINEN ULLA-MARI

Politično področje Notranji trg in carinska unija | Območje svobode, varnosti in pravice | Človekove pravice

Ključna beseda ekonomske analize | elektronski dokaz | EVROPSKA UNIJA | GOSPODARSTVO | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazenska tožba | komunikacije | MEDNARODNI ODNOSI | opravljanje storitev | osebni podatki | politika sodelovanja | PRAVO | pravo Evropske unije | predlog (EU) | pričanje | računalniška kriminaliteta | sodstvo | TRGOVINA | trženje | varstvo podatkov | čezmejno sodelovanje | študija učinkov

Povzetek The IA provides a comprehensive description of the problem and the options are clearly linked to the objectives and the problem definition. It would have benefited the analysis if coherence and complementarity between this initiative and other proposed EU legislation would have been further explained. Moreover, stakeholders' views are mentioned in a rather general way throughout the IA report and also, the problem drivers are not evenly discussed. It is to be noted that the proposed Regulation does not entirely follow the IA as it does not include legislative measures on direct access and access to databases, and on the other hand, it includes additional conditions for issuing a European Production Order.

Briefing EN

Cryptocurrencies and blockchain

Vrsta publikacije Študija

Datum 05-07-2018

Zunanji avtor Prof. Dr. Robby HOUBEN and Alexander SNYERS, University of Antwerp, Research Group Business & Law, Belgium

Politično področje Ekonomske in monetarne zadeve | Finančna in bančna vprašanja

Ključna beseda boj proti kriminalu | davčna utaja | denarni odnosi | denarno poslovanje | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | država članica EU | ekonomska geografija | elektronski denar | elektronsko bančništvo | emisija denarja | FINANCE | finančne storitve | GEOGRAFIJA | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | kreditne in finančne institucije | mednarodna valuta | ogrožanje državne varnosti | POLITIKA | politika in javna varnost | pranje denarja | PRAVO | prost pretok kapitala | računalniška kriminaliteta | terorizem | virtualna valuta

Povzetek More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide. This paper prepared by Policy Department A elaborates on this phenomenon from a legal perspective, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion. It contains policy recommendations for future EU standards.

Študija EN

Virtual currencies and terrorist financing: assessing the risks and evaluating responses

Vrsta publikacije Študija

Datum 04-06-2018

Zunanji avtor Tom KEATINGE, David CARLISLE, Florence KEEN

Politično področje Dolgoročno načrtovanje | Območje svobode, varnosti in pravice

Ključna beseda boj proti kriminalu | denarno poslovanje | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | elektronsko bančništvo | EVROPSKA UNIJA | FINANCE | financiranje terorizma | finančna zakonodaja | finančne storitve | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | kreditne in finančne institucije | ogrožanje državne varnosti | plačilni sistem | policijsko sodelovanje (EU) | POLITIKA | politika in javna varnost | pranje denarja | PRAVO | pretok kapitala | prost pretok kapitala | računalniška kriminaliteta | virtualna valuta

Povzetek This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the TERR Committee, explores the terrorist financing (TF) risks of virtual currencies (VCs), including cryptocurrencies such as Bitcoin. It describes the features of VCs that present TF risks, and reviews the open source literature on terrorist use of virtual currencies to understand the current state and likely future manifestation of the risk. It then reviews the regulatory and law enforcement response in the EU and beyond, assessing the effectiveness of measures taken to date. Finally, it provides recommendations for EU policymakers and other relevant stakeholders for ensuring the TF risks of VCs are adequately mitigated.

Študija EN

Cyber-security [What Think Tanks are thinking]

Vrsta publikacije Briefing

Datum 27-04-2018

Avtor CESLUK-GRAJEWSKI Marcin

Politično področje Varnost in obramba

Ključna beseda boj proti kriminalu | digitalizacija | dokumentacija | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | država članica EU | ekonomska geografija | Evropa | evropska varnost | GEOGRAFIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | možganski trust | obramba | obrambna politika | politična geografija | pravice in svoboščine | PRAVO | prenosno omrežje | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | Rusija | varstvo podatkov | varstvo zasebnosti

Povzetek Cyber-security can be defined as the protection of computer systems and mobile devices from theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. Cyber-crime and cyber-attacks have become a growing threat to governments, businesses and individuals as digital technologies advance. There have also been allegations of cyber-espionage, proliferation of fake news and misuse of social media in some electoral campaigns. The European Commission updated the European Union's cyber-security strategy in September 2017, to promote cyber-resilience and joint response across the bloc. This note offers links to reports and commentaries from some major international think-tanks and research institutes on cyber-security and relations issues. More reports on the topic can be found in a previous edition of 'What Think Tanks are thinking', published in February 2017.

Briefing EN

Public Security Exception in the Area of non-personal Data in the European Union

Vrsta publikacije Briefing

Datum 16-04-2018

Zunanji avtor Dr. Kristina Irion

Politično področje Dolgoročno načrtovanje | Notranji trg in carinska unija | Ocena zakonodaje in politik v praksi | Pravo EU: pravni sistem in akti | Sprejemanje zakonodaje s strani Evropskega parlamenta in Sveta | Varstvo potrošnikov

Ključna beseda digitalna tehnologija | dokumentacijska obdelava podatkov | dostop do informacij | država članica EU | ekonomska geografija | enotni digitalni trg | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | pravice in svoboščine | PRAVO | pravo EU | pravo Evropske unije | predpisi o obdelavi podatkov | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | shranjevanje podatkov | tehnologija in tehnični predpisi | varstvo podatkov | zaščita komunikacij | čezmejni pretok podatkov

Povzetek In order to avoid conflict with the freedom to conduct a business and the freedom of contract the wording of article 4(1) should be amended and be addressed to the Member States;
• The proposal underplays that information security has a legal dimension to it, notoriously so because member states' national security activities operate outside the scope of EU law;
• The principle aversion against locality that emanates from the proposal may not be fully aligned with state-of-the-art technology where multiple data mirrors geographically distribute a dataset. For example, one local mirror is advisable for business continuity in the event of a disruption of transmission infrastructure;
• Not all non-personal data is created equal; from the stream of non-personal data that is for example generated in the Internet of Things (IoT) data necessary to control real world devises should in addition be locally accessible;
• Whithout contradicting the philosophy behind the free flow of non-personal data proposal this briefing presents examples for interventions that should be justifyable on grounds of public policy or the protection of health and life of humans, animals or plants.

Briefing EN

Optimal Scope for Free Flow of Non-Personal Data in Europe

Vrsta publikacije Briefing

Datum 15-03-2018

Zunanji avtor Dr. Simon Forge

Politično področje Dolgoročno načrtovanje | Notranji trg in carinska unija | Ocena zakonodaje in politik v praksi | Pravo EU: pravni sistem in akti | Sprejemanje zakonodaje s strani Evropskega parlamenta in Sveta | Varstvo potrošnikov

Ključna beseda digitalna tehnologija | dokumentacijska obdelava podatkov | dostop do informacij | država članica EU | ekonomska geografija | enotni digitalni trg | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | odprti podatki | pravice in svoboščine | PRAVO | pravo EU | pravo Evropske unije | predpisi o obdelavi podatkov | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | shranjevanje podatkov | tehnologija in tehnični predpisi | varstvo podatkov | zaupnost | zaščita komunikacij | čezmejni pretok podatkov

Povzetek Data is not static in a personal/non-personal classification – with modern analytic methods, certain non-personal data can help to generate personal data – so the distinction may become blurred. Thus, de-anonymisation techniques with advances in artificial intelligence (AI) and manipulation of large datasets will become a major issue.
In some new applications, such as smart cities and connected cars, the enormous volumes of data gathered may be used for personal information as well as for non-personal functions, so such data may cross over from the technical and non-personal into the personal domain.
A debate is taking place on whether current EU restrictions on confidentiality of personal private information should be relaxed so as to include personal information in free and open data flows. However, it is unlikely that a loosening of such rules will be positive for the growth of open data. Public distrust of open data flows may be exacerbated because of fears of potential commercial misuse of such data, as well of leakages, cyberattacks, and so on.
The proposed recommendations are: to promote the use of open data licences to build trust and openness, promote sharing of private enterprises' data within vertical sectors and across sectors to increase the volume of open data through incentive programmes, support testing for contamination of open data mixed with personal data to ensure open data is scrubbed clean - and so reinforce public confidence, ensure anti-competitive behaviour does not compromise the open data initiative.

Briefing EN

The underlying causes of the digital gender gap and possible solutions for enhanced digital inclusion of women and girls

Vrsta publikacije Študija

Datum 15-02-2018

Zunanji avtor MS KONSTANTINA DAVAKI

Politično področje Pravo intelektualne lastnine | Vprašanje spola, enakost in različnost

Ključna beseda digitalizacija | digitalna tehnologija | digitalni razkorak | dokumentacija | enakost spolov | informacije in obdelava informacij | informacijska tehnologija | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | poklici v informatiki | pravice in svoboščine | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | strokovno izpopolnjevanje | tehnologija in tehnični predpisi | trg dela | trg dela | zaposlovanje | ZAPOSLOVANJE IN DELOVNE RAZMERE

Povzetek This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the FEMM Committee, attempts to reveal the links between the different factors (access, skills, socio-economic and cultural), which prevent women from having equal access to digital technology. It then suggests ways of dealing with online and offline inequalities to the effect of closing the digital gender gap and improving women's and girls' digital inclusion and future technology-related career paths.

Študija EN

Ten issues to watch in 2018

Vrsta publikacije: Poglobljena analiza

Datum: 08-01-2018

Avtor: BASSOT Etienne

Politično področje: Demokracija | Demokracija EU, institucionalno in parlamentarno pravo | Ekonomske in monetarne zadeve | Finančna in bančna vprašanja | Izobraževanje | Območje svobode, varnosti in pravice | Pravo EU: pravni sistem in akti | Socialna politika | Varnost in obramba | Vprašanje spola, enakost in različnost | Zunanje zadeve

Ključna beseda: Azija in Oceanija | denarni odnosi | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomska geografija | euroobmočje | Evropa | EVROPSKA UNIJA | evropske volitve | Evropski parlament | FINANCE | finance EU | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | izstop iz EU | mednarodne zadeve | mednarodni odnosi | MEDNARODNI ODNOSI | migracija | migracije | mladinska politika | POLITIKA | politika in javna varnost | politična geografija | proračun EU | računalniška kriminaliteta | Severna Koreja | socialna neenakost | socialni okvir | strategija EU | terorizem | varstvo podatkov | volilni postopek in glasovanje | Združeno kraljestvo

Povzetek: This is the second edition of an annual EPRS publication designed to identify key issues and policy areas that are likely to feature prominently on the political agenda of the European Union over the coming year. Topics presented include: the implications for the EU of the terrorism threat, the North Korean issue, the security challenges posed by disinformation, fake news and cyber-crime, the ongoing migration crisis and rising inequalities. Other important policy areas covered are youth empowerment, the EU budget, the future of the euro area, the European elections in 2019 and, last but not least, Brexit.

Poglobljena analiza: DE, EN, ES, FR, IT, PL

Achieving a sovereign and trustworthy ICT industry in the EU

Vrsta publikacije: Študija

Datum: 20-12-2017

Zunanji avtor: EPRS, DG

Politično področje: Dolgoročno načrtovanje | Industrija | Območje svobode, varnosti in pravice | Varstvo potrošnikov

Ključna beseda: boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | enotni digitalni trg | EVROPSKA UNIJA | graditev Evrope | industrija informacijske tehnologije | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kvalificiran delavec | MEDNARODNI ODNOSI | ozaveščanje javnosti | POLITIKA | politika in javna varnost | politika sodelovanja | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | raziskave in razvoj | računalniška kriminaliteta | tehnologija | tehnologija in tehnični predpisi | tretja država | trg dela | učinek informacijske tehnologije | ZAPOSLOVANJE IN DELOVNE RAZMERE

Povzetek: This study attempts to identify and assess policy options for the EU to achieve cyber-resilience, and to develop capabilities, and industrial and technological resources for a trustworthy EU cyberspace, with a view also to promoting core values, such as online privacy protection. The findings could form the basis for an assessment of alternative measures to improve the resilience of the European ICT industry and the EU's strategic decision-making capacity, and enhance the resilience of critical information technology networks. The study further reviews the current state of reciprocity between search engine services and individual customers. The ultimate aim of this study is to develop concrete policy options to be considered by EU institutions and Member States – and potentially to be used as background by EP committees for their legislative and own-initiative reports.

Študija: DE, EN, FR

Priloga 1: EN

EU Cybersecurity Agency and cybersecurity certification

Vrsta publikacije: Briefing

Datum: 20-12-2017

Avtor: EISELE Katharina

Politično področje: Industrija | Notranji trg in carinska unija | Območje svobode, varnosti in pravice

Ključna beseda: Agencija Evropske unije za kibernetsko varnost | delovanje institucij | ekonomske analize | EVROPSKA UNIJA | GOSPODARSTVO | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijsko omrežje | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | prenosno omrežje | računalniška kriminaliteta | varstvo podatkov | študija učinkov

Povzetek: This note seeks to provide an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above proposal, which is the main part of the 'Cybersecurity package', submitted on 13 September 2017 and referred to Parliament's Committee on Industry, Research and Energy (ITRE). As announced in the State of the Union Address 2017 and the Commission's communication on Europe's Cyber Resilience System and Cybersecurity Industry, the initiative aims to reform the European Union Agency for Network and Information Security (ENISA or 'Agency') in order to enhance its supporting functions for Member States in achieving cybersecurity resilience and to acknowledge the Agency's responsibilities under the new directive on security of network and information systems (NIS Directive). In addition, the proposal establishes a voluntary European cybersecurity certification framework to promote such certification schemes for specific information and communication technology (ICT) products and services, and to allow for mutual recognition of certificates so as to avoid further market fragmentation.

Briefing: EN

Perspectives on transatlantic cooperation: Transatlantic cyber-insecurity and cybercrime - Economic impact and future prospects

Vrsta publikacije Študija

Datum 07-12-2017

Zunanji avtor Benjamin C. Dean, Iconoclast Tech
Foreword by Patryk Pawlak, formerly of EPRS, now of EU Institute for Security Studies
Administrator responsible: Elena Lazarou, Members' Research Service, EPRS

Politično področje Varnost in obramba | Zunanje zadeve

Ključna beseda EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | javna varnost | kazensko pravo | kibernetika | meddržavno sodelovanje (EU) | mednarodne zadeve | MEDNARODNI ODNOSI | naravoslovne in uporabne vede | ogrožanje državne varnosti | POLITIKA | politika in javna varnost | PRAVO | razkritje informacij | računalniška kriminaliteta | varovanje tajnosti podatkov | ZNANOST | čezatlantski odnosi

Povzetek Over the past two decades, an 'open' internet and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the spread of insecure digital technologies has also enabled costly new forms of crime, and created systemic risks to transatlantic and national critical infrastructure, threatening economic growth and development. The transnational nature of these phenomena make it very difficult for effective policy solutions to be implemented unilaterally by any one jurisdiction. Cooperation between stakeholders in both the EU and US is required in the development and implementation of policies to increase the security of digital technologies and increase societal resilience to the cybersecurity risks associated with critical infrastructure. Although there is a great deal of congruence between the stated policy goals in both the EU and US, obstacles to effective cooperation impede effective transatlantic policy development and implementation in some areas. This study examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues that policy-makers on either side of the Atlantic could work together on, and explains where effective cooperation is sometimes impeded.

Študija EN

Digitising Industry (Industry 4.0) and Cybersecurity

Vrsta publikacije Briefing

Datum 18-10-2017

Avtor GYORFFI Miklos Laszlo

Politično področje Industrija | Ocena zakonodaje in politik v praksi

Ključna beseda digitalizacija | dokumentacija | država članica EU | ekonomska geografija | enotni digitalni trg | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | industrijsko izdelovanje | informacije in obdelava informacij | informacijska tehnologija | informacijska tehnologija in obdelava podatkov | informatika | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | javna varnost | komunikacije | POLITIKA | politika in javna varnost | prenosno omrežje | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | strategija EU | tehnologija in tehnični predpisi | varstvo podatkov

Povzetek The digitalisation of manufacturing industry, i.e. employing in depth digital technologies for the performance of good production raises additional cybersecurity questions. Currently EU cybersecurity policies are mainly targeting network security and large infrastructures of public interest, with little emphasis on the needs of a digitised industry. Still, recent policy developments do provide framework of possibly covering these needs.

Briefing EN

The digital economy in the EU [What Think Tanks are thinking]

Vrsta publikacije Briefing

Datum 19-05-2017

Avtor CESLUK-GRAJEWSKI Marcin

Politično področje Notranji trg in carinska unija

Ključna beseda digitalna tehnologija | digitalni razkorak | enotni digitalni trg | EVROPSKA UNIJA | evropska varnost | gospodarska rast | gospodarska reforma | gospodarska struktura | gospodarske razmere | GOSPODARSTVO | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | možganski trust | obdelava podatkov | odprti podatki | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | strokovno izpopolnjevanje | tehnologija in tehnični predpisi | telekomunikacijska politika | zaposlovanje | ZAPOSLOVANJE IN DELOVNE RAZMERE | zbiranje podatkov

Povzetek The digital revolution is reshaping the European Union's economy, from financial services and telecoms to creative industries and the way workers are employed. While posing certain threats, such as cyber-attacks, new technologies offer vast opportunities, provided that people acquire the right skill-sets to underpin their use. Seeking to tap the full potential of digitalisation, the European Commission is pushing ahead with its Digital Single Market Strategy. On 10 May, it presented a mid-term review of this strategy, calling for swift approval of proposals already presented and outlining further actions on online platforms, the data economy and cybersecurity. This note offers links to recent studies and reports from major international think tanks and research institutes on problems and opportunities relating to digitalisation.

Briefing EN

The European Union Agency for Network and Information Security (ENISA)

Vrsta publikacije Briefing

Datum 19-05-2017

Avtor ZYGIEREWICZ Anna

Politično področje Ocena zakonodaje in politik v praksi | Prenos in izvajanje zakonodaje | Varnost in obramba

Ključna beseda Agencija Evropske unije za kibernetsko varnost | delovanje institucij | dokumentacija | ekonomske analize | EVROPSKA UNIJA | evropska varnost | Evropski parlament | GOSPODARSTVO | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | institucionalne pristojnosti (EU) | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvršilna oblast in javna uprava | javno posvetovanje | javno-zasebno partnerstvo | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | okvirni program za raziskave in razvoj | POLITIKA | poročilo o dejavnosti | pravo Evropske unije | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | statistika EU | uredba (EU)

Povzetek Information and communication technologies play an increasing role in modern-day life and in the creation of a digital society. To ensure further growth, significant investments in security are necessary. Cybersecurity is a growing concern for citizens, influencing their digital activity. It is also a significant cost for the economy. In 2015, the estimated worldwide economic impact of cyber-attacks reached US$500 billion. The cybersecurity market in Europe was estimated at €20.1 billion. The European Union Agency for Network and Information Security (ENISA) was established to support the EU and the Member States in enhancing and strengthening their ability to prevent, detect and respond to network and information security (NIS) problems and incidents. ENISA is part of the broader legal and policy environment, which includes the EU cybersecurity strategy and the recently adopted directive on security of networks and information systems across the EU.

Briefing EN

Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU

Vrsta publikacije Študija

Datum 16-05-2017

Zunanji avtor EPRS, DG; Panagiotis Trimintzios, Georgios Chatzichristos, Silvia Portesi, Prokopios Drogkaris, Lauri Palkmets, Dimitra Liveri and Andrea Dufkova.

Politično področje Varnost in obramba

Ključna beseda brezpilotni zrakoplov | država članica EU | ekonomska geografija | EVROPSKA UNIJA | evropska varnost | GEOGRAFIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucija EU | institucije EU in evropska javna uprava | institucionalne pristojnosti (EU) | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvršilna oblast in javna uprava | javno-zasebno partnerstvo | klasifikacija podjetij | komunikacije | mednarodna organizacija | mednarodna varnost | MEDNARODNE ORGANIZACIJE | mednarodne zadeve | MEDNARODNI ODNOSI | NATO | POLITIKA | politika sodelovanja | POSLOVANJE IN KONKURENCA | PROMET | računalniška kriminaliteta | skupna varnostna in obrambna politika | sodelovanje EU-NATO | strokovno izpopolnjevanje | svetovne organizacije | tretja država | zaposlovanje | ZAPOSLOVANJE IN DELOVNE RAZMERE | zasebno podjetje | zračni in vesoljski promet

Povzetek This report is the result of a study conducted by the European Union Agency for Network and Information Security (ENISA) for the European Parliament's Science and Technology Options Assessment (STOA) Panel with the aim of identifying risks, challenges and opportunities for cyber-defence in the context of the EU Common Security and Defence Policy (CSDP). Acceptance of cyber as an independent domain calls for the investigation of its integration with the EU's current and future policies and capabilities. ENISA analysed the related literature and work on cybersecurity, including its own publications, to form the basis for this study. In addition, a number of stakeholders, experts and practitioners, from academia, EU institutions and international organisations, were consulted in order to ensure the study is well-founded and comprehensive. The study revolves around three thematic areas, namely: policies, capacity building, and the integration of cyber in the CSDP missions, with the last one being the main focus of the study. For each thematic area, we compile a set of policy options, covering different levels, starting from the EU's political/strategic level and progressing down to the operational and even tactical/technical levels of the CSDP's supporting mechanisms. These policy options are summarised in a separate options briefing document accompanying this study.

Študija EN

Priloga EN

Priloga 2 FR

Priloga 3 DE

Cyber Security Strategy for the Energy Sector

Vrsta publikacije Na kratko

Datum 22-03-2017

Avtor GOUARDERES Frederic

Politično področje Dolgoročno načrtovanje | Energija | Industrija | Raziskovalna politika

Ključna beseda digitalna tehnologija | ENERGETIKA | energetika | energetska politika | energetska politika EU | evropska varnost | informacijska tehnologija in obdelava podatkov | informacijsko vojskovanje | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | tehnologija in tehnični predpisi | varovanje tajnosti podatkov

Povzetek The study Cyber Security Strategy for the Energy Sector explores the development of energy specific cyber security solutions and defensive practices. It provides an assessment of existing European policies and legislation to address cyber security in the energy sector and recommends additional policy prescriptions that may be necessary to protect Europe and its citizens. This leaflet presents short summary of this study. Link to the original publication: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

Na kratko EN

Countering hybrid threats: EU-NATO cooperation

Vrsta publikacije Briefing

Datum 02-03-2017

Avtor PAWLAK Patryk

Politično področje Varnost in obramba

Ključna beseda DRUŽBENA IN SOCIALNA VPRAŠANJA | EVROPSKA UNIJA | evropska varnost | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | javna varnost | kazensko pravo | mednarodna varnost | MEDNARODNE ORGANIZACIJE | MEDNARODNI ODNOSI | mednarodno pravo | NATO | nesreča, ki jo povzroči človek | obremenitve okolja | ogrožanje državne varnosti | OKOLJE | okoljska politika | POLITIKA | politika in javna varnost | politika sodelovanja | PRAVO | PROMET | prometna politika | računalniška kriminaliteta | skupna zunanja in varnostna politika | svetovne organizacije | tehnološka nevarnost | tretja država | tveganje za zdravje | varnost prevoza | vojaško sodelovanje | vzajemna pomoč | zdravstvo

Povzetek The concept of hybrid threat has gained traction in relation to Russia's actions in Ukraine and the ISIL/Da'esh campaigns going far beyond Syria and Iraq. Faced with this constantly evolving challenge, the European Union and NATO have taken several steps to strengthen their respective capabilities and pursue common objectives through closer cooperation. The EU-NATO joint declaration adopted in July 2016 in the margins of the Warsaw NATO Summit represents a clear step forward in this regard. The document outlines new areas for practical cooperation, in particular with regard to hybrid threats, building resilience in cybersecurity, and strategic communications. The Council conclusions of 6 December 2016 stressed that the implementation of the joint declaration is a key political priority for the EU. It welcomed the progress achieved in advancing EU-NATO relations, including implementing and operationalising parallel procedures and playbooks for interaction in countering hybrid threats. With a view to ensuring further progress, the Council endorsed a common set of proposals focused on better coordination, situational awareness, strategic communication, crisis response, and bolstering resilience. The North Atlantic Council endorsed the same set of measures. Reports on implementation, including possible suggestions for future cooperation, should be provided on a biannual basis from the end of June 2017. This is an updated edition of an At a Glance note published in June 2015.

Briefing EN

Multimedijske vsebine Countering hybrid threats: EU-NATO cooperation [Policy Podcast]

A global strategy on foreign and security policy for the EU

Vrsta publikacije Briefing

Datum 02-03-2017

Avtor PAWLAK Patryk

Politično področje Globalno upravljanje | Varnost in obramba

Ključna beseda brezpilotni zrakoplov | civilna misija EU | država članica EU | ekonomska geografija | ekonomske analize | evropska obrambna politika | EVROPSKA UNIJA | GEOGRAFIJA | GOSPODARSTVO | graditev Evrope | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | oborožene sile | obramba | politika sodelovanja | PROMET | računalniška kriminaliteta | satelitske komunikacije | skupna varnostna in obrambna politika | statistika EU | tretja država | vojaška misija EU | Vojaški odbor Evropske unije | vojaško sodelovanje | zračni in vesoljski promet | zunanja politika

Povzetek Tracking European Commission priority initiatives in 2017 – Number 1 The letter from Donald Tusk, President of the European Council, of 31 January 2017, notes that 'the challenges currently facing the European Union are more dangerous than ever before in the time since the signature of the Treaty of Rome'. Indeed, the current evolving international environment and geopolitical shifts highlight the need for effective and coherent implementation of the EU global strategy. The top strategic priorities for the implementation of the strategy, as decided by the Foreign Affairs Council on 17 October 2016 include: security and defence; building resilience and an integrated approach to conflicts and crises; addressing the internal/external security nexus; updating existing strategies and preparing new ones; and enhancing public diplomacy. Strengthening EU cooperation on external security and defence was also discussed at the European Council meeting in December 2016. Heads of State or Government focused on three priorities: implementation of the EU global strategy in the security and defence area, the European defence action plan, and the implementation of the EU-NATO Joint Declaration signed in Warsaw in July 2016. The first implementation report is expected in June 2017. This is an updated edition of a briefing published in April 2016.

Briefing EN

Cyber-security [What Think Tank are thinking]

Vrsta publikacije Briefing

Datum 03-02-2017

Avtor CESLUK-GRAJEWSKI Marcin

Politično področje Varnost in obramba

Ključna beseda ekonomska geografija | ENERGETIKA | energetska politika | Evropa | GEOGRAFIJA | industrijska špijonaža | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | možganski trust | nahajališče energetskega vira | ogrožanje državne varnosti | POLITIKA | politika in javna varnost | politična geografija | PRAVO | prenosno omrežje | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | Rusija | tehnologija in tehnični predpisi | terorizem | varstvo podatkov | volilni postopek in glasovanje | volitve

Povzetek Allegations of interference in the US electoral campaign in 2016 through cyber espionage and leaks have put the spotlight on cyber-security and cybercrime, not only for ensuring financial or strategic advantages, but increasingly as means of pursuing political aims. As digital technologies grow in importance, the clear view among analysts is that cyber-crime is becoming a major threat to governments, businesses and societies as a whole. This note offers links to reports and commentaries from some major international think tanks and research institutes on cyber-security and related issues.

Briefing EN

The 2016 “Winter Package” on European Security and Defence: Constitutional, Legal and Institutional Implications

Vrsta publikacije Poglobljena analiza

Datum 16-12-2016

Zunanji avtor Steven Blockmans (CEPS and University of Amsterdam, the Netherlands)

Politično področje Pravo EU: pravni sistem in akti

Ključna beseda brezpilotni zrakoplov | država članica EU | ekonomska geografija | ekonomske analize | evropska obrambna politika | EVROPSKA UNIJA | evropska varnost | GEOGRAFIJA | GOSPODARSTVO | graditev Evrope | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | oborožene sile | obramba | politika sodelovanja | PROMET | računalniška kriminaliteta | satelitske komunikacije | skupna varnostna in obrambna politika | statistika EU | vojaška misija EU | Vojaški odbor Evropske unije | vojaško letalstvo | vojaško sodelovanje | zračni in vesoljski promet | zunanja politika

Povzetek This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Constitutional Affairs of the European Parliament. It examines a series of constitutional, legal and institutional implications of the proposals endorsed by the December 2016 European Council for the further development of the Common Security and Defence Policy in the framework of the current Treaties.

Poglobljena analiza EN

The European Council and European defence cooperation: Developments since June 2016

Vrsta publikacije Briefing

Datum 12-12-2016

Avtor ANGHEL Suzana Elena

Politično področje Varnost in obramba

Ključna beseda brezpilotni zrakoplov | civilna misija EU | država članica EU | ekonomska geografija | ekonomske analize | evropska obrambna politika | EVROPSKA UNIJA | Evropski svet | GEOGRAFIJA | GOSPODARSTVO | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | obramba | politika sodelovanja | PROMET | računalniška kriminaliteta | satelitske komunikacije | skupna varnostna in obrambna politika | statistika EU | vojaška misija EU | Vojaški odbor Evropske unije | vojaško letalstvo | vojaško sodelovanje | zračni in vesoljski promet | zunanja politika

Povzetek At its December 2016 meeting, the European Council will consider options for strengthening European defence cooperation. This paper focuses on security and defence developments since June 2016, when the European Council last addressed security and defence, in particular EU-NATO cooperation. It considers the process that led to the inclusion of security and defence on the December 2016 European Council agenda, as well as the expected outcome of the meeting.

Briefing EN

Cyber Security Strategy for the Energy Sector

Vrsta publikacije Študija

Datum 05-12-2016

Zunanji avtor David Healey (Analysys Mason Limited), Sacha Meckler (nalysys Mason Ltd.), Usen Antia (nalysys Mason Ltd.) and Edward Cottle (nalysys Mason Ltd.)

Politično področje Dolgoročno načrtovanje | Energija | Industrija | Raziskovalna politika

Ključna beseda digitalna tehnologija | ENERGETIKA | energetika | energetska politika | Evropa | evropska varnost | evropsko sodelovanje | GEOGRAFIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvršilna oblast in javna uprava | javno-zasebno partnerstvo | kazensko pravo | mednarodna varnost | MEDNARODNI ODNOSI | ogrožanje državne varnosti | POLITIKA | politika sodelovanja | politična geografija | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | standardizacija | tehnologija in tehnični predpisi | Ukrajina | usklajevanje standardov

Povzetek This study is provided by the Policy Directorate at the request of the ITRE Committee.
The EU energy infrastructure is transitioning into a decentralised, digitalised smart energy system. Already, energy operations are increasingly becoming the target of cyber-attacks with potentially catastrophic consequences. Development of energy specific cyber security solutions and defensive practices are therefore essential. Urgent action is required, including empowering a coordination body, to promote sharing of incident information, development of best practice and relevant standards.

Študija EN

Research for TRAN Committee - Prospects for “Remote” En-Route Air Traffic Services

Vrsta publikacije Študija

Datum 15-08-2016

Zunanji avtor Stephen Wainwright and Rosie Offord, Mark Scott (Steer Davies Gleave)

Politično področje Dolgoročno načrtovanje | Promet | Turizem

Ključna beseda brezžične telekomunikacije | Evropska agencija za varnost v letalstvu | EVROPSKA UNIJA | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | prevozni predpisi | PROMET | prometna politika | računalniška kriminaliteta | satelitske komunikacije | varnost prevoza | zračni in vesoljski promet | zračni promet

Povzetek Remote tower services, where aircraft at an airport are remote-controlled from a separate location, have been introduced to some airports and are being tested at several others. By reviewing the current and emerging technologies, considering some of the risks associated with these technologies and evaluating the contribution of the NextGen and SESAR programmes, this paper aims to assess the feasibility of also providing “remote” en-route Air Traffic Services in Europe.

Študija EN

EYE 2016 – Golden Eye: Who rules tomorrow's Europe?

Vrsta publikacije Na kratko

Datum 28-04-2016

Avtor MONTELEONE Shara

Politično področje Območje svobode, varnosti in pravice

Ključna beseda digitalni razkorak | eksteritorialnost | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodno pravo | organizacija prevoza | osebni podatki | pravice in svoboščine | PRAVO | prevoz oseb | PROMET | računalniška kriminaliteta | svoboda izražanja | varstvo podatkov | varstvo zasebnosti

Povzetek The development of digital technologies has made access to and availability of personal data easier for companies, public authorities and citizens. Keeping control over our personal data means keeping control over our life. Personal data collection and processing are regulated by EU law with the aim of striking a balance between rights to privacy and to data protection and other rights or interests (e.g. freedom of expression, public security). 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

Na kratko EN

EYE 2016 – Cyber-attacks: Visible danger, invisible enemy

Vrsta publikacije Na kratko

Datum 28-04-2016

Avtor PAWLAK Patryk

Politično področje Varnost in obramba

Ključna beseda Agencija Evropske unije za kibernetsko varnost | boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | EVROPSKA UNIJA | evropska varnost | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | intelektualna lastnina | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | mednarodna varnost | MEDNARODNI ODNOSI | mednarodno sodelovanje | ogrožanje državne varnosti | POLITIKA | politika in javna varnost | politika sodelovanja | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | računalniško piratstvo | skupna varnostna in obrambna politika | terorizem | učinek informacijske tehnologije

Povzetek The advance of information and communication technologies (ICT) has created numerous opportunities for human development, and reshaped the ways in which our societies communicate, work or learn. However, our reliance on internet-based platforms can also be a source of vulnerability, exploited by criminal networks for financial or political aims. XXXXXXXX Please click here for the full publication in PDF format

Na kratko EN

Data protection reform package: Final steps

Vrsta publikacije Na kratko

Datum 12-04-2016

Avtor MONTELEONE Shara

Politično področje Območje svobode, varnosti in pravice

Ključna beseda EVROPSKA UNIJA | Evropski Nadzornik za varstvo podatkov | graditev Evrope | informacije in obdelava informacij | informacijska družba | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | Listina EU o temeljnih pravicah | osebni podatki | policijsko sodelovanje (EU) | pravice in svoboščine | PRAVO | prenos podatkov | razkritje informacij | računalniška kriminaliteta | varovanje tajnosti podatkov | varstvo podatkov | varstvo zasebnosti

Povzetek A package to reform the EU legal framework on data protection (DP) was presented by the European Commission in January 2012. Aimed at strengthening citizens' rights uniformly while reducing burdens for companies and public authorities, the package takes a comprehensive approach, including a general regulation and a directive concerning data protection for police and law enforcement purposes. Following negotiations towards a second-reading agreement, compromises on both texts have been reached, and votes in plenary, scheduled for the April I session, are now required to confirm them.

Na kratko EN

EU-US cooperation in Justice and Home Affairs – an overview

Vrsta publikacije Briefing

Datum 06-04-2016

Avtor CIRLIG Carmen-Cristina

Politično področje Območje svobode, varnosti in pravice | Zunanje zadeve

Ključna beseda Amerika | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomska geografija | ekstremizem | Evropska unija | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | izmenjava informacij | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodne zadeve | MEDNARODNI ODNOSI | mednarodni sporazum | mejna kontrola | migracija | migracije | območje svobode, varnosti in pravice | odnosi EU | POLITIKA | politika in javna varnost | politična geografija | pristojnosti EP | računalniška kriminaliteta | sodelovanje na področju notranjih zadev | terorizem | varstvo podatkov | Združene države

Povzetek The United States is the key partner of the European Union in the area of justice and home affairs (JHA), including in the fight against terrorism. While formal cooperation on JHA issues between the US and the EU goes back to the 1995 New Transatlantic Agenda, it is since 2001 in particular that cooperation has intensified. Today, and for the period up until 2020, the key areas of transatlantic efforts in the JHA field are personal data protection, counter-terrorism and countering violent extremism, migration and border controls, tracing of firearms and explosives, money laundering and terrorism financing, cybercrime, drugs and information exchange. Regular dialogues at all levels, extensive operational cooperation and a series of legal agreements demonstrate the development of the transatlantic partnership on JHA. Assessments state that cooperation on law enforcement and counter-terrorism has led to hundreds of successful joint operations each year, and many foiled terrorist plots. Nevertheless, important challenges remain, in particular in light of the revelations of US mass surveillance activities and the resultant growth in EU concerns about US standards for data privacy. The European Parliament is making use of its extended powers in the JHA field, by urging a high level of data protection as well as effective and non-discriminatory means of redress for EU citizens in the US over improper use of their personal data.

Briefing EN

Multimedijske vsebine EU-US cooperation in Justice and Home Affairs – an overview

A New Deal for energy consumers

Vrsta publikacije Briefing

Datum 05-01-2016

Avtor WILSON Alex Benjamin

Politično področje Energija

Ključna beseda cena energije | cene | določanje cen | DRUŽBENA IN SOCIALNA VPRAŠANJA | ENERGETIKA | energetska politika | energetska učinkovitost | FINANCE | INDUSTRIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | merilna naprava | pomoč socialno ogroženim | potrošniška cena | potrošnja | pravice in svoboščine | PRAVO | računalniška kriminaliteta | socialno varstvo | strojegradnja | TRGOVINA | varstvo podatkov | varstvo potrošnikov | varstvo zasebnosti | varčevanje z energijo

Povzetek On 15 July 2015, the European Commission adopted a Communication on Delivering a New Deal for energy consumers ('New Deal'), as part of the Summer Energy Package. The New Deal is one of several consumer-related actions envisaged in the Energy Union strategy, and is designed to inform future actions in this field, including proposed legislation.

The New Deal highlights the need for greater transparency around energy prices: wholesale and retail prices are diverging as taxes account for a growing share of energy bills, placing a disproportionate burden on household consumers. It emphasises the importance of easy switching between energy suppliers and calls for the phasing out of regulated retail prices, which discourage market competition and investment in infrastructure. The New Deal argues that greater energy efficiency is necessary, demand response among consumers should be facilitated, and community production initiatives encouraged. The Commission considers that rolling out smart meters across the EU is necessary to encourage greater demand response. Yet the precise cost savings for consumers from smart metering (and demand response in general) remain rather unclear, while smart metering has more positive effects when accompanied by incentives to change patterns of energy use (e.g. dynamic pricing). The New Deal calls for new measures to address vulnerable consumers and energy poverty in the EU, with reports by the Commission and European Parliament shedding light on these issues.

The New Deal seeks to encourage the development of smart homes and networks, which will require a range of new energy technologies. The growing use of ICT in smart grids has raised concerns about data protection and the risk of cyber hacking in smart grids. In past resolutions, the European Parliament expressed strong support for key ideas outlined in the New Deal, and has called for consumers to play a more active role in the energy transition.

Briefing EN

Empowering women on the Internet

Vrsta publikacije: Poglobljena analiza
Datum: 30-10-2015
Avtor: MARZOCCHI Ottavio
Politično področje: Socialna politika | Vprašanje spola, enakost in različnost | Zaposlovanje
Ključna beseda: dostop do informacij | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | enakost spolov | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | mednarodna vloga EU | organizacija poslovanja | podjetništvo | položaj žensk | POSLOVANJE IN KONKURENCA | pravice in svoboščine | PRAVO | računalniška kriminaliteta | spolno nadlegovanje | telekomunikacijska industrija | trgovina z ljudmi | učinek informacijske tehnologije

Povzetek: Upon request of the FEMM Committee, the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs examined the actions taken at the international and European level to empower women on the Internet. The research aims at exploring the opportunities, risks/threats and challenges for women in relation to the digital world and the Internet, notably in the areas of employment, entrepreneurship, cyber-activism, stereotyping, harassment, sexual violence and trafficking/modern slavery.

Poglobljena analiza EN

Cyber diplomacy: Confidence-building measures

Vrsta publikacije: Briefing
Datum: 28-10-2015
Avtor: PAWLAK Patryk
Politično področje: Globalno upravljanje | Območje svobode, varnosti in pravice | Varnost in obramba
Ključna beseda: ASEAN | boj proti kriminalu | diplomatski odnosi | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | elektronski dokaz | evropska varnost | generalni sekretar ZN | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | mednarodna varnost | MEDNARODNE ORGANIZACIJE | mednarodne zadeve | mednarodni odnosi | MEDNARODNI ODNOSI | ogrožanje državne varnosti | organizirani kriminal | OVSE | policijski nadzor | POLITIKA | politika in javna varnost | PRAVO | računalniška kriminaliteta | sodstvo | svetovne organizacije | terorizem | varstvo podatkov | virtualna skupnost | Združeni narodi | zunajevropske organizacije

Povzetek: The growing importance of internet-enabled platforms for delivery of government, financial, and public services makes them one of the key priorities for national security. Over recent years, state, state-sponsored and non-state actors (i.e. terrorist organisations, organised crime groups) alike have resorted to intrusive techniques to gain the economic, political or security upper hand over their competitors and adversaries. The evolving landscape of threats, and challenges linked to attribution of attacks to specific perpetrators, have further increased the risks of misunderstanding and misperception of operations in cyberspace. Against this background, a number of international and regional organisations in Europe, Asia and Latin America have embarked on the process of developing confidence-building measures in cyberspace, with a focus on improving communication and information exchange, transparency and verification, cooperation and restraint measures. While these are welcome, there is growing concern that the nascent global 'cyber stability regime' may be undermined by diverging concepts, methods and measures elaborated within these diverse frameworks. The European Union has embraced the peaceful development of cyberspace as one of its key priorities in the EU Cybersecurity Strategy. It contributes actively to the ongoing debates about norms, provides support to regional confidence-building processes, and pursues the objective of a stable, safe and secure cyberspace by providing funding for capacity building in partner countries.

Briefing EN

The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?

Vrsta publikacije: Študija
Datum: 28-10-2015
Zunanji avtor: Ben Hayes (Transnational Institute - TNI) ; Julien Jeandesboz (University of Amsterdam - UvA) and Centre d'Études sur les Conflits, Liberté et Sécurité - CCLS) ; Francesco Ragazzi (Leiden University, Netherlands and Centre d'Études sur les Conflits, Liberté et Sécurité - CCLS) ; Stephanie Simon (University of Amsterdam - UvA) ; Valsamis Mitsilegas (Queen Mary University of London, the UK) ;
This study was coordinated by the Centre d'Études sur les Conflits, Liberté et Sécurité (CCLS) and the Centre for European Policy Studies (CEPS) and conducted under the scientific supervision of Didier Bigo (CCLS and Sciences Po Paris and King's College London) and Amandine Scherrer (European Studies Coordinator and Associate Researcher at CCLS)
Politično področje: Območje svobode, varnosti in pravice | Varnost in obramba
Ključna beseda: Agencija Evropske unije za kibernetsko varnost | boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | Europol | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvajanje prava EU | komunikacije | organizacija pravnega sistema | POLITIKA | politika in javna varnost | PRAVO | pravo Evropske unije | pravosodno sodelovanje v kazenskih zadevah (EU) | pristojnost institucije | pristojnost sodišč | pristojnosti EP | razkritje informacij | računalniška kriminaliteta | varstvo podatkov

Povzetek: This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. With a number of high-profile criminal cases, such as 'Silk Road', cybercrime has been very much in the spotlight in recent years, both in Europe and elsewhere. While this study shows that cybercrime poses significant challenges for law enforcement, it also argues that the key cybercrime concern for law enforcement is legal rather than technical and technological. The study further underlines that the European Parliament is largely excluded from policy development in the field of cybercrime, impeding public scrutiny and accountability.

Študija EN

Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses

Vrsta publikacije Študija

Datum 28-10-2015

Zunanji avtor Nicole van der Meulen, Eun A. Jo and Stefan Soesanto (RAND Europe)

Politično področje Območje svobode, varnosti in pravice | Varnost in obramba

Ključna beseda Agencija Evropske unije za kibernetsko varnost | Amerika | boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomska geografija | Europol | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | MEDNARODNI ODNOSI | policijsko sodelovanje | politika sodelovanja | politična geografija | računalniška kriminaliteta | učinek informacijske tehnologije | varstvo podatkov | Združene države

Povzetek This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. It sets out to develop a better understanding of the main cybersecurity threats and existing cybersecurity capabilities in the European Union and the United States. The study further examines transnational cooperation and explores perceptions of the effectiveness of the EU response, pinpointing remaining challenges and suggesting avenues for improvement.

Študija EN

Cyber diplomacy: EU dialogue with third countries

Vrsta publikacije Briefing

Datum 29-06-2015

Avtor PAWLAK Patryk

Politično področje Območje svobode, varnosti in pravice

Ključna beseda Amerika | Azija in Oceanija | boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomska geografija | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | Indija | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | Japonska | Južna Koreja | Kitajska | komunikacije | mednarodna varnost | mednarodna varnost | mednarodna vloga EU | MEDNARODNI ODNOSI | politična geografija | računalniška kriminaliteta | varstvo podatkov | Združene države

Povzetek The current global debates about the role of governments in internet governance and the application of international law in cyberspace will have significant impact on the future of the internet. With a view to shaping their outcome, the EU is focusing on a number of priority areas: protecting the digital economy, reducing cybercrime, enhancing international stability, protecting the free and open internet, and capacity-building in third countries.

The need for closer engagement with key international partners, as a way towards promoting the EU's political, economic and strategic interests was recognised in the EU Cybersecurity Strategy of 2013, and the Council Conclusions on Cyber Diplomacy adopted in February 2015. The EU is pursuing this objective through cyber dialogues with China, India, Japan, South Korea and the United States, as well as other consultation venues where cyber issues are among the agenda items.

With internet and new communications technologies becoming an integral component of everyday life, the European Parliament plays a crucial role in ensuring that internet and digital technologies strengthen, rather than undermine, human development. It can do so through legislation and agenda-setting, parliamentary diplomacy and capacity building, awareness raising and its budgetary powers.

Briefing EN

Consumer protection aspects of mobile payments

Vrsta publikacije Briefing

Datum 22-06-2015

Avtor VALANT Jana

Politično področje Notranji trg in carinska unija | Varstvo potrošnikov

Ključna beseda denarno poslovanje | elektronski denar | elektronsko poslovanje | FINANCE | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | konkurenca | medsebojna povezava sistemov | mobilni telefon | nedopustno oglaševanje | organizacija poslovanja | POSLOVANJE IN KONKURENCA | poslovna etika | potrošnja | računalniška kriminaliteta | TRGOVINA | trženje | učinek informacijske tehnologije | varstvo podatkov | varstvo potrošnikov

Povzetek Over the next few years, mobile commerce in Europe is expected to grow at an average compound annual rate of 42%. The way in which consumers purchase goods and services is changing significantly as new technologies permit the development of an increasing number of cashless payment solutions. There are various forms of mobile payment (payment, for which the payment data and the payment instruction is initiated, transmitted or confirmed via a mobile phone or device). They include payments via SMS, direct billing (by adding the payment to the monthly mobile phone bill), mobile web payments (using a credit/debit card or pre-registration at an online payment provider), and Near Field Communication (NFC). However some of the challenges to consumer protection, such as lack of interoperability between mobile payment options, personal data protection, digital identity theft and fraud, prevent greater consumer take-up of mobile payments. Unfair commercial practices in e-commerce relevant to mobile payments include misleading advertising, hidden payment obligation and IP tracking. Other consumer protection issues are dormant assets, lack of accessibility and readability of payment-related information, and concerns related to vulnerable consumers. While the current legislative framework is undergoing revision as a result of the European Commission's new proposal for a Directive on payment services in the internal market, some stakeholders voice concerns.

Briefing EN

Understanding hybrid threats

Vrsta publikacije Na kratko

Datum 22-06-2015

Avtor PAWLAK Patryk

Politično področje Varnost in obramba

Ključna beseda Azija in Oceanija | državljanska vojna | ekonomska geografija | Evropa | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | Kitajska | mednarodna varnost | MEDNARODNE ORGANIZACIJE | MEDNARODNI ODNOSI | NATO | POLITIKA | politika in javna varnost | politična geografija | računalniška kriminaliteta | Rusija | Severna Koreja | skupna zunanja in varnostna politika | svetovne organizacije | terorizem | Ukrajina | vojna za mejo | vojno pravo

Povzetek 'Hybrid threats' are often invoked in reference to the ongoing conflict in Ukraine and the ISIL/Da'esh campaign in Iraq. As policy-makers struggle to grasp what hybrid threats mean for national security, it is pertinent to recall the origins, the meaning, and legal challenges associated with this concept.

Na kratko EN

Common Security and Defence Policy (CSDP) - EUCO policy developments since December 2013: European Council Briefing

Vrsta publikacije Briefing

Datum 17-06-2015

Avtor ANGHEL Suzana Elena

Politično področje Sprejemanje zakonodaje s strani Evropskega parlamenta in Sveta | Varnost in obramba

Ključna beseda delovanje institucij | evropska oboroževalna politika | EVROPSKA UNIJA | Evropski svet | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | MEDNARODNI ODNOSI | oborožitvena industrija | obramba | odnosi EU | politika sodelovanja | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | proračun za obrambo | raziskave in intelektualna lastnina | računalniška kriminaliteta | skupna varnostna in obrambna politika | tehnologija in tehnični predpisi | tehnologija z dvojno rabo | varstvo podatkov | vojaške raziskave | vojaško sodelovanje

Povzetek The June 2015 European Council will deal mainly with European Common Security and Defence Policy developments, i.e. progress made in implementing the roadmap established in December 2013. The Heads of State or Government will agree a new roadmap enabling Member States to deepen defence and security cooperation and to better address the emerging threats with which the EU is increasingly confronted. A revised policy implementation framework, which will include objectives and reporting deadlines, is also expected to be agreed.

Briefing EN

Cybersecurity and cyberdefence: EU Solidarity and Mutual Defence Clauses

Vrsta publikacije Briefing

Datum 05-06-2015

Avtor PAWLAK Patryk

Politično področje Območje svobode, varnosti in pravice | Varnost in obramba

Ključna beseda Agencija Evropske unije za kibernetsko varnost | EVROPSKA UNIJA | Evropske pogodbe | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodno pravo | mednarodno pravo o človekovih pravicah | pravice in svoboščine | pravna podlaga | PRAVO | pravo Evropske unije | računalniška kriminaliteta | skupna varnostna in obrambna politika | varstvo podatkov | vzajemna pomoč

Povzetek Faced with an increasing number of complex crises with a trans-border dimension, the European Union has invested significant energy and resources in strengthening its crisis- and disaster-management capabilities. To that effect, the Treaty of Lisbon equipped the Union with two provisions aimed at improving the EU's response to natural or man-made disasters (the Solidarity Clause) and military aggression against an EU Member State (the Mutual Defence Clause). For some time, both clauses remained purely theoretical concepts, without clear rules regarding their activation or procedures once either of the two is invoked by a Member State. In 2014, after many months of discussion, the Member States agreed on arrangements for the implementation of the 'Solidarity Clause'. The 'Mutual Defence Clause' has yet to see similar progress. Whether backed by procedures or not, so far the Member States have been reluctant to make use of either of the two provisions. Many areas of human activity are increasingly dependent on information technology. At the same time, over the past year some major media outlets and companies – including Sony and TV5 Monde – have become victims of cyber-attacks. Consequently, policy-makers are increasingly preoccupied about the risk of cyber-attacks with disastrous consequences for critical national infrastructure. Given the interconnectedness between the Member States and their inherent limitations to tackle a complex disaster provoked by a cyber-attack alone, there is some debate about the likelihood of the Solidarity and Mutual Defence Clauses eventually being invoked. The European Parliament has addressed these issues on three different occasions but its role once any of the clauses is activated remains to be defined.

Briefing EN

Cybersecurity: Jihadism and the internet

Vrsta publikacije: Na kratko

Datum: 18-05-2015

Avtor: PAWLAK Patryk

Politično področje: Varnost in obramba | Zunanje zadeve

Ključna beseda: DRUŽBENA IN SOCIALNA VPRAŠANJA | evropska varnost | FINANCE | financiranje in naložbe | informacijska tehnologija in obdelava podatkov | internet | islam | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | kultura in religija | mednarodna varnost | MEDNARODNI ODNOSI | način financiranja | POLITIKA | politika in javna varnost | politična propaganda | računalniška kriminaliteta | terorizem | učinek informacijske tehnologije | verski fundamentalizem

Povzetek: Since the beginning of the conflict in Syria in March 2011, the numbers of European citizens supporting or joining the ranks of ISIL/Da'esh have been growing steadily, and may now be as high as 4 000 individuals. At the same time, the possible avenues for radicalisation are multiplying and the risks of domestic terrorism increasing. The proliferation of global jihadi messaging online and their reliance on social networks suggest that the internet is increasingly a tool for promoting jihadist ideology, collecting funds and mobilising their ranks.

Na kratko: EN

Russia's armed forces: Reforms and challenges

Vrsta publikacije: Poglobljena analiza

Datum: 29-04-2015

Avtor: RUSSELL Martin

Politično področje: Varnost in obramba | Zunanje zadeve

Ključna beseda: družboslovne vede | ekonomska geografija | Evropa | GEOGRAFIJA | geopolitika | informacijska tehnologija in obdelava podatkov | institucionalna reforma | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNE ORGANIZACIJE | MEDNARODNI ODNOSI | NATO | oborožene sile | obramba | obrambna politika | POLITIKA | politika in javna varnost | politična geografija | politična propaganda | računalniška kriminaliteta | Rusija | svetovne organizacije | Ukrajina | vojaška oprema | vojna za mejo | ZNANOST | zunanja politika

Povzetek: After a long period of neglect and decline, the Russian armed forces have once again taken centre stage. On top of their alleged involvement in Ukraine, incursions into the airspace and territorial waters of neighbouring countries are becoming more frequent, and large-scale military drills have been held throughout the country. The traditional Victory Day parade through Moscow on 9 May celebrates Russian military prowess.

In line with their increasingly active role, the Russian armed forces are undergoing a modernisation process with sweeping reforms and a major rearmament programme. In the context of rising tensions with NATO and a potentially escalating conflict in Ukraine, the crucial question is whether the country now has a modern fighting machine capable of taking on a more substantial adversary.

Poglobljena analiza: DE, EN, FR

Workshop on Building Blocks of the Ubiquitous Digital Single Market

Vrsta publikacije: Študija

Datum: 03-02-2015

Zunanji avtor: Nick Sohnemann (FutureCandy, Germany), Christoph Pennings (iDate, France), Edwin Maaskant (Gartner Consulting, USA), Robert D. Atkinson (Information Technology & Innovation Foundation - ITIF, USA), Kim Soung Hie (KAIST Graduate School of IT & Media Management, South Korea), Silver Tammik (Economic Affairs at the Permanent Representation of Estonia to the EU, Belgium), Anne Fleur van Veenstra (TNO Strategy & Policy, Netherlands), J. Scott Marcus (Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Germany) and Andreas Mitrakas (European Union Agency for Network and Information Security - ENISA, Belgium)

Politično področje: Notranji trg in carinska unija | Območje svobode, varnosti in pravice | Varstvo potrošnikov

Ključna beseda: Azija in Oceanija | ekonomska geografija | elektronska uprava | elektronsko poslovanje | enotni trg | Estonija | Evropa | EVROPSKA UNIJA | GEOGRAFIJA | gospodarska rast | gospodarske razmere | GOSPODARSTVO | graditev Evrope | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvršilna oblast in javna uprava | Južna Koreja | komunikacije | POLITIKA | politična geografija | prenosno omrežje | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | računalniška kriminaliteta | tehnologija in tehnični predpisi | tehnološka sprememba | telekomunikacijska politika | TRGOVINA | trženje | učinek informacijske tehnologije

Povzetek: Digital technologies enable new disruptive business models and fundamentally improved e-government solutions. They can transform the Digital Single Market into the main engine of growth and job creation. The workshop aims at giving an overview of most advanced market and technological trends built on mobile connectivity and cloud computing. It points at Estonia and South Korea as leading jurisdictions that made the most of digital technologies both in private and public sectors. It examines net neutrality and cybersecurity as upcoming political and regulatory challenges.

Študija: EN

Mass Surveillance - Part 2: Technology foresight, options for longer term security and privacy improvements

Vrsta publikacije Študija

Datum 13-01-2015

Zunanji avtor Company:
Capgemini Consulting

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

Politično področje Dolgoročno načrtovanje | Raziskovalna politika

Ključna beseda EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | kriptografija | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | obramba | odprtokodna programska oprema | osebni podatki | pravice in svoboščine | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave posledic uvajanja novih tehnologij | računalniška kriminaliteta | tehnologija in tehnični predpisi | učinek informacijske tehnologije | varstvo podatkov | vohunjenje | zaščita komunikacij

Povzetek 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 EuropeanInformation 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.

Študija EN

Priloga 1 EN

Priloga 2 EN

Multimedijske vsebine 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

Vrsta publikacije Študija

Datum 12-01-2015

Zunanji avtor Company:
TECNALIA Research and Investigation

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

Politično področje Dolgoročno načrtovanje | Raziskovalna politika

Ključna beseda elektronska pošta | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | kriptografija | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | obramba | osebni podatki | pravice in svoboščine | PRAVO | računalniška kriminaliteta | učinek informacijske tehnologije | varstvo podatkov | vohunjenje | zaščita komunikacij | zlonamerna programska oprema

Povzetek 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.

Študija EN

Priloga 1 EN

Priloga 2 EN

Multimedijske vsebine Mass surveillance and citizen rights in the EU part 1

Internal Security Strategy: open and safe Europe

Vrsta publikacije: Na kratko
Datum: 05-12-2014
Avtor: PRPIC Martina
Politično področje: Območje svobode, varnosti in pravice
Ključna beseda: boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | EVROPSKA UNIJA | evropska varnost | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | medinstitucionalni odnosi (EU) | mednarodna varnost | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | organizirani kriminal | POLITIKA | politika in javna varnost | program EU | računalniška kriminaliteta | terorizem
Povzetek: Security and defence of its citizens are of high importance in the EU. However, any EU security policy must also respect the values on which the EU is based, such as respect for fundamental rights. The EU's Internal Security Strategy (ISS) for 2010 to 2014 was created to answer those different needs. There have been three reports on its implementation. The last of these, published this year, not only evaluates the implementation of the ISS, but identifies possible future challenges to be tackled in the forthcoming internal security strategy for the 2015-20 period.
Na kratko: DE, EN, ES, FR, IT, PL

Cyber defence in the EU: Preparing for cyber warfare?

Vrsta publikacije: Briefing
Datum: 29-10-2014
Avtor: CIRLIG Carmen-Cristina
Politično področje: Območje svobode, varnosti in pravice | Varnost in obramba
Ključna beseda: Amerika | Azija in Oceanija | Bližnji in Srednji Vzhod | država članica EU | ekonomska geografija | Evropa | EVROPSKA UNIJA | GEOGRAFIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | Južna Koreja | kazensko pravo | Kitajska | MEDNARODNE ORGANIZACIJE | MEDNARODNI ODNOSI | NATO | obramba | ogrožanje državne varnosti | politična geografija | PRAVO | računalniška kriminaliteta | Rusija | Severna Koreja | skupna varnostna in obrambna politika | strateška obramba | svetovne organizacije | varstvo podatkov | Združene države | zlonamerna programska oprema
Povzetek: In recent years, cyber attacks on a serious scale have become a matter of concern to states, due to the threat they can pose to national security, but also a potential foreign policy and military tool to be added to existing options in their arsenals.
Briefing: EN

Bitcoin: Market, economics and regulation

Vrsta publikacije: Briefing
Datum: 11-04-2014
Avtor: SZCZEPANSKI Marcin
Politično področje: Ekonomske in monetarne zadeve
Ključna beseda: davčna utaja | denarno poslovanje | elektronski denar | emisija denarja | FINANCE | finančna zakonodaja | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | konvertibilnost valute | pranje denarja | PRAVO | prost pretok kapitala | računalniška kriminaliteta | učinek informacijske tehnologije | špekulativni kapital
Povzetek: Bitcoin is a digital currency which started circulating in 2009. It was the first form of virtual money to become relatively popular. Bitcoin is public in nature as it maintains a log of all transactions. These are verified by its users in a process called mining. The extent of computing power and energy needed to mine bitcoins is set to increase over time.
Briefing: EN

EU approach to cyber-security

Vrsta publikacije: Na kratko
Datum: 31-03-2014
Avtor: FERRARO Francesca
Politično področje: Območje svobode, varnosti in pravice
Ključna beseda: Agencija Evropske unije za kibernetsko varnost | boj proti kriminalu | direktiva (EU) | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | Europol | evropska konvencija | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvršilna oblast in javna uprava | mednarodne zadeve | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | obramba | POLITIKA | pravo Evropske unije | program EU | računalniška kriminaliteta | upravno sodelovanje | varstvo podatkov | vohunjenje
Povzetek: 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.
Na kratko: EN

Cyber security in the European Union

Vrsta publikacije Briefing

Datum 12-11-2013

Avtor BAKOWSKI Piotr

Politično področje Območje svobode, varnosti in pravice | Raziskovalna politika | Varstvo potrošnikov

Ključna beseda Agencija Evropske unije za kibernetsko varnost | evropska konvencija | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija | informacijska tehnologija in obdelava podatkov | informacijski sistem | institucije EU in evropska javna uprava | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | mednarodne zadeve | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | pravni red EU | pravo Evropske unije | prenos podatkov | računalniška kriminaliteta | varstvo podatkov | zlonamerna programska oprema

Povzetek Over the past few decades, the digital revolution has brought global connectivity to an entirely new level. Information and communication technologies (ICT) are crucial for virtually all modern services, both civilian and military. Convenient as it is, such growing reliance on ICT entails and increasing risk of cyber attacks. These attacks may target individuals, businesses, entire networks or even the critical infrastructure of one or more EU Member States.

Briefing EN

Attacks against information systems

Vrsta publikacije Na kratko

Datum 27-06-2013

Avtor FERRARO Francesca

Politično področje Območje svobode, varnosti in pravice

Ključna beseda direktiva (EU) | evropska konvencija | EVROPSKA UNIJA | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijski sistem | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazenska sankcija | kazensko pravo | komunikacije | mednarodne zadeve | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | PRAVO | pravo Evropske unije | računalniška kriminaliteta | varstvo podatkov

Povzetek To fight cross-border crimes affecting information and communications networks (cybercrime) is a priority for the EU internal security strategy. To counter so-called cyber-attacks in a borderless space, both the Council of Europe and the EU have drawn up common strategies, operational measures and legislation.

Na kratko EN

Network and Information Security across the Union: Initial Appraisal of the Commission's Impact Assessment

Vrsta publikacije Briefing

Datum 15-04-2013

Avtor BALLON Elke

Politično področje Notranji trg in carinska unija | Predhodna ocena učinka | Varstvo potrošnikov

Ključna beseda ekonomske analize | elektronska uprava | EVROPSKA UNIJA | GOSPODARSTVO | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | informacijski sistem | IZOBRAŽEVANJE IN KOMUNIKACIJE | izvršilna oblast in javna uprava | OKOLJE | okoljska politika | POLITIKA | pravo Evropske unije | predlog (EU) | preprečevanje okoljskega tveganja | razkritje informacij | računalniška kriminaliteta | računalniško omrežje | varstvo podatkov | študija učinkov

Povzetek This note seeks to provide an initial analysis of the strengths and weaknesses of the European Commission's Impact Assessment (IA) accompanying the proposal for a Directive concerning measures to ensure a high level of network and information security across the Union.
Network and Information Security (NIS) is defined as 'the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems' (IA, p. 6). The internet and other networks and information systems underpin services which support the functioning of our society and economy, for example public administration, finance and banking, energy, transport, health, as well, by definition, internet services like e-commerce platforms and social networks.

Briefing DE, EN, FR

Fighting Cyber Crime and Protecting Privacy in the Cloud

Vrsta publikacije Študija

Datum 15-10-2012

Zunanji avtor Didier Bigo (Centre d'Etudes sur les Conflits, C&C), Gertjan Boulet (under coordination of the Centre for European Policy Studies, CEPS), Caspar Bowden (under coordination of the Centre d'Etudes sur les Conflits, C&C), Sergio Carrera (Centre for European Policy Studies, CEPS), Julien Jeandesboz (Centre d'Etudes sur les Conflits, C&C) and Amandine Scherrer (Centre d'Etudes sur les Conflits, C&C)

Politično področje Območje svobode, varnosti in pravice

Ključna beseda boj proti kriminalu | centralni podatkovni strežnik | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | organizacija pravnega sistema | osebni podatki | pravice in svoboščine | PRAVO | pristojnost sodišč | računalniška kriminaliteta | shranjevanje podatkov | varstvo podatkov | varstvo zasebnosti | zaščita komunikacij

Povzetek This study addresses the challenges raised by the growing reliance on cloud computing. It starts by investigating the issues at stake and explores how the EU is addressing the identified concerns. The study then examines the legal aspects in relation to the right to data protection, the issues of jurisdiction, responsibility and regulation of data transfers to third countries. These questions have been neglected in EU policies and strategies, despite very strong implications on EU data sovereignty and the protection of citizens' rights.

Študija EN

ACTA - Anti-Counterfeiting Trade Agreement

Vrsta publikacije Na kratko

Datum 29-06-2012

Avtor KLUGMAN-VUTZ Cornelia

Politično področje Mednarodna trgovina

Ključna beseda DRUŽBENA IN SOCIALNA VPRAŠANJA | EVROPSKA UNIJA | farmacevtski izdelek | graditev Evrope | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | intelektualna lastnina | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | mednarodna pogajanja | mednarodne zadeve | MEDNARODNI ODNOSI | ponarejanje denarja | pravice in svoboščine | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | sporazum (EU) | temeljne pravice | varstvo podatkov | varstvo zasebnosti | zdravstvo

Povzetek The Anti-Counterfeiting Trade Agreement (ACTA) is a plurilateral agreement between the EU, its Member States (MS) and ten other countries, including the USA and Japan.

Na kratko EN

Proceedings of the workshop on 'Cyber Security in Europe' - Brussels, 31 August 2011

Vrsta publikacije Študija

Datum 15-09-2011

Zunanji avtor Freddy Dezeure (Interinstitutional Computer Emergency Response Pre-Configuration Team), Steve Purser (European Network and Information Security Agency - ENISA), Ferenc Suba (CERT-Hungary - National Cyber Security Centre), Mikko Hypponen (F-Secure), William Beer (Cyber Security Practice, PwC UK) and Markus Schaffrin (eco-Association of the German Internet Industry)

Politično področje Industrija | Raziskovalna politika

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | EVROPSKA UNIJA | informacijska tehnologija in obdelava podatkov | institucija EU | institucije EU in evropska javna uprava | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | klasifikacija podjetij | komunikacije | mala in srednje velika podjetja | multinacionalna družba | POSLOVANJE IN KONKURENCA | računalniška kriminaliteta

Povzetek The general purpose of the workshop was to summarise existing and emerging threats that pose significant risks to networks and critical information, and to identify the drivers of these threats and to associate these key elements with security controls that can help to mitigate the risks. The workshop also sought to analyse possible European responses to challenges related to cyber security. Furthermore, the event aimed to facilitate an exchange of views and provide a forum for discussion with MEPs and all other participants.

Študija EN

Skrajšana različica DE, FR

Consumer Behaviour in a Digital Environment

Vrsta publikacije Študija

Datum 15-08-2011

Zunanji avtor Patrice Muller (London Economics, Project director), Mette Damgaard (London Economics, Project manager and lead author), Annabel Litchfield (London Economics), Mark Lewis (London Economics) and Julia Hörnle (Queen Mary University of London)

Politično področje Notranji trg in carinska unija | Varstvo potrošnikov

Ključna beseda civilno pravo | elektronsko poslovanje | informacije in obdelava informacij | informacijska družba | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | nakupovalne navade | nedovoljena trgovina | obveščanje potrošnikov | odgovornost proizvajalca | poprodajne storitve | potrošnja | PRAVO | razkritje informacij | računalniška kriminaliteta | TRGOVINA | trgovinska politika | trženje

Povzetek This study analyses consumer behaviour and the interaction between consumers and businesses in the digital environment. At issue is how consumers benefit from the digital environment and whether and how they change their purchasing behaviour. A number of barriers to e-commerce and a more integrated European digital market are identified and specific policy recommendations are provided.

Študija EN

Skrajšana različica DE, FR

The Role of ENISA in Contributing to a Coherent and Enhanced Structure of Network and Information Security in the EU and Internationally

Vrsta publikacije Študija

Datum 11-07-2011

Zunanji avtor J. Scott Marcus, Marieke Klaver, Gabriela Bodea, Annette Hillebrand and Peter Stamm

Politično področje Industrija | Območje svobode, varnosti in pravice

Ključna beseda Agencija Evropske unije za kibernetsko varnost | EVROPSKA UNIJA | informacije in obdelava informacij | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | pravice in svoboščine | PRAVO | prenos podatkov | računalniška kriminaliteta | varstvo podatkov | zaščita komunikacij

Povzetek This study provides analysis to support an ongoing discussion over the future course of ENISA. It assesses many aspects of the effectiveness of ENISA, and considers possible ways to improve its efficiency and effectiveness going forward. The level and balance of staffing, and the efficiency of mission-related travel arrangements, prove to be important factors.

Študija EN

Skrajšana različica DE, FR

The EU Internal Security Strategy, the EU Policy Cycle and the Role of (AFSJ) Agencies - Promise, Perils and Pre-requisites

Vrsta publikacije Poglobljena analiza

Datum 16-05-2011

Zunanji avtor Madalina Busuioc and Deirdre Curtin (Amsterdam Centre for European Law and Governance, the Holland)

Politično področje Območje svobode, varnosti in pravice | Varnost in obramba

Ključna beseda DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | Eurojust | Europol | EVROPSKA UNIJA | evropska varnost | Frontex | graditev Evrope | informacijska tehnologija in obdelava podatkov | institucije EU in evropska javna uprava | IZOBRAŽEVANJE IN KOMUNIKACIJE | mednarodna varnost | MEDNARODNI ODNOSI | organizirani kriminal | POLITIKA | politika in javna varnost | računalniška kriminaliteta | terorizem

Povzetek The present briefing note analyses and reflects on the EU policy cycle (within the broader context of the EU's internal security strategy), with a focus on the role of European agencies and ongoing initiatives for inter-agency cooperation. It discusses the specific approach adopted, its state of play while outlining its main promises as well as identifying potential pitfalls.
A number of positive suggestions in the form of "pre-requisites" or antidotes are put forward to suggest how each of these potentially problematic issues could (and in our view should) be addressed. These issues deserve further institutional consideration and should be taken up and elaborated in follow-up measures and documents to strengthen the policy cycle and the internal security strategy in order for it to be to live up to its promise.

Poglobljena analiza DE, EN, ES, FR, IT

Cybersecurity and Cyberpower : Concepts, Conditions and Capabilities for Cooperation for Action within the EU

Vrsta publikacije Študija

Datum 15-04-2011

Zunanji avtor KLIMBURG, Alexander (Austrian Institute for International Afffairs - OIIP, Austria) and TIRMAA-KLAAR, Heli (Estonian Foreign Policy Institute, Estonia)

Politično področje Javno mednarodno pravo | Območje svobode, varnosti in pravice | Varnost in obramba | Zasebno mednarodno pravo in pravosodno sodelovanje v civilnih zadevah | Zunanje zadeve

Ključna beseda Amerika | Azija in Oceanija | država članica EU | ekonomska geografija | Evropa | EVROPSKA UNIJA | evropska varnost | GEOGRAFIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | Kitajska | komunikacije | mednarodna varnost | MEDNARODNE ORGANIZACIJE | mednarodne zadeve | MEDNARODNI ODNOSI | mednarodno pravo | mednarodno pravo | NATO | POLITIKA | politika in javna varnost | politična geografija | PRAVO | računalniška kriminaliteta | Rusija | skupna zunanja in varnostna politika | svetovne organizacije | terorizem | večstranski odnosi | Združene države

Povzetek The study analyses policy options for strengthening cybersecurity within the EU and examining potential points-of-entry, including within the Common Security and Defence Policy (CSDP). The study provides an overview of the principle concepts and definitions of cyber security and cyber war, drawing attention to the complexity and cross-jurisdictional nature of the field. In addition to examining current cyber threats to the EU, the study also analyses the capacity of the EU to address more sophisticated cyber-attacks within a common framework. In this respect the study offers important insights into the political, operational and structural challenges that need to be addressed in order to protect the EU and its citizens as well and to exercise “cyberpower” on the international stage. The study takes-stock of the existing NATO and EU capabilities related to cyber security and highlights the added value of the EU in applying a diverse range of policies that can help enable it to comprehensively tackle the increasing range of cyber threats. The study has been requested to introduce Members of the European Parliament's Sub-Committee on Security and Defence (SEDE) to the current issues in cyber security and cyber warfare, as well as to provide a selection of policy recommendations, including within the CSDP context. The study also provides innovative conceptual understanding on what might constitute EU “cyberpower”.

Študija EN

Russian organised crime: The EU perspective

Vrsta publikacije Briefing

Datum 04-03-2011

Avtor BAKOWSKI Piotr

Politično področje Ekonomske in monetarne zadeve | Območje svobode, varnosti in pravice | Zunanje zadeve

Ključna beseda boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekonomska geografija | Evropa | EVROPSKA UNIJA | FINANCE | GEOGRAFIJA | graditev Evrope | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | organizirani kriminal | politična geografija | pranje denarja | PRAVO | pravosodno sodelovanje v kazenskih zadevah (EU) | promet s prepovedanimi drogami | prost pretok kapitala | računalniška kriminaliteta | Rusija | trgovina z ljudmi

Povzetek Since the fall of the Soviet Union, Russian organised crime groups have grown increasingly present in the European Union. The extent of their fraud and money laundering activities distinguishes them from other non–EU groups.

Briefing EN

Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks

Vrsta publikacije Poglobljena analiza

Datum 02-02-2009

Zunanji avtor Paul Cornish (Chatham House, London, UK)

Politično področje Območje svobode, varnosti in pravice | Varnost in obramba | Zunanje zadeve

Ključna beseda DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | ekstremizem | EVROPSKA UNIJA | graditev Evrope | informacijska tehnologija | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | kultura in religija | mednarodna varnost | mednarodna varnost | MEDNARODNI ODNOSI | območje svobode, varnosti in pravice | organizirani kriminal | POLITIKA | politika in javna varnost | računalniška kriminaliteta | skupna zunanja in varnostna politika | terorizem | verski fundamentalizem

Povzetek This paper examines Cyber-Security and Politically, Socially and Religiously Motivated Cyber-Attacks, focusing on the European Union as an international organisation with a fragmented yet developing interest in cyber-security.

Poglobljena analiza EN

Strengthening Security and Fundamental Freedoms on the Internet - an EU Policy on the Fight Against Cyber Crime

Vrsta publikacije: Poglobljena analiza

Datum: 15-01-2009

Zunanji avtor: Steve Peers (University of Essex, United Kingdom)

Politično področje: Območje svobode, varnosti in pravice | Človekove pravice

Ključna beseda: boj proti kriminalu | DRUŽBENA IN SOCIALNA VPRAŠANJA | družbene in socialne zadeve | informacijska tehnologija in obdelava podatkov | internet | IZOBRAŽEVANJE IN KOMUNIKACIJE | kazensko pravo | komunikacije | organizirani kriminal | otroška pornografija | POLITIKA | politika in javna varnost | pravice in svoboščine | PRAVO | računalniška kriminaliteta | terorizem | trgovina z ljudmi | zaščita komunikacij

Povzetek: This study examines the human rights aspects of the Internet, and looks in detail at the relevant criminal law rules of the Council of Europe and the EU. It also examines other aspects of the issue of cyber-crime, such as data protection rights, the EU's Safer Internet programme, child pornography, attacks on information systems, terrorism, racism and xenophobia.
The study concludes that the EU should set the following priorities in this area:
a) the adoption of a non-binding Internet Bill of Rights, a draft of which is presented in the Annex;
b) the development of EU substantive and procedural criminal law regarding cybercrime; and
c) the development of EU operational action as regards cyber-crime.

Poglobljena analiza: EN, FR

Security Technologies for Digital Media

Vrsta publikacije: Študija

Datum: 01-05-2001

Zunanji avtor: Franck Leprevost (Université de Grenoble, France) and Bertrand Warusfel (Université de Paris V, Paris, France)

Politično področje: Industrija | Kultura | Pravo intelektualne lastnine

Ključna beseda: avtorska pravica | digitalna tehnologija | informacije in obdelava informacij | informacijska družba | informacijska tehnologija in obdelava podatkov | IZOBRAŽEVANJE IN KOMUNIKACIJE | komunikacije | pravice in svoboščine | pravni viri in pravna področja | PRAVO | PROIZVODNJA, TEHNOLOGIJA IN RAZISKOVANJE | raziskave in intelektualna lastnina | računalniška kriminaliteta | tehnologija in tehnični predpisi | telekomunikacije | uskladitveni pravni akt | zaupnost | zaščita komunikacij

Povzetek: The aim of this study is to present a number of options on the question of digital content security technology to the European Parliament, particularly the Committee on Legal Affairs and the Internal Market, and the European Commission, including operational options.

Študija: EN, FR