



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

Lista över publikationer från parlamentets Think Tank

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

Sökkriterier som har använts för att skapa listan :

Sortera Sortera efter datum

Sökord "Europeiska unionens cybersäkerhetsbyrå"

19 Resultat

Skapades den : 17-04-2024

Cybersecurity actors in the EU

Publikationstyp Kort sammanfattning

Datum 09-01-2024

Författare CAR POLONA

Politikområde Område med frihet, säkerhet och rättvisa

Sökord digitalt innehåll | EKONOMI | EU-institutionerna och EU:s förvaltning | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | gränsöverskridande dimension | informationskrigföring | informationssäkerhet | informationsteknik och databehandling | internationell säkerhet | INTERNATIONELLA FÖRBINDELSER | PRODUKTION, TEKNIK OCH FORSKNING | regioner och regionalpolitik | teknik och tekniska föreskrifter | UTBILDNING OCH KOMMUNIKATION

Sammanfattning Cyberattack numbers have surged in recent years, leading to the formation of entities at all levels to prevent attacks or mitigate the harm they may cause. An efficient EU-level response requires coordination and the timely exchange of information. Several bodies and networks have been set up to this end; this paper explains their respective roles.

Kort sammanfattning [EN](#)

The use of contract agents in decentralised EU agencies

Publikationstyp Studie

Datum 15-05-2023

Extern avdelning Nathalie VANDAELE, Thierry VAN SCHOU BROECK, Dave DE VOEGHT, Thomas PENSAERT, Katarzyna REISENZEIN, Merel VANDERSEYPEN

Politikområde Budget | Budgetkontroll | Utvärdering av lagstiftning och politik i praktiken

Sökord administrering och avlönning av personal | budget | budgetkontroll | decentralisering | ersättning för arbete | EU-institutionerna och EU:s förvaltning | EU-tjänsteman | europeisk integration | Europeiska jämställdhetsinstitutet | Europeiska kemikaliemyndigheten | Europeiska miljöbyrån | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | Europeiska värdepappers- och marknadsmyndigheten | Europol | FINANSER | personal | POLITIK | SYSSELSÄTTNING OCH ARBETE | verkställande makt och offentlig förvaltning

Sammanfattning This study examines the management of Contract Agents in seven decentralised Agencies of the European Union: ECHA, EEA, EIGE, ENISA, ESMA, Eurofound and Europol. It evaluates the evolution of Contract Agents as part of the workforce, and presents findings on processes related to personnel budgeting, recruitment and retention, salary and remuneration, and advancement prospects for contract staff. This document was prepared by the Policy Department at the request of the Committee on Budgetary Control.

Studie [EN](#)

EU cyber-defence capabilities

Publikationstyp Kort sammanfattning

Datum 30-09-2021

Författare LATICI Tania

Politikområde Säkerhet och försvar | Utrikesfrågor

Sökord bekämpning av grov brottslighet | databrottslighet | desinformation | EU-institutionerna och EU:s förvaltning | EU-strategi | europeisk integration | europeisk säkerhet | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationskrigföring | informationssäkerhet | informationsteknik och databehandling | internationell säkerhet | INTERNATIONELLA FÖRBINDELSER | kommunikation | POLITIK | politik och allmän säkerhet | samhällsfrågor | skydd av kritisk infrastruktur | SOCIALA FRÅGOR | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION

Sammanfattning 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.

Kort sammanfattning [DE](#), [EN](#), [ES](#), [FR](#), [IT](#), [PL](#)

The new European cybersecurity competence centre and network

Publikationstyp Briefing

Datum 19-05-2021

Författare NEGREIRO ACHIAGA Maria Del Mar

Politikområde Den inre marknaden och tullunionen | Industri | Parlamentets och rådets antagande av lagstiftning

Sökord dokumentation | EU-förslag | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | EU-program | EU-strategi | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | forskning och immateriell äganderätt | forskning och utveckling | informationssäkerhet | informationsteknik och databehandling | PRODUKTION, TEKNIK OCH FORSKNING | ramprogram för forskning och utveckling | sammanfattning | spridning av EU-information | UTBILDNING OCH KOMMUNIKATION

Sammanfattning On 13 September 2017, the Commission adopted a cybersecurity package with a series of initiatives to further improve EU cyber-resilience, deterrence and defence. A year later, the Commission presented a proposal for the creation of a European cybersecurity competence centre with a related network of national coordination centres. The initiative aims to improve and strengthen the EU's cybersecurity capacity, by stimulating the European technological and industrial cybersecurity ecosystem as well as coordinating and pooling necessary resources in Europe. The competence centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework, for 2021-2027. Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE). The report was adopted on 19 February 2019 in the ITRE committee. On 17 April 2019 the Parliament adopted its position at first reading, after two trilogue meetings, before the European elections. A new trilogue meeting took place more than a year later, on 25 June 2020, and further negotiations followed. During the fifth trilogue meeting on 11 December 2020, the negotiators of the Council and the European Parliament reached a provisional agreement. The Council adopted the legislation on 20 April 2021 at first reading. The ITRE committee adopted the draft recommendation for second reading on 26 April 2021, and it is expected that the European Parliament will adopt the text during the May 2021 plenary session.

Briefing [EN](#)

Cyber: How big is the threat?

Publikationstyp Kort sammanfattning

Datum 09-07-2019

Författare LATICI Tania

Politikområde Säkerhet och försvar | Utrikesfrågor

Sökord EU-institutionerna och EU:s förvaltning | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationskrigföring | informationsnät | informationssäkerhet | informationsteknik | informationsteknik och databehandling | internationell säkerhet | INTERNATIONELLA FÖRBINDELSER | kommunikation | UTBILDNING OCH KOMMUNIKATION

Sammanfattning The internet has transformed the world into a global village transcending physical borders and palpable distances. Often described as 'fog' or a 'globalised network of networks', cyberspace is extremely complex, accessible to everyone and difficult to pinpoint. While thanks to these characteristics cyberspace has opened countless social, economic and political opportunities, it has also become a source of disruption, conflict and geopolitical rivalries. The European Union has recognised that cyber-security and cyber-defence are critical for both its prosperity and security, and is emerging as an increasingly capable cyber player.

Kort sammanfattning [EN](#)

ENISA and a new cybersecurity act

Publikationstyp Briefing

Datum 05-07-2019

Författare NEGREIRO ACHIAGA Maria Del Mar

Politikområde Den inre marknaden och tullunionen | Industri | Parlamentets och rådets antagande av lagstiftning

Sökord databrottslighet | EU-förslag | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationsnät | informationsteknik och databehandling | institutionernas arbetssätt | kommunikation | nationellt parlament | ordinarie lagstiftningsförfarande | parlament | POLITIK | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION | överföringsnät

Sammanfattning 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](#)

ENISA and new EU Cybersecurity Act

Publikationstyp Kort sammanfattning

Datum 06-03-2019

Författare NEGREIRO ACHIAGA Maria Del Mar

Politikområde Den inre marknaden och tullunionen | Industri | Parlamentets och rådets antagande av lagstiftning

Sökord EU-institutionerna och EU:s förvaltning | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationssäkerhet | informationsteknik och databehandling | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION

Sammanfattning The European Commission proposed to increase EU resilience and response to cyber-attacks via a permanent mandate and an enhanced role for the EU Agency for Network Information Security (ENISA), the EU cybersecurity agency. It also envisages creating the first EU cybersecurity certification framework for ICT products and services, where ENISA will play an important role. The European Parliament's Industry, Research and Energy Committee (ITRE) adopted its report on 10 July 2018, as well as a mandate to enter into interinstitutional negotiations. The Council adopted its mandate on 8 June 2018. During the fifth trilogue meeting on 10 December 2018 an agreement was reached. It is due to be voted by Parliament in plenary during March.

Kort sammanfattning [DE](#), [EN](#), [ES](#), [FR](#), [IT](#), [PL](#)

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

Publikationstyp Briefing

Datum 19-02-2019

Författare KONONENKO Vadim

Politikområde Industri | Konsumentskydd | Säkerhet och försvar

Sökord databrottslighet | EKONOMI | ekonomisk analys | EU-förslag | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | EU-strategi | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | genomförandeorgan | gränsöverskridande samarbete | information och informationsbehandling | informationssäkerhet | informationsteknik och databehandling | INTERNATIONELLA FÖRBINDELSER | konsekvent-undersökning | PRODUKTION, TEKNIK OCH FORSKNING | samarbetspolitik | teknik | teknik och tekniska föreskrifter | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION

Sammanfattning 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](#)

Implementation and functioning of the '.eu' top level domain name

Publikationstyp Briefing

Datum 12-10-2018

Författare KONONENKO Vadim

Politikområde Den inre marknaden och tullunionen | Ekonomiska och monetära frågor

Sökord digital inre marknad | EKONOMI | ekonomisk analys | EU-institutionerna och EU:s förvaltning | europeisk integration | europeisk symbol | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | Europeiska unionens immaterialrättsmyndighet | Internetadress | kommunikation | konsekvent-undersökning | PRODUKTION, TEKNIK OCH FORSKNING | reglering på telekommunikationsområdet | teknik och tekniska föreskrifter | teknisk specifikation | UTBILDNING OCH KOMMUNIKATION

Sammanfattning The scope of the problem could have been defined in more precise terms. Furthermore, it remains unclear how the proposed options could help achieve one of the two general objectives of the initiative namely enabling or building an online European identity as the options (including the preferred one) are mostly concerned with the technical improvements of the regulatory framework. Stakeholder views do not appear to be fully reflected in the report and it is unclear how they fed into the IA. A more thorough integration of the recommendations of the Regulatory Scrutiny Board, which appear to be only partially addressed, would have benefited the quality of the IA.

Briefing [EN](#)

EU Cybersecurity Agency and cybersecurity certification

Publikationstyp Briefing

Datum 20-12-2017

Författare EISELE Katharina

Politikområde Den inre marknaden och tullunionen | Industri | Område med frihet, säkerhet och rättvisa

Sökord databrottslighet | EKONOMI | ekonomisk analys | EU-institutionerna och EU:s förvaltning | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationsnät | informationsteknik och databehandling | institutionernas arbetssätt | kommunikation | konsekvent-undersökning | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION | överföringsnät

Sammanfattning 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](#)

En digital agenda för Europa

Publikationstyp Faktablad om EU

Datum 01-06-2017

Författare MACIEJEWSKI Mariusz

Politikområde Forskningspolitik

Sökord datarätt | dataöverföring | digital teknik | EU-institutionerna och EU:s förvaltning | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | forskning och immateriell äganderätt | HANDEL OCH AFFÄRSVERKSAMHET | immateriell äganderätt | information och informationsbehandling | informationsteknik | informationsteknik och databehandling | inre marknad | Internet | kommunikation | kommunikationspolitik | konsumentskydd | konsumtion | PRODUKTION, TEKNIK OCH FORSKNING | teknik och tekniska föreskrifter | tillgång till information | UTBILDNING OCH KOMMUNIKATION

Sammanfattning Sedan 1995 har informations- och kommunikationsteknik (IKT) lett till produktivitetsökningar och tillväxt i EU[1]. Begreppet IKT omfattar ett brett tekniskt spektrum, från informationsteknologi (IT), över telekommunikation, etermedia och alla former av bearbetning och överföring av ljud och bild, till nätverksbaserade kontroll- och övervakningsfunktioner. De tre senaste årtiondena har teknisk "konvergens" lett till att gränserna mellan telekommunikationer, radio- och tv-sändningar och IT suddats ut. Smarta mobiler, surfplattor och smart tv är de tydligaste exemplen på detta fenomen. Linjära radio- och tv-sändningar fortsätter visserligen att vara det viktigaste mediet för distribution av information och underhållning i Europa, men alltmer audiovisuellt innehåll finns tillgängligt på begäran samtidigt som exponentiell tillväxt av konnektivitet i form av 4G – som snart kommer att öka till 5G – och "sakernas internet", som omfattar anslutna bilar, kroppsnära enheter och sensorer, leder till att internet blir alltmer generellt närvarande.

Faktablad om EU [BG](#), [CS](#), [DA](#), [DE](#), [EL](#), [EN](#), [ES](#), [FI](#), [FR](#), [HU](#), [IT](#), [LT](#), [LV](#), [NL](#), [PT](#), [RO](#), [SV](#), [ET](#), [HR](#), [MT](#), [PL](#), [SK](#), [SL](#)

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

Publikationstyp Briefing

Datum 19-05-2017

Författare ZYGIEREWICZ Anna

Politikområde Införlivande och genomförande av lagstiftning | Säkerhet och försvar | Utvärdering av lagstiftning och politik i praktiken

Sökord databrottslighet | dokumentation | EKONOMI | ekonomisk analys | EU-förordning | EU-institutionerna och EU:s förvaltning | EU-institutionernas befogenheter | EU-lagstiftning | EU-statistik | Europaparlamentet | europeisk säkerhet | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | forskning och immateriell äganderätt | informationsteknik och databehandling | institutionernas arbetssätt | internationell säkerhet | INTERNATIONELLA FÖRBINDELSER | Internet | kommunikation | offentligt samråd | partnerskap mellan den offentliga och den privata sektorn | POLITIK | PRODUKTION, TEKNIK OCH FORSKNING | ramprogram för forskning och utveckling | UTBILDNING OCH KOMMUNIKATION | verksamhetsberättelse | verkställande makt och offentlig förvaltning

Sammanfattning 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](#)

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

Publikationstyp Kort sammanfattning

Datum 28-04-2016

Författare PAWLAK Patryk

Politikområde Säkerhet och försvar

Sökord bekämpning av grov brottslighet | databrottslighet | EU-institutionerna och EU:s förvaltning | europeisk integration | europeisk säkerhet | europeisk säkerhets- och försvarspolitik | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | forskning och immateriell äganderätt | högförräderi | immateriell äganderätt | informationsteknik och databehandling | informationsteknikens inverkan | internationell säkerhet | INTERNATIONELLA FÖRBINDELSER | internationellt samarbete | Internet | kommunikation | LAG OCH RÄTT | piratverksamhet inom dataindustrin | POLITIK | politik och allmän säkerhet | PRODUKTION, TEKNIK OCH FORSKNING | samarbetspolitik | samhällsfrågor | SOCIALA FRÅGOR | straffrätt | terrorism | UTBILDNING OCH KOMMUNIKATION

Sammanfattning 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

Kort sammanfattning [EN](#)

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

Publikationstyp Studie

Datum 28-10-2015

Extern avdelning 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)

Politikområde Område med frihet, säkerhet och rättvisa | Säkerhet och försvar

Sökord bekämpning av grov brottslighet | databrottslighet | datakommunikation | domstolars behörighet | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | Europaparlamentets befogenheter | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | Europol | genomförande av EU-rätten | information och informationsbehandling | informationsteknik och databehandling | institutionell behörighet | Internet | kommunikation | LAG OCH RÄTT | POLITIK | politik och allmän säkerhet | rättssystemets organisation | samhällsfrågor | SOCIALA FRÅGOR | straffrättsligt samarbete inom EU | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION

Sammanfattning 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.

Studie [EN](#)

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

Publikationstyp Studie

Datum 28-10-2015

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

Politikområde Område med frihet, säkerhet och rättvisa | Säkerhet och försvar

Sökord Amerika | bekämpning av grov brottslighet | databrottslighet | ekonomisk geografi | EU-institutionerna och EU:s förvaltning | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | Europol | Förenta staterna | GEOGRAFI | information och informationsbehandling | informationsteknik och databehandling | informationsteknikens inverkan | INTERNATIONELLA FÖRBINDELSER | Internet | kommunikation | polisiärt samarbete | politisk geografi | samarbetspolitik | samhällsfrågor | SOCIALA FRÅGOR | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION

Sammanfattning 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.

Studie [EN](#)

Cybersecurity and cyberdefence: EU Solidarity and Mutual Defence Clauses

Publikationstyp Briefing

Datum 05-06-2015

Författare PAWLAK Patryk

Politikområde Område med frihet, säkerhet och rättvisa | Säkerhet och försvar

Sökord databrottslighet | EU-fördrag | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | europeisk integration | europeisk säkerhets- och försvarspolitik | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationsteknik och databehandling | internationell lagstiftning om mänskliga rättigheter | internationell rätt | LAG OCH RÄTT | rättigheter och friheter | rättslig grund | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION | ömsesidigt bistånd

Sammanfattning 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](#)

EU approach to cyber-security

Publikationstyp Kort sammanfattning

Datum 31-03-2014

Författare FERRARO Francesca

Politikområde Område med frihet, säkerhet och rättvisa

Sökord administrativt samarbete | bekämpning av grov brottslighet | databrottslighet | ett område med frihet, säkerhet och rättvisa | EU-direktiv | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | EU-program | Europakonvention | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | Europol | försvar | information och informationsbehandling | informationsteknik och databehandling | internationell politik | INTERNATIONELLA FÖRBINDELSER | POLITIK | samhällsfrågor | SOCIALA FRÅGOR | spionage | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION | verkställande makt och offentlig förvaltning

Sammanfattning 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.

Kort sammanfattning [EN](#)

Cyber security in the European Union

Publikationstyp Briefing

Datum 12-11-2013

Författare BAKOWSKI Piotr

Politikområde Forskningspolitik | Konsumentskydd | Område med frihet, säkerhet och rättvisa

Sökord databrottslighet | dataöverföring | ett område med frihet, säkerhet och rättvisa | EU-institutionerna och EU:s förvaltning | EU-lagstiftning | EU:s rättssystem | Europakonvention | europeisk integration | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationssystem | informationsteknik | informationsteknik och databehandling | internationell politik | INTERNATIONELLA FÖRBINDELSER | Internet | kommunikation | skadeprogram | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION

Sammanfattning 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](#)

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

Publikationstyp **Studie**

Datum **11-07-2011**

Extern avdelning **J. Scott Marcus, Marieke Klaver, Gabriela Bodea, Annette Hillebrand and Peter Stamm**

Politikområde **Industri | Område med frihet, säkerhet och rättvisa**

Sökord **databrottslighet | dataöverföring | EU-institutionerna och EU:s förvaltning | EUROPEISKA UNIONEN | Europeiska unionens cybersäkerhetsbyrå | information och informationsbehandling | informationsteknik och databehandling | kommunikation | kommunikationshemlighet | LAG OCH RÄTT | rättigheter och friheter | uppgiftsskydd | UTBILDNING OCH KOMMUNIKATION**

Sammanfattning **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.**

Studie [EN](#)

Sammanfattning [DE](#), [FR](#)