RESEARCH IN FOCUS

Annex to EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals

Julia Schuetze

Stiftung Neue Verantwortung

November 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.

Abstract

The need for more US–EU collaboration on cybersecurity policy has been identified by policymakers and diplomats from the EU and the US in their official Cyber Dialogues 2018 and 2019 as well as by international cybersecurity policy scholars. As the EU shapes its cybersecurity policies and fosters coordination among member states, cooperation at the EU level becomes more important to the US. EU–US cooperation to achieve shared policy goals such as prosecution and prevention of cybercrime has already resulted in implementing policy instruments together such as a joint exercise or information-sharing agreement specifically on cybercrime. Nevertheless, on a broader strategic level and with the focus on responses to malicious cyber-activities, concrete steps forward have been difficult to achieve in an environment where the EU and the US grapple with an ever-changing threat landscape that targets their values and ways of life and has made them focus on developing further their own processes and policy approaches in 2018–2020.

This paper sets out to find actions that the EU and US can implement together. It takes a practical approach by first identifying joint strategic goals and analysing the commonalities of EU and US cybersecurity policy. This allows a broader perspective on what the EU and US joint strategic goals really are, and what is feasible to do together. It is important to take account of the limitations and divergences that, as many others have pointed out, make cooperation difficult, but this paper uses them more as a means to find which instruments are actually feasible. Anyone who is interested to learn more about the EU and US, as well as those who are looking to find a way forward for transatlantic cooperation, will find glimpses of hope here and there in a policy field where it cannot be denied that the EU and US diverge as much as they converge.

1. Policy instruments that are unique to the EU

1.1. EU Council conclusions

European Union institutions

Main goal(s) of the policy instrument

> Prevention, Mitigation/Response

Main government resource(s) used to implement this instrument

> Authority/Information

Main target stakeholders

> Internal Actors, External Actors, Own Institutions

Description of Implementation

> On 16 April 2018, the Council adopted conclusions on malicious cyber-activities which underline the importance of a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply. The Council could use this instrument of the Cyber Diplomacy Toolbox to express a political position, to invite another EU institution to take action, or to prepare a proposal for coordinated Member States' action on a specific issue.

Examples of Implementation

> In reaction to WannaCry and NotPetya: 'On 16 April 2018, the Council adopted conclusions on malicious cyber activities which underline the importance of a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply.'

References

https://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/

Limitation(s) for joint implementation

> Availability of Instrument

1.2. Support of lawful response

European Union institutions

Main goal(s) of the policy instrument

> Mitigation/Response

Main government resource(s) used to implement this instrument

> Organisation, Treasure, Information

Main target stakeholders

> Internal Actors

Description of Implementation

> Through this instrument of the Cyber Diplomacy Toolbox, the EU can support responses by Member States that can take the form of any lawful measure, ranging from diplomatic steps to the use of stronger individual or cooperative responses by invoking e.g. Mutual defence clause (Article 42.7 TEU) or Solidarity clause (Article 222 TFEU).

Examples of Implementation

> Has not been implemented.

References

https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

Limitation(s) for joint implementation

> Availability of Instrument

1.3. Certifications (Framework)

European Union institutions

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Organisation, Information

Main target stakeholders

> Internal Actors

Description of Implementation

> The EU Cybersecurity Act establishes an EU certification framework for ICT digital products, services and processes. The European cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes.

Examples of Implementation

> Following the entry into force of the Cybersecurity Act on 27 June 2019, the European Commission launched a call for applications to select members of the Stakeholder Cybersecurity Certification Group (SCCG). The call was open to academic institutions, consumer organisations, conformity assessment bodies, standard-developing organisations, companies, trade associations and other membership organisations. The SCCG will be responsible for advising the Commission and the EU Agency for Cybersecurity (ENISA) on strategic issues regarding cybersecurity certification, and assisting the Commission in the preparation of the Union rolling work programme.

References

https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

Limitation(s) for joint implementation

> Availability of Instrument

1.4. Screening of foreign direct investements (Framework)

European Union institutions

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Authority, Information

Main target stakeholders

> Internal Actors

Description of Implementation

> 'In March 2019, the EU adopted Regulation (EU) No 2019/45211 setting up a framework for the screening of investments from non-EU countries that may affect security or public order. Accordingly, by October 2020, a cooperation mechanism (between the Member States and the Commission) will be established to exchange information and to issue comments in relation to foreign direct investment. The new legislation will contribute to strengthening the overall intelligence on foreign direct investment across the EU and, consequently, to improving resilience mechanisms against hybrid threats, inter alia in the area broadly regarded as critical infrastructure protection and beyond.

Examples of Implementation

> Member States and the Commission will examine effects on, inter alia, critical infrastructures (physical or virtual) including energy, transport, water, health, communications, media, data processing or storage, aerospace, defence, electoral or financial infrastructure, and sensitive facilities, as well as land and real estate crucial for the use of such infrastructure; critical technologies and dual use items, including artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, and quantum and nuclear technologies as well as nanotechnologies and biotechnologies, etc.

References

> https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2. Policy instruments that are unique to the US

2.1. Identification of countries posing risks to US cybersecurity

US (federal government)

Main goal(s) of the policy instrument

> Detection, Mitigation/Response

Main government resource(s) used to implement this instrument

> Authority, Information

Main target stakeholders

> Internal Actors, External Actors

Description of Implementation

> The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (H.R. 5515) was signed into law on 13 August 2018. It states that within 180 days of enactment, the Secretary of Defense 'shall create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list.' Another section grants authority to 'disrupt, defeat, and deter cyber attacks' originating from the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran, including attempts to influence American elections and democratic processes'.

Examples of Implementation

> The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (H.R. 5515) was signed into law on 13 August 2018. It states that within 180 days of enactment, the Secretary of Defense 'shall create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list.' Another section grants authority to 'disrupt, defeat, and deter cyber attacks' originating from the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran, including attempts to influence American elections and democratic processes'.

References

> https://www.wiley.law/alert-Important-Cyber-Provisions-Now-Law-Under-the-2019-NDAA

> https://www.congress.gov/bill/115th-congress/house-bill/5515/text

Limitation(s) for joint implementation

> Availability of Instrument

2.2. Banning the use of technologies from certain companies in communications networks

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Authority

Main target stakeholders

> Internal Actors

Description of Implementation

> The Executive Order on Securing the Information and Communications Technology and Services Supply Chain, issued in May 2019 and extended through 2021, puts limits on foreign involvement in the nation's carrier networks if they are deemed to pose a national security risk.

Examples of Implementation

> Bureau of Industry and Security (BIS) in the Department of Commerce added Huawei Technologies Co., Ltd. (Huawei) and certain non-US affiliates to the Entity List (with additional affiliates added in August 2019) on the basis of information that provided a reasonable basis to conclude that Huawei is engaged in activities that are contrary to US national security or foreign policy interests.

References

> https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts

> https://www.reuters.com/article/us-usa-huawei-tech/u-s-commerce-department-extends-huawei-license-through-may-15-idUSKBN20X32G

> https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

Notes

> Only implemented together with Five Eyes countries that also have this instrument.

Limitation(s) for joint implementation

> Availability of Instrument

2.3. Building/joining coalitions of the willing states for collective response

US (federal government)

Main goal(s) of the policy instrument

> Mitigation/Response

Main government resource(s) used to implement this instrument

> Information, Organisation

Main target stakeholders

> External Actors

Description of Implementation

> Building or joining coalitions of the willing states for collective response means to work together to cooperate and coordinate each other's response openly.

Examples of Implementation

> US-led Deterrence Initiative – 'The US government is aiming to build a broad coalition of "like-minded" nations to join a US-led "deterrence initiative" that includes collective response to malicious cyber-activities by China, Russia, Iran and North Korea, says Robert Strayer, deputy assistant secretary of state for cyber and international communications and information policy.'

> Joining coordinated attribution effort of WannaCry: 'Other governments and private companies agree. The United Kingdom, Australia, Canada, New Zealand, and Japan have seen our analysis, and they join us in denouncing North Korea for WannaCry.'

References

> https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

> https://breakingdefense.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/

Notes

> Only implemented together with Five Eyes countries that also have this instrument.

Limitation(s) for joint implementation

> Availability of Instrument

2.4. Red-teaming

US (federal government)

Main goal(s) of the policy instrument

> Prevention, Detection

Main government resource(s) used to implement this instrument

> Information, Organisation

Main target stakeholders

> Own Institutions

Description of Implementation

> The 90-day assessments begin with about two weeks of reconnaissance that might culminate in a carefully crafted spearphishing email. Department of Homeland Security (DHS): 'We send a phishing email and it beacons back to our host in Arlington, and then we have a foothold' into the organisation, said Karas, DHS's director of national cybersecurity assessments and technical services. 'From there, we pivot to other computers, to domain controllers, to enterprise computers.'

Examples of Implementation

> The DHS has carried out quiet 'red-teaming' exercises at three federal agencies, breaking into networks and telling agency officials how it was done.

References

> https://www.cyberscoop.com/red-teaming-dhs-quietly-slowly-uncovers-agency-vulnerabilities/

Limitation(s) for joint implementation

> Availability of Instrument

2.5. Cybersecurity trainings and workforce analysis and development frameworks

US (federal government)

Main goal(s) of the policy instrument

Prevention

Main government resource(s) used to implement this instrument

> Information, Organisation

Main target stakeholders

> Own Institutions, Internal Actors

Description of Implementation

> Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up to date on skills and evolving threats. The Department of Homeland Security (DHS) is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation. DHS offers training and educational resources for a range of stakeholder groups, such as federal workers but also parents and schoolteachers.

Examples of Implementation

> The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work and workers, regardless of where, or for whom, the work is performed.

> NICCS is an online resource for cybersecurity training that connects government employees, students, educators, and industry with cybersecurity training providers throughout the nation.

> The Federal Virtual Training Environment (FedVTE) is a free, online, on-demand cybersecurity training system managed by DHS that is available to federal and state, local, tribal and territorial (SLTT) government personnel, veterans, and federal government contractors, and contains more than 800 hours of training on topics such as ethical hacking, surveillance, risk management and malware analysis.

References

> https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework#

> https://www.cisa.gov/publication/stopthinkconnect-parent-and-educator-resources

Limitation(s) for joint implementation

> Availability of Instrument

2.6. Development of national and sector-specific protection plan

US (federal government)

Main goal(s) of the policy instrument

Prevention, Mitigation/Response

Main government resource(s) used to implement this instrument

> Information, Organisation and Authority

Main target stakeholders

> Own Institutions, Internal Actors

Description of Implementation

> Each sector-specific agency is responsible for developing and implementing a sector-specific plan (SSP), which details the application of the National Infrastructure Protection Plan (NIPP) concepts to the unique characteristics and conditions of its sector. SSPs have been updated to align with the NIPP 2013.

Examples of Implementation

> The Transportation Systems Sector-Specific Plan details how the NIPP risk-management framework is implemented within the context of the unique characteristics and risk landscape of the sector.

> Each sector-specific agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The postal and shipping sector was consolidated within the transportation systems sector in 2013 under Presidential Policy Directive 21.

> The Department of Homeland Security and the Department of Transportation are designated as the co-sector-specific agencies for the transportation systems sector.

References

> https://www.dhs.gov/xlibrary/assets/nipp_sctrplans.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2.7. Declaration of intent signed jointly with third country

US (federal government)

Main goal(s) of the policy instrument

Prevention, Mitigation/Response

Main government resource(s) used to implement this instrument

> Information

Main target stakeholders

> External Actors

Description of Implementation

> This is a formal or explicit statement or announcement on joint actions and intended goals and activities of one or more countries. All letters of intent lay out the basis of a deal, including cost, time frame and contingencies. Though the letter of intent is nonbinding, it is an important outline of the key terms that the parties involved in the transaction have agreed upon. Removing the clause that makes it binding would reduce the contract/ agreement/treaty to a mere declaration of intent.

Examples of Implementation

> Singapore and the US signed a Declaration of Intent on Cybersecurity Technical Assistance Programme. The Singapore–US Cybersecurity Technical Assistance Programme for Association of Southeast Asian Nations (ASEAN) member states encapsulates elements of Singapore's ASEAN Cyber Capacity Programme (ACCP) and the US's Digital Connectivity and Cybersecurity Partnership initiative. The programme will extend the work of the annual Singapore–US Third Country Training Programme Workshop on Cybersecurity. It aims to deliver three cybersecurity training workshops on various aspects of technical cybersecurity capacity building annually, with the involvement of key industry partners. The training workshops will take place in Singapore and selected regional venues, in partnership with interested ASEAN partners.

References

> https://www.csa.gov.sg/news/press-releases/singapore-and-the-us-sign-doi-on-cybersecurity-technical-assistance-programme

Limitation(s) for joint implementation

> Availability of Instrument

2.8. Memorandum of understanding on cybersecurity cooperation

US (federal government)

Main goal(s) of the policy instrument

Prevention, Mitigation/Response

Main government resource(s) used to implement this instrument

> Information/Organisation

Main target stakeholders

> External Actors

Description of Implementation

> A memorandum of agreement (MOA) or cooperative agreement is a document written between parties to cooperatively work together on an agreed-upon project or meet an agreed-upon objective. The purpose of an MOA is to have a written understanding of the agreement between parties. The MOA can be a legal document that is binding and hold the parties responsible to their commitment, or just a partnership agreement. A memorandum of understanding (MOU) is an agreement between two or more parties outlining the terms and details of an understanding. It expresses a convergence of will between the parties, indicating an intended common line of action. It is often used in cases where parties do not imply a legal commitment or in situations where the parties cannot create a legally enforceable agreement. It is a more formal alternative to a 'gentlemen's agreement'. In the context of joint use agreements, an MOU is often used to define each party's expectations and responsibilities. These MOUs typically address issues such as: (1) who bears responsibility for the costs of maintenance and repairs, (2) insurance and liability, (3) staffing and communications, and (4) conflict resolution.

Examples of Implementation

> The US and Singapore signed in 2016 a cybersecurity MOU to formalise their commitment to work together in building a secure and resilient cyberspace through cybersecurity cooperation. The agreement covers cooperation in key areas including regular Computer Emergency Response Team (CERT)–CERT information exchanges and sharing of best practices, coordination in cyber-incident response and sharing of best practices on Critical Information Infrastructure protection, cybersecurity trends and practices. The parties also commit to conduct joint cybersecurity exercises and collaborate on regional cyber-capacity building and cybersecurity awareness building activities.

References

> https://www.csa.gov.sg/news/press-releases/singapore-us-mou

Limitation(s) for joint implementation

> Availability of Instrument

2.9. Requirement of cybersecurity funding analysis in overall budget

US (federal government)

Main goal(s) of the policy instrument

Prevention

Main government resource(s) used to implement this instrument

> Authority/Information

Main target stakeholders

> Own Institutions

Description of Implementation

> Section 630 of the Consolidated Appropriations Act, 2017 (Pub. L. No. 115-31) amended 31 U.S.C. § 1105 (a) (35) to require that a cybersecurity funding analysis be incorporated into the President's Budget.

Examples of Implementation

> The FY 2019 President's Budget includes $15 billion of budget authority for cybersecurity-related activities, a $583.4 million (4.1%) increase on the FY 2018 Estimate. Due to the sensitive nature of some activities, this amount does not represent the entire cyber budget.

References

> https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2.10. Establishment of information security programmes by federal agencies

US (federal government)

Main goal(s) of the policy instrument

Prevention

Main government resource(s) used to implement this instrument

> Authority

Main target stakeholders

> Own Institutions

Description of Implementation

> A 2014 law, the Federal Information Security Management Act (FISMA), requires federal agencies to develop, document and implement information security programmes and have independent evaluations of those programmes and practices.

Examples of Implementation

> Directive that authorises the issuance of Treasury Department Publication (TD P) 85-01, 'Treasury IT Security Program', which contains Department-wide IT security requirements and supporting guidance. TD P 85-01 shall define controls for providing such protection. The Chief Information Officer (CIO) is authorised to prescribe, publish and maintain TD P 85-01, which is issued as a separate document. It shall for example (1) set forth the minimum standards or requirements for the security of non-national security and national security IT systems and the information they process, store and communicate.

References

> https://www.gao.gov/products/GAO-19-545?mobile_opt_out=1

> https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td85-01.aspx

Limitation(s) for joint implementation

> Availability of Instrument

2.11. Identification/Certification of cybersecurity workforce in federal agencies

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Authority/Information

Main target stakeholders

> Own Institutions

Description of Implementation

> As required by the Federal Cybersecurity Workforce Assessment Act of 2015, all federal agencies are to identify all positions that perform information technology and cybersecurity, and assign the appropriate employment code to a position. Further, through the John S. McCain National Defense Authorisation Act, the Department of Defense established a Cyber Institute and within 240 days a report had to be submitted to congressional committees on the feasibility of establishing a Cybersecurity Apprentice Program to support on-the-job training for certain cybersecurity positions and facilitate the acquisition of cybersecurity certifications.

Examples of Implementation

> Interpretive Guidance for Cybersecurity Positions by United States Office for Personnel Management on Attracting, Hiring and Retaining a Federal Cybersecurity Workforce.

> US General Services Administration puts out an order that the General Services Administration (GSA) must identify all positions that require the performance of information technology, cybersecurity, or other cyber-related functions; and assign a corresponding cybersecurity code to such positions using the National Initiative for Cybersecurity Education (NICE) coding structure. GSA is required to submit an annual report to the Office of Personnel Management (OPM) that describes the information technology, cybersecurity or other cyber-related roles identified and substantiates the critical need for the designation.

References

> https://www.gao.gov/products/GAO-19-144

> https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/interpretive-guidance-for-cybersecurity-positions.pdf

> https://www.gsa.gov/directives-library/cybersecurity-data-standard-codes-92921-hrm

Limitation(s) for joint implementation

> Availability of Instrument

2.12. Regular reporting requirement for sector-specific critical infrastructure information

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Authority/Information

Main target stakeholders

> Own Institutions

Description of Implementation

> Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21) and EO 13636 demand that sector-specific agencies must support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.

Examples of Implementation

> DHS report guidelines

References

> https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

> https://www.aapa-ports.org/files/PDFs/Sector%20Critical%20Infrastructure%20and%20Key%20Resources%20Protection%20Annual%20Report%20Guidance.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2.13. Mandatory risk reviews for federal agencies

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Authority/Information

Main target stakeholders

> Own Institutions

Description of Implementation

> The Trump Administration issued a much-anticipated Executive Order (EO) addressing cybersecurity, 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure' (11 May 2017). It directs federal executive agency heads to undertake various cybersecurity-related reviews and to report findings to the White House within prescribed timetables ranging from 60 days to one year.

Examples of Implementation

> The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

References

> https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Limitation(s) for joint implementation

> Availability of Instrument

2.14. Monitoring

US (federal government)

Main goal(s) of the policy instrument

> Detection

Main government resource(s) used to implement this instrument

> Authority/Organisation

Main target stakeholders

> Internal Actors, External Actors

Description of Implementation

> Enhanced monitoring techniques to enable the detection and localisation of threats. The Cybersecurity Information Sharing Act (CISA) authorises businesses to monitor their information systems and all information stored on, processed by, or transiting the information system, as long as the monitoring is for the purpose of protecting the information or information systems. The law grants to businesses full immunity from government and private lawsuits and other claims that may arise out of CISA-compliant monitoring in which businesses may engage.

Examples of Implementation

> The NCPS Intrusion Detection capability, delivered via EINSTEIN 1 (E1) (historically known as Block 1.0) and EINSTEIN 2 (E2), is a passive, signature-based sensor grid that monitors network traffic for malicious activity to and from participating Federal Executive D/As.

> The Wide Area Network (WAN) Monitoring effort 'seeks to develop distributed network monitoring capabilities and devices that can be used to identify, characterise, enable, optimise and protect the WANs that compose the Global Information Grid (GIG). This program will develop advanced capabilities to monitor the WANs that will comprise the GIG for detecting information flows that are indicative of malicious behavior, routing problems, or compromised mission capability.'

> Capabilities to deploy intrusion detection systems using passive sensors.

References

> https://www.cisa.gov/national-cybersecurity-protection-system-ncps

> https://www.darpa.mil/attachments/(2G10)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2007%20(Approved).pdf

> https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Limitation(s) for joint implementation

> Availability of Instrument

2.15. Counterintelligence

US (federal government)

Main goal(s) of the policy instrument

> Prevention, Detection, Mitigation/Response

Main government resource(s) used to implement this instrument

> Authority/Organisation/Information

Main target stakeholders

> External Actors

Description of Implementation

> The National Counterintelligence Strategy 2020–2022 names the use of counterintelligence to track and counter foreign operations.

Examples of Implementation

> Develop, train, and retain a cadre of cyber counterintelligence and technical security experts. Development of this national security community will allow for more rapid recognition of threats and vulnerabilities, and more agile responses and integrated approaches to counter adversary cyber and technical activities. Enhance our cyber counterintelligence toolkit: We will work to develop and acquire new capabilities to track and counter foreign cyber and technical operations against the United States and leverage partnerships with the private sector to develop effective countermeasures.

References

> https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf;

> https://www.darpa.mil/attachments/(2G10)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2007%20(Approved).pdf

> https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Limitation(s) for joint implementation

> Availability of Instrument

2.16. (Informal) cooperation on attribution with private sector

US (federal government)

Main goal(s) of the policy instrument

> Detection, Mitigation/Response

Main government resource(s) used to implement this instrument

> Information

Main target stakeholders

> Internal Actors

Description of Implementation

> Cyber attribution is the process by which evidence of a malicious cyber-activity is collected, analysed and associated to an originating party (i.e. the attacker). The US government may informally cooperate with the private sector or publicly mention attribution done by the private sector.

Examples of Implementation

> CrowdStrike provided forensic evidence and analysis for the FBI to review during its investigation into a 2016 hack of Democratic National Committee (DNC) emails.

References

> https://www.rand.org/content/dam/rand/pubs/working_papers/WR1200/WR1267/RAND_WR1267.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2.17. Military network defensive capabilities

US (federal government)

Main goal(s) of the policy instrument

> Prevention, Detection, Mitigation/Response

Main government resource(s) used to implement this instrument

> Organisation/Authority

Main target stakeholders

> Own Institutions

Description of Implementation

> Department of Defense Directive 8530.1: Computer Network Defense (CND), 8 January 2001. 1.1. 'Establishes, in accordance with the computer network defense (CND) policy, definition, and responsibilities necessary to provide the essential structure and support to the Commander in Chief, US Space Command (USCINCSPACE) for Computer Network Defense (CND) within Department of Defense information systems and computer networks.' CND is defined by the US Department of Defense (DoD) as 'Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks' . The broad scope of these CND activities may very well include components that would be considered computer network exploitation (CNE) and computer network attack (CNA).

Examples of Implementation

> Cyber Command's goal is to make sure it has the opportunity to be in foreign cyberspace to be able to conduct operations to counter threats.

> Cyber National Guard: Cyber soldiers are trained to execute offensive cyberspace operations, conduct computer network defence, and detect malicious activity on the electromagnetic battlefield, using advanced military networks and cyberweapon systems.

> Cyber Command's mission against ISIS.

References

> https://www.cyberscoop.com/cyber-command-pentagon-counter-isis-glowing-symphony-foia/

> https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/ https://www.nationalguard.com/careers/cyber

> https://fas.org/irp/offdocs/ppd/ppd-20.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2.18. Coordinated vulnerability disclosure (CVD) process

US (federal government)

Main goal(s) of the policy instrument

> Prevention, Mitigation/Response

Main government resource(s) used to implement this instrument

> Organisational/Informational

Main target stakeholders

> Internal Actors

Description of Implementation

> Coordinated vulnerability disclosure (CVD) is a process for reducing adversary advantage while an information security vulnerability is being mitigated. CVD is a process, not an event. Releasing a patch or publishing a document are important events within the process, but do not define it.

Examples of Implementation

> The Cybersecurity Information Sharing Act's (CISA) CVD programme coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s).

References

> https://www.cisa.gov/coordinated-vulnerability-disclosure-process

> https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Limitation(s) for joint implementation

> Availability of Instrument

2.19. Vulnerability equity management process

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Organisation/Information

Main target stakeholders

> Internal Actors

Description of Implementation

> In accordance with paragraph (49) of National Security Policy Directive-54/Homeland Security Policy Directive-23, Cybersecurity Policy, and the Joint Plan for the Coordination and Application of Offensive Capabilities to Defend US Information Systems, the US government created the Vulnerabilities Equities Process (VEP).

Examples of Implementation

> The VEP is a process used by the US federal government to determine on a case-by-case basis how it should treat zero-day computer security vulnerabilities: whether to disclose them to the public to help improve general computer security, or to keep them secret for offensive use.

References

> https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

Limitation(s) for joint implementation

> Availability of Instrument

2.20. Technical services (e.g. vulnerability scanning)

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Organisation

Main target stakeholders

> Internal Actors, Own Institutions

Description of Implementation

> All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organisations generally, and include cyber hygiene: vulnerability scanning, phishing campaign assessment (PCA), risk and vulnerability assessment (RVA) and validated architecture design review (VADR).

Examples of Implementation

> CISA offers vulnerability scanning (formerly known as cyber hygiene scanning) of internet-accessible systems for known vulnerabilities on a continual basis. As potential vulnerabilities are identified, CISA notifies the organisation so that preemptive risk mitigation efforts may be implemented in order to avert vulnerability exploitation. CISA also offers remote penetration testing (RPT), utilising a dedicated remote team to assess and identify and mitigate vulnerabilities to exploitable pathways. While similar to an RVA, RPT focuses entirely on externally accessible systems.

References

> https://www.us-cert.gov/resources/ncats

Limitation(s) for joint implementation

> Availability of Instrument

2.21. Intelligence sharing with certain states

US (federal government)

Main goal(s) of the policy instrument

> Prevention, Detection, Mitigation/Response

Main government resource(s) used to implement this instrument

> Information

Main target stakeholders

> External Actors

Description of Implementation

> US federal agencies share intelligence about malicious cyber-activities with certain partner countries.

Examples of Implementation

> The 'Five Eyes' intelligence alliance of five English-speaking nations has joined forces with Japan, Germany and France to introduce an information-sharing framework on cyberattacks from countries such as China, people linked to the Japanese government have said.

References

> https://mainichi.jp/english/articles/20190204/p2a/00m/0na/001000c

Notes

> EU member states are part of such intelligence-sharing alliances and may or may not be able to share certain information with other EU member states or the EU, which are not in the alliances.

Limitation(s) for joint implementation

> Availability of Instrument

2.22. Extradition requests

US (federal government)

Main goal(s) of the policy instrument

> Mitigation/Response

Main government resource(s) used to implement this instrument

> Authority

Main target stakeholders

> External Actors

Description of Implementation

> Extradition is where a jurisdiction delivers a person accused or convicted of committing a crime in another jurisdiction over to that jurisdiction's law enforcement. It is a cooperative law enforcement process between the two jurisdictions and depends on the arrangements made between them.

Examples of Implementation

> A 20-year-old Cypriot wanted for hacking offences in the United States is set to be the country's first citizen to be extradited there.

> US asked also to extradite Lori Love, British citizen but a british appeals court on rejected demands from the US government for the extradition citing the inability of US prisons to humanely and adequately treat his medical and mental health ailments.

References

> https://www.reuters.com/article/us-czech-usa-russia-cybercrime/russian-accused-of-massive-u-s-hacking-is-extradited-pleads-not-guilty-idUSKBN1H60VU

> https://www.securityweek.com/first-cypriot-be-extradited-us-hacking-charges

> https://theintercept.com/2018/02/06/citing-u-s-prison-conditions-british-appeals-court-refuses-to-extradite-accused-hacker-lauri-love-to-the-u-s/

Notes

> In partnership with EU member states.

Limitation(s) for joint implementation

> Availability of Instrument

2.23. Software component transparency multi-stakeholder process

US (federal government)

Main goal(s) of the policy instrument

> Prevention

Main government resource(s) used to implement this instrument

> Organisation, Information

Main target stakeholders

> Internal Actors, External Actors

Description of Implementation

> Develops and executes an approach for how manufacturers and vendors can communicate useful and actionable information about the third-party/embedded software components that comprise modern software and IoT devices, and how enterprises can use this data to foster better security decisions and practices. The goal of this initiative is to foster a market offering greater transparency to organisations, which can then integrate this data into their risk-management approach.

Examples of Implementation

> The National Telecommunications and Information Administration (NTIA) is convening a multi-stakeholder process to develop greater transparency of software components for better security across the digital ecosystem.

References

> https://www.npr.org/2019/12/16/788490509/congress-allocates-425-million-for-election-security-in-new-legislation?t=1581602872008

> https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency

Limitation(s) for joint implementation

> Availability of Instrument

2.24. Other 'instruments of national power', e.g. ban of company products

US (federal government)

Main goal(s) of the policy instrument

> Prevention, Mitigation/Response

Main government resource(s) used to implement this instrument

> Information

Main target stakeholders

> External Actors

Description of Implementation

> The National Cyber Strategy states that in response to a cyberattack all possible national security instruments would be available, such as military instruments other than cyber. Moreover, the John S. McCain National Defense Authorization Act established that 'all instruments of national power' will be used to defend, deter and respond to significant cyber threats.

Examples of Implementation

> The Trump administration banned US companies from trading with Huawei after it accused the Chinese giant of espionage and IP (intellectual property) theft. The ban centred on any technology related to 5G technology.

References

> https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Notes

> Possible via NATO Art. 5

Limitation(s) for joint implementation

> Availability of Instrument

2.25. Indictments

US (federal government)

Main goal(s) of the policy instrument

> Mitigation/Response

Main government resource(s) used to implement this instrument

> Authority

Main target stakeholders

> External Actors; Internal Actors

Description of Implementation

> An indictment is a criminal accusation that a person has committed a crime.

Examples of Implementation

> On 19 May 2014, the US Department of Justice indicted five Chinese military hackers for computer hacking and economic espionage directed at six American entities in the US nuclear power, metals and solar products industries.

> The US has charged four members of China's People's Liberation Army with hacking into the credit-reporting agency Equifax.

References

> https://fas.org/sgp/crs/row/IN10376.pdf

> https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/

> https://www.hsdl.org/?abstract&did=788047

> https://www.jstor.org/stable/2706946?seq=1

Limitation(s) for joint implementation

> Availability of Instrument

3. Policy instruments EU and US have in common but with limitations for joint implementation

3.1. Participation in UN processes, e.g. UNGGE

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Organisation, Information **Main target stakeholders** External Actors **Description of Implementation** The US participates in the United Nations Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security (formerly: on developments in the field of information and telecommunications in the context of international security), a UN-mandated working group in the field of information security. Six working groups have been established since 2004, including the GGE 2019–2021. **Examples of Implementation** - A US resolution (A/C.1/73/L.37) underlined the reports of the UN GGE (2010, 2013, and 2015) and called for the establishment of another GGE, mandated to further study norms, confidence-building measures and capacity-building measures, taking account of their effective implementation, to report to the UN General Assembly (GA) in autumn 2021. **References** https://dig.watch/processes/un-gge	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** External Actors **Description of Implementation** The EU is consulted by the United Nations GGE on advancing responsible state behaviour in cyberspace in the context of international security (formerly: on developments in the field of information and telecommunications in the context of international security), a UN-mandated working group in the field of information security. Six working groups have been established since 2004, including the GGE 2019–2021. **Examples of Implementation** - According to UN Resolution 73/223, the UNGGE was obliged to hold regional consultations with the African Union, the European Union, the Organization for Security and Co-operation in Europe (OSCE), the ASEAN and the Organization of American States (OAS). **References** https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf
Limitation(s) for joint implementation	
Legal/Political authority	

3.2. Public attribution

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Mitigation/Response, Prevention **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** Public attribution of cyber incidents to state and non-state actors. Cyber attribution is the process by which evidence of a malicious cyber-activity is collected, analysed, and associated to an originating party (i.e. the attacker). **Examples of Implementation** - Obama Administration attributed to Russia in 2016. - Trump Administration attributed that Russia was behind the NotPetya malware attack following its announcement of North Korea's role in the similar WannaCry attack. **References** https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/ **Notes** US has done coordinated attribution with EU member states, e.g. the coordinated attribution of NotPetya included the governments of the US, the UK, Denmark, Lithuania, Estonia, Canada, and Australia and called out Russia in official statements. Official statements of support came from New Zealand, Norway, Latvia, Sweden and Finland.	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** External Actors **Description of Implementation** Public attribution of cyber incidents to state and non-state actors. Cyber attribution is the process by which evidence of a malicious cyber-activity is collected, analysed, and associated to an originating party (i.e. the attacker). **Examples of Implementation** - In the Council Decision Common Foreign and Security Policy (CFSP)) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its member states, the EU attributed cyber incidents to non-state actors (six individuals and three entities) from Russia and China. **References** https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/
Limitation(s) for joint implementation	
Legal/Political authority	

3.3. Démarches

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority, Information **Main target stakeholders** External Actors **Description of Implementation** A démarche is considered less formal and is 'a request or intercession with a foreign official': a written request that is presented without attribution from the composing state and is, therefore, delivered in person. It may signal to a state an EU position on malicious cyber-activities. **Examples of Implementation** - The former Office of the Coordinator for Cyber Issues used diplomatic démarches to seek the assistance of more than 20 countries when a persistent Iranian-sponsored botnet targeted US financial institutions. This collective action, where each country used its authorities and tools to help address a shared threat, proved very effective in mitigating the malicious activity. **References** https://www.afsa.org/diplomacy-cyberspace	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority/Information **Main target stakeholders** External Actors **Description of Implementation** A démarche is considered less formal and is 'a request or intercession with a foreign official': a written request that is presented without attribution from the composing state and is, therefore, delivered in person. It may signal to a state an EU position on malicious cyber-activities. **Examples of Implementation** - Demarchés are not public but are seen as a tool in the cyber-diplomacy toolbox. EU démarches improve understanding of the national policies of other states with regard to international peace and security, with a view to reducing risks of misperceptions or misunderstanding in the case of malicious cyber-incidents that may be considered as originating in or transiting through their territory. **References** https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf
Limitation(s) for joint implementation	
Legal/Political authority	

3.4. Sanctions

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Mitigation/Response **Main government resource(s) used to implement this instrument** Authority, Treasure **Main target stakeholders** External Actors **Description of Implementation** The cyber-related sanctions programme represents the implementation of multiple legal authorities. Some of these authorities are in the form of Executive Orders issued by the President. Other authorities are public laws (statutes) passed by Congress. These authorities are further codified by US Department of the Treasury's Office of Foreign Assets Control (OFAC) in its regulations, which are published in the Code of Federal Regulations (CFR). Modifications to these regulations are posted in the Federal Register. The US sanctions regime was initially covered by Executive Order 13694 in 2015 and was expanded by Executive Order 13757 in 2017, detailing the scope of cyber actions that are subject to sanctions. **Examples of Implementation** - OFAC announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. **References** https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information https://home.treasury.gov/news/press-releases/sm774	**Main goal(s) of the policy instrument** Mitigation/Response **Main government resource(s) used to implement this instrument** Authority/Treasure **Main target stakeholders** External Actors **Description of Implementation** The EU may impose restrictive measures against third countries, entities or individuals on the basis of a Council decision adopted under Article 29 of the Treaty on European Union (TEU) coupled with a Council regulation setting out the necessary measures for its operation, adopted under Article 215 of the Treaty on the Functioning of the European Union (TFEU). On 17 May 2019, the Council established a framework that allows the EU to impose targeted restrictive measures to deter and respond to cyberattacks that constitute an external threat to the EU or its member states, including cyberattacks against third states or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP). Cyberattacks falling within the scope of this new sanctions regime are those that have significant impact and that originate or are carried out from outside the EU, or use infrastructure outside the EU, or are carried out by persons or entities established or operating outside the EU, or are carried out with the support of persons or entities operating outside the EU. Attempted cyberattacks with a potentially significant effect are also covered by this sanctions regime. **Examples of Implementation** - The Council decided to impose restrictive measures against six individuals and three entities responsible for or involved in various cyberattacks. These include the attempted cyberattack against the Organisation for the Prohibition of Chemical Weapons (OPCW) and those publicly known as 'WannaCry', 'NotPetya' and 'Operation Cloud Hopper'. **References** https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/ https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/
Limitation(s) for joint implementation	
Legal/Political authority	

3.5. Adoption of OSCE cyber confidence-building measures

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Information, Authority **Main target stakeholders** External Actors **Description of Implementation** The OSCE participating states in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in cooperation with relevant international organisations, hereinafter referred to as 'security of and in the use of ICTs'. They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate cooperation, transparency, predictability and stability, and to reduce the risks of misperception, escalation and conflict that may stem from the use of ICTs. **Examples of Implementation** Statement by the US: 'The United States welcomes the adoption of additional cyber confidence-building measures (CBMs) to enhance inter-State co-operation, transparency, predictability and stability among participating States. These practical risk-reduction measures build on an earlier set of CBMs adopted in 2013 that were without precedent in the international arena.' - Implementation of CBMs such as cyber-dialogues. **References** https://www.osce.org/pc/227791?download=true	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information, Authority **Main target stakeholders** External Actors **Description of Implementation** The OSCE participating states in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in cooperation with relevant international organisations, hereinafter referred to as 'security of and in the use of ICTs'. They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate cooperation, transparency, predictability and stability, and to reduce the risks of misperception, escalation and conflict that may stem from the use of ICTs. **Examples of Implementation** Statement by the EU: 'The European Union and its Member States welcome the adoption of the additional cyber confidence-building measures to reduce the risks of conflict stemming from the use of the information and communication technologies. This decision complements and consolidates the initial set of CBMs that was adopted in 2013, which was the first of its kind adopted by a regional organization. EU supports the Decision No. 1202 OSCE Confidence-Building measures to reduce the risks of conflict stemming from the use of information and communication technologies.' - Implementation of CBMs such as cyber-dialogues. **References** https://www.osce.org/pc/227791?download=true

Limitation(s) for joint implementation

Legal/Political authority

3.6. Requirement of a cybersecurity R&D strategic plan

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Own Institutions **Description of Implementation** Cybersecurity Enhancement Act of 2014 (Public Law 113-274) requires the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development (NITRD) Program to develop a strategy for cybersecurity research and development to guide the overall direction of federally funded R&D in cybersecurity. **Examples of Implementation** - The 2019 Plan identifies four interrelated defensive capabilities (deter, protect, detect and respond) and six priority areas for cybersecurity R&D (artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development) as the focusing structure for federal cybersecurity R&D activities and investments to benefit the nation. **References** https://www.whitehouse.gov/wp-content/uploads/2019/12/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf https://www.nitrd.gov/cybersecurity https://www.congress.gov/bill/113th-congress/senate-bill/1353	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Internal Actors **Description of Implementation** The European Union Framework Programme for Research and Innovation 2021–2027 (Horizon Europe) is informed by the Strategic Plan for Horizon Europe. Any cybersecurity funded research should drive the implementation of the relevant parts of Digital Europe and Horizon Europe programmes according to its multi-annual strategic plan, and the strategic planning process of Horizon Europe. **Examples of Implementation** - The 2019 document on the strategic plan for Horizon Europe mentions the goals of 'Increased cybersecurity based on more effective use of digital technologies, strong orientation on privacy and fundamental rights and a robust digital infrastructure to counter cyber-attacks'. **References** https://ec.europa.eu/research/pdf/horizon-europe/ec_rtd_orientations-towards-the-strategic-planning.pdf

Limitation(s) for joint implementation

Legal/Political authority

3.7. Public statements

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Mitigation/Response **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** External Actors **Description of Implementation** Public statements in response to malicious cyber-activities or to define cybersecurity policy in reaction. **Examples of Implementation** - Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment. - In 2012 State Department Legal Adviser Harold Koh took an important step towards publicly elucidating the US positions on how international law applies to cyberspace **References** https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&=&context=fss_papers&=&sei-redir=1&referer=https%253A%252F%252Fwww.google.com%252Furl%253Fq%253Dhttps%253A%252F%252Fdigitalcommons.law.yale.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%25253D5858%252526context%25253Dfss_papers%2526sa%253DD%2526ust%253D1591087151263000%2526usg%253DAFQjCNFLq5Kl-70STfuMSTBJ12_iDC__oQ#search=%22https%3A%2F%2Fdigitalcommons.law.yale.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D5858%26context%3Dfss_papers%22	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Information, Authority **Main target stakeholders** External Actors, Internal Actors **Description of Implementation** Statements in response to cyberattacks or in order to define cybersecurity policy and explain reaction. Issuing a statement expressing concern or condemning general cyber trends or certain cyber-activities could have a signalling function and underline awareness, as well as serving as a form of strategic communication and, by signalling the likely consequences of malicious cyber activity, influencing potential aggressors to refrain from engaging in malicious cyber-activities. Statements can be requested by the member states, the High Representative/Vice President (HRVP), the HRVP Cabinet or the Spokesperson's Team or proposed by an EU delegation. Member states are consulted on declarations by the High Representative on behalf of the EU, usually by means of the Correspondance Européenne (COREU) silence procedure. Guidelines on statements and declarations set out four types of statements at EU level, namely: declarations by the High Representative on behalf of the EU; High Representative statements; spokesperson statements; and local EU statements. **Examples of Implementation** - In reaction to WannaCry, European Commission spokesperson Margaritas Schinas stated that 'The use of cyberattacks for criminal purposes is an increasing threat which requires a global and coordinated response from the EU and its member states. While member states remain on the front line for much of this work, the EU has an important role to play in shaping and updating strategies to deal with these threats and reinforcing the regulatory framework at the EU level on cybersecurity and cybercrime.' - In reaction to the 28 October 2019 cyberattack targeting Georgia, the EU put out a declaration by the High Representative on behalf of the EU with a call to promote and conduct responsible behaviour in cyberspace, condemning the attack. **References** https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf https://www.dw.com/en/eu-agencies-had-tools-to-contain-wannacry-ransomware/a-38850576

https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/

Limitation(s) for joint implementation

Legal/Political authority

3.8. Promotion of threat intelligence sharing by other stakeholders with government or peers

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Detection **Main government resource(s) used to implement this instrument** Authority/Treasure **Main target stakeholders** Internal Actors **Description of Implementation** The concept of Information Sharing and Analysis Centers (ISACs) was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed on 22 May 1998, after which the federal government asked each critical infrastructure sector to establish sector-specific organisations to share information about threats and vulnerabilities. Programmes are set up and funding may be provided for other activities that promote the sharing of information among stakeholders. **Examples of Implementation** - Some ISACs formed as early as 1999, and most have been in existence for at least ten years, e.g. the Electricity ISAC (E-ISAC). - The Department of Energy (DOE) announced a funding award for Dragos' 'Neighborhood Keeper' Program for Threat Detection and Shared Threat Intelligence Across Small Infrastructure Providers. - DHS's National Network of Fusion Centers typically provides information sharing and analysis for an entire state. These centers, run by state and local governments, are designed to take what may seem to be disparate pieces of information on a variety of subjects and 'fuse ' them together to be able to recognise threat indicators. An example of a fusion centre that focuses on cyber matters is the DC NTIC Cyber Center. - Businesses will enjoy immunity from any lawsuit that may arise out of such sharing. However, CISA also provides that sharing of cyber-threat information with the federal government will not constitute the waiver of any applicable provision or protection provided by existing law, including trade secret protection. **References** https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability https://www.nationalisacs.org/member-isacs https://dragos.com/media/department-of-energy-doe-announces-funding-award-for-dragos-	**Main goal(s) of the policy instrument** Prevention, Detection **Main government resource(s) used to implement this instrument** Authority/Information/Treasure/Organisation **Main target stakeholders** Internal Actors **Description of Implementation** EU institutions foster the sharing of threat intelligence through networks and communities by setting incentives via European legislations such as the NIS Directive and the Cybersecurity Act to nurture the creation of sectoral ISACs and PPPs within the EU. The NIS Directive tasks the operators to implement requirements on incident reporting. The creation of sectoral ISACs at national level could further assist with the implementation of these provisions. Further EU institutions inform about intelligence sharing and fund projects that foster threat intelligence sharing. The EU also supports the sharing of information organisationally by establishing different fora. **Examples of Implementation** - Computer Security Incident Response Teams (CSIRTs) provide information about threat intelligence processes to their constituency and partners for protecting their assets and avoiding being the target of an attack. - ENISA also contributes, with a Report on Cyber Security Information Sharing in the Energy Sector. - Funding of the MISP – Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing. - Establishment of the CSIRT network, which comprises EU member states' appointed CSIRTs and CERT-EU (CSIRTs network members). - EU Aviation ISAC. - The creation of an EU Hybrid Fusion Cell within the existing EU INTCEN structure to receive and analyse classified and open-source information on hybrid threats. **References** https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/energy https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing https://ec.europa.eu/digital-single-market/en/news/misp-open-source-platform-threat-intelligence

neighborhood-keeper-program-for-threat-detection-and-shared-threat-intelligence-across-small-infrastructure-pro/	https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report/ https://www.un.org/disarmament/wp-content/uploads/2019/08/georgia-73-27-73-266-dea-mod.pdf

Note: European companies could be identified that take part in US ISACs but with no joint implementation of concepts of ISACs or promotion of such, therefore this does not constitute joint implementation.

Limitation(s) for joint implementation

Legal/Political authority

3.9. International (operational) agreements

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Authority/Information **Main target stakeholders** External Actors **Description of Implementation** International agreements are understandings or commitments between two or more countries. An agreement between two countries is called 'bilateral', while an agreement between several countries is 'multilateral'. 'Informal agreements are the most common form of international cooperation. Ranging from simple oral deals to detailed executive agreements, they permit states to conclude profitable bargains without the formality of treaties' (Lipson, 1991). **Examples of Implementation** - US–China Cybersecurity Agreement: In principle, the US and China agreed, among other things, to provide timely responses to requests for information and assistance concerning malicious cyber-activities, refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property, pursue efforts to further identify and promote appropriate norms of state behaviour in cyberspace within the international community, and establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. - Ratified the Budapest Convention. **References** https://fas.org/sgp/crs/row/IN10376.pdf https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/ https://www.hsdl.org/?abstract&did=788047 https://www.jstor.org/stable/2706946?seq=1	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information/Organisation/Authority **Main target stakeholders** Internal Actors, External Actors **Description of Implementation** International agreements are understandings or commitments between two or more countries. An agreement between two countries is called 'bilateral', while an agreement between several countries is 'multilateral'. 'Informal agreements are the most common form of international cooperation. Ranging from simple oral deals to detailed executive agreements, they permit states to conclude profitable bargains without the formality of treaties' (Lipson, 1991). **Examples of Implementation** - Europol's operational agreements. - Signed the Budapest Convention, the only binding international agreement on cybersecurity focusing on cybercrime. It facilitates operational cooperation and sets guidelines for developing and harmonising the national legal frameworks. **References** https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1 https://www.jstor.org/stable/2706946?seq=1

Note: European companies could be identified that take part in US ISACs but with no joint implementation of concepts of ISACs or promotion of such, therefore this does not constitute joint implementation.

Examples of joint implementation

Agreement between The United States of America and Europol and Supplemental Agreement between Europol and The United States of America on the Exchange of Personal Data and Related Information.

Limitation(s) for joint implementation

Legal/Political authority

3.10. Incident reporting

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Detection, Mitigation/Response **Main government resource(s) used to implement this instrument** Organisational/Informational, Authority **Main target stakeholders** Internal Actors **Description of Implementation** Incident reporting is not made mandatory by the federal government for most critical infrastructure operators or companies. Federal and SLTT regulators may have mandatory reporting requirements for certain types of cyber-incidents in certain sectors. Incident reporting is therefore encouraged by provision of platforms and networks. However, there may be mandatory reporting on incidents, such as the DoD Reporting Requirements on Cyber Breaches and Loss of PII and CUI. In the case of 'a significant loss of personally identifiable information [PII] [or] controlled unclassified information [CUI] by a cleared defense contractor', the Secretary 'shall promptly submit to the congressional defense committees notice in writing of such loss'. Whether or how this provision will impact notification requirements for contractors and vendors remains to be seen. **Examples of Implementation** - The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. - The DoD Reporting Requirements for cleared defence contractors. **References** https://www.us-cert.gov/forms/report	**Main goal(s) of the policy instrument** Detection, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Internal Actors **Description of Implementation** Incident reporting is an important requirement of the NIS Directive. Groups within the scope of the NIS Directive must notify a central authority of incidents that could significantly impact the continuity of services. **Examples of Implementation** - On member-state level in Germany: certain critical infrastructure operators must share incidents with Germany's federal office for information security. **References** https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
Limitation(s) for joint implementation	
Legal/Political authority	

3.11. Declaring critical infrastructures for special protection

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Internal Actors **Description of Implementation** Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7. PPD-21 identifies 16 critical infrastructure sectors. **Examples of Implementation** - The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector. The nation's transportation system quickly, safely and securely moves people and goods through the country and overseas. **References** https://www.cisa.gov/critical-infrastructure-sectors https://www.cisa.gov/transportation-systems-sector	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Internal Actors **Description of Implementation** The NIS Directive requires the declaration of essential service operators, which have to abide by certain rules. **Examples of Implementation** - Implemented on member-state level, e.g. the German IT Security Act (ITSiG) came into force on 25 July 2015. Section 8a (1) BSIG states that operators of critical infrastructures must take organisational and technical precautions to avoid disruptions in the availability, integrity, authenticity and confidentiality of their IT-related systems, components and processes. Critical infrastructures (KRITIS) are organisational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences. A legislative decree was issued in accordance with Section 10 (1) BISG that sets out which systems are considered to be critical infrastructure. The industry-specific security standard is structured as a framework and is based on the content of the international series of standards ISO / IEC 27000. **References** https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/B3S_ITK_V1.06_en.pdf?__blob=publicationFile
Limitation(s) for joint implementation	
Legal/Political authority	

3.12. Requirement of responsible agency/contact for responses

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Own Institutions **Description of Implementation** PPD-21 assigns a federal agency, known as a Sector-Specific Agency (SSA), to lead a collaborative process for critical infrastructure security within each of the 16 critical infrastructure sectors. **Examples of Implementation** - For the Water and Wastewater Systems Sector, the Environmental Protection Agency is the SSA. **References** https://www.cisa.gov/sector-specific-agencies	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Internal Actors **Description of Implementation** NIS Directive demands point of contact on member states level for operational and technical response and the EU cyber diplomacy toolbox foresees a contact point on member states level as well which are usually the cyber attachés **Examples of Implementation** - cyber attachés on member state level for cyber diplomacy toolbox - NIS point of contact in Germany - Single point of contact Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik **References** https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-germany
Limitation(s) for joint implementation	
Legal/Political authority	

4. Policy instruments the US and EU have in common lower joint implementation limitations and address joint goals

4.1. Crowd-sourced vulnerability identification via hackathons and bug bounty challenges (with awards)

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Detection **Main government resource(s) used to implement this instrument** Organisational/Treasure/Authority **Main target stakeholders** Internal Actors **Description of Implementation** The Department of Defense Strategy 2018 noted that the DoD will continue to identify crowdsourcing opportunities, such as hackathons and bug bounties, in order to identify and mitigate vulnerabilities more effectively and to foster innovation. **Examples of Implementation** - The DoD Invited hackers to test enterprise system security used for global operations. - Hack the Pentagon programme. - Hack the Air Force challenge. - The President's Cup cybersecurity competition gives awards. **References** https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf https://www.hackerone.com/press-release/us-department-defense-kicks-fifth-bug-bounty-challenge-hackerone https://fortune.com/2019/05/05/trump-president-cup-cybersecurity-contest-america/ https://www.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F91459-cisa-hosts-first-annual-presidents-cup-cybersecurity-competition **Notes** - Only implemented together with Five Eyes countries that also have this instrument.	**Main goal(s) of the policy instrument** Prevention, Detection **Main government resource(s) used to implement this instrument** Organisational, Treasure **Main target stakeholders** Internal Actors **Description of Implementation** The EU's bug bounty programme and hackathons are implemented through the European Parliament's pilot project 'Governance and quality of software code – Auditing of free and open source software'. It is part of EU-FOSSA, which is managed by the European Commission's Directorate General of Informatics (DIGIT). **Examples of Implementation** - The EU-FOSSA 2 bug bounty programme has received over 400 bug reports and has paid close to €100,000 (April 2019). - In 2019, the EU-FOSSA 2 project organised three hackathon events in Brussels. **References** https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2020-06/EU-FOSSA%202%20-%20D3.3%20Hackathon%20Results%20Summary%20FINAL.pdf https://www.youtube.com/watch?v=oPCeDAD9sjk EU-FOSSA 2 https://joinup.ec.europa.eu/collection/eu-fossa-2/news/ready-challenge https://ec.europa.eu/digital-single-market/en/news/eu-bug-bounty-programme-open-source-software-gives-awards-eur-25000

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Common understanding of threats and vulnerabilities

4.2. Digital forensics capacities

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Mitigation/Response **Main government resource(s) used to implement this instrument** Organisation **Main target stakeholders** Internal Actors, Own Institutions **Description of Implementation** Digital forensics capacities are there for the collection, preservation, analysis and presentation of computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence or law enforcement investigations. **Examples of Implementation** - Through the Cyber Forensics project, DHS S&T partners with the NIST CFTT project to provide forensic tool testing reports to the public. The CFTT project has established a methodology for testing computer forensic software tools utilising tool specifications, test procedures, test criteria, test sets and test hardware. - The FBI has cyber squads in each of its 56 field offices, with more than 1,000 advanced cyber-trained FBI agents, analysts and forensic examiners (numbers from 2011). **References** https://www.dhs.gov/science-and-technology/nist-cftt-reports	**Main goal(s) of the policy instrument** Detect and react **Main government resource(s) used to implement this instrument** Organisation, Information **Main target stakeholders** Internal Actors, Own Institutions **Description of Implementation** Europol's European Cybercrime Centre (EC3) was launched in January 2013 to strengthen the law enforcement response to cybercrime in the EU and thereby help protect European citizens and businesses. The EC3 provides highly specialised technical and digital forensic support capabilities to investigations and operation. **Examples of Implementation** - The development in 2013 of the forensic lab that provides a professional and fully equipped environment for technical support in digital forensics. - Forensic crime scene investigation CSI photography to support member states on the spot is being developed. - Under the umbrella of EC3, a number of the EU's leading digital forensic experts called for the adoption of the Cyber-investigation Analysis Standard Expression (CASE) as a standard digital forensic format at a meeting hosted at the agency's headquarters in The Hague on 11 and 12 May 2017. **References** https://www.europol.europa.eu/newsroom/news/eu-forensic-experts-call-for-action-new-cyber-investigation-standard https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf

Examples of joint implementation

The Agreement Between the US and the European Police Office states in Article 3 that Europol and the US agree to exchange technical information that includes, but is not limited to, forensic police methods and investigative procedures. see https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1

Limitation(s) for joint implementation

Resources

4.3. Funding to improve cybersecurity

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Treasure, Authority **Main target stakeholders** Internal Actors **Description of Implementation** Congress passes a funding bill that includes grants that states can apply to in order to improve election infrastructure. **Examples of Implementation** - In 2019 Congress allocated about $425 million in funding for election security ahead of the 2020 presidential election. **References** https://www.npr.org/2019/12/16/788490509/congress-allocates-425-million-for-election-security-in-new-legislation?t=1581602872008	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Treasure, Authority **Main target stakeholders** Internal Actors **Description of Implementation** Under the call 'Protecting the infrastructure of Europe and the people in the European smart cities of Horizon 2020', the Commission allocates around €7–8 million per project to address both physical and cyber threats to critical infrastructure. The latest Connecting Europe Facility (CEF) cybersecurity call offers funding opportunities to key stakeholders identified by the NIS Directive such as European CSIRTs, operators of essential services (banks, hospitals, electricity and gas providers, railways, airlines, domain name providers, etc.) and various public authorities. **Examples of Implementation** - Example projects funded are Secure and Safe Internet of Things (SERIOT) security frameworks and technological validation to optimise IoT platforms and networks information security in a holistic and cross-layered approach; SecureIoT works on predictive, spanned IoT security services to be used as building blocks, security data collection and monitoring by IoT developers. **References** https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross
Limitation(s) for joint implementation	
Resources	
Potential to address the following joint goals (ranked):	
Assisting each other in improving resilience	

4.4. Cyber threat and vulnerability (indicator) analysis

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Organisation/Information **Main target stakeholders** Own Institutions **Description of Implementation** Federal agencies do assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations. **Examples of Implementation** - Technical report about the Cyber Threat and Vulnerability Analysis of the US Electric Sector by US Department of Energy Office of Scientific and Technical Information - Department of Homeland Security's Continuous Diagnostics and Mitigation program build a dashboard, the CDM, which provides agencies with overall data on their cybersecurity risks and vulnerabilities. **References** https://www.osti.gov/biblio/1337873-cyber-threat-vulnerability-analysis-electric-sector https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf https://www.cisa.gov/critical-infrastructure-vulnerability-assessments https://www.fifthdomain.com/civilian/dhs/2020/04/01/agencies-to-get-more-insight-into-their-cybersecurity-posture-this-month/?utm_source=Sailthru&utm_medium=email&utm_campaign=Fifth%20Daily%204.3&utm_term=Editorial%20-%20Daily%20Brief	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information/Organisation **Main target stakeholders** Internal Actors **Description of Implementation** 2016 Joint Framework and 2018 Joint Communication on (FoP) Countering Hybrid Threats. The Council's Friends of Presidency Group on Countering Hybrid Threats has continued its work on a risk survey launched in December 2017 and addressed to the Member States to identify key vulnerabilities, including specific hybrid-related indicators, potentially affecting national and pan-European structures and networks. To date, 24 member states have provided input to the survey. The Commission, in cooperation with member states, has finalised the work on developing vulnerability indicators for the resilience and protection of critical infrastructure against hybrid threats. The report also covers related areas such as societal and media vulnerabilities that are pertinent to hybrid threats. The manual of indicators was adopted in November 2018 and put at the disposal of member states via the dedicated Critical Infrastructure Information and Warning Network (CIWIN) document repository. **Examples of Implementation** - Vulnerability Indicators for energy systems - In December 2015, DG Energy created the Energy Expert Cyber Security Platform (EECSP) in cooperation with other services. Its purpose was precisely to analyse the specific needs of the energy sector in terms of cybersecurity. Based on its findings and as a direct action following from the Clean Energy for All Europeans package, the European Commission set up a Stakeholder Working Group to focus on practical approaches and solutions to improve the resilience of the energy network in spring 2017. The group finalised its report and recommendations to the Commission early 2019. - Briefing by the European Parliamentary Research Service (EPRS). - Proposed follow-up actions include the engagement of member states in practical exercises to further test the concept and identify vulnerabilities, gaps and areas for improvement, as well as further work on the areas of detection of a hybrid campaign/attack and attribution of the relevant activities. **References** https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf

https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf

Limitation(s) for joint implementation
Resources
Potential to address the following joint goals (ranked):
Common understanding of threat and vulnerabilities

4.5. Gathering and sharing of best practices

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Detection and Mitigation/Response **Main government resource(s) used to implement this instrument** Information/Treasure/Organisation **Main target stakeholders** Internal Actors **Description of Implementation** The Department of Homeland Security Cybersecurity and Infrastructure Agency as well as other federal agencies gather and publish best practices in an effort to bolster cybersecurity and benchmark activities of domestic target groups, such as local governments, companies and critical infrastructures. **Examples of Implementation** - DHS informs small organisations on cybersecurity best practices. - The US Department of Transportation, National Highway Traffic Safety Administration granted a study that gathered best practices and observations in the field of cybersecurity involving electronic control systems across a variety of industry segments where the safety of life is concerned **References** https://healthitsecurity.com/news/dhs-shares-cybersecurity-best-practices-for-small-organizations https://www.hsdl.org/?view&did=806518 https://www.us-cert.gov/resources/sltt	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information/Organisation **Main target stakeholders** Internal Actors **Description of Implementation** 2016 Joint Framework and 2018 Joint Communication on (FoP) Countering Hybrid Threats. The Council's Friends of Presidency Group on Countering Hybrid Threats has continued its work on a risk survey launched in December 2017 and addressed to the Member States to identify key vulnerabilities, including specific hybrid-related indicators, potentially affecting national and pan-European structures and networks. To date, 24 member states have provided input to the survey. The Commission, in cooperation with member states, has finalised the work on developing vulnerability indicators for the resilience and protection of critical infrastructure against hybrid threats. The report also covers related areas such as societal and media vulnerabilities that are pertinent to hybrid threats. The manual of indicators was adopted in November 2018 and put at the disposal of member states via the dedicated Critical Infrastructure Information and Warning Network (CIWIN) document repository. **Examples of Implementation** - Vulnerability Indicators for energy systems - In December 2015, DG Energy created the Energy Expert Cyber Security Platform (EECSP) in cooperation with other services. Its purpose was precisely to analyse the specific needs of the energy sector in terms of cybersecurity. Based on its findings and as a direct action following from the Clean Energy for All Europeans package, the European Commission set up a Stakeholder Working Group to focus on practical approaches and solutions to improve the resilience of the energy network in spring 2017. The group finalised its report and recommendations to the Commission early 2019. - Briefing by the European Parliamentary Research Service (EPRS). - Proposed follow-up actions include the engagement of member states in practical exercises to further test the concept and identify vulnerabilities, gaps and areas for improvement, as well as further work on the areas of detection of a hybrid campaign/attack and attribution of the relevant activities. **References** https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf

https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf

Examples of joint implementation
EU and US share best practices via fora such as the Global Forum for Cyber Expertise. US best practices are cited in EU best practice examples and the exchange of best practices is noted in EU–US Dialogue as a joint goal.
Limitation(s) for joint implementation
Resources
Potential to address the following joint goals (ranked):
Becoming and Assisting each other in improving resilience; improving cybersecurity workforce; improving response mechanisms and cooperation among a diverse set of stakeholders

4.6. Classified and open-source cyber-threat intelligence gathering and sharing by government with other stakeholders

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Detection **Main government resource(s) used to implement this instrument** Authority/Organisation **Main target stakeholders** Internal Actors **Description of Implementation** The Cybersecurity Information Sharing Act of 2015 directs the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense and the Attorney General, in consultation with the heads of the appropriate federal entities, to jointly develop and issue procedures to facilitate and promote e.g. timely sharing of classified cyber-threat indicators (CTIs) and defensive measures (DMs) in the possession of the federal government with representatives of relevant federal entities and non-federal entities that have appropriate security clearances; timely sharing with relevant federal entities and non-federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorised uses under this title, in the possession of the federal government that may be declassified and shared at an unclassified level; and timely sharing with relevant federal entities and non-federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the federal government. **Examples of Implementation** - The vision of the Enhance Shared Situational Awareness (ESSA) initiative is to create real-time cybersecurity situational awareness, to enable integrated operational actions, and to improve the security of the US government and US critical infrastructure. ESSA lays the foundation to share the right information, in time to make a difference and in formats that reduce human workload and time to action. - The DHS's free Automated Indicator Sharing (AIS). AIS participants connect to a DHS-managed system in the Department's National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber-threat indicators. - In April 2017, the Intelligence Community Security Coordination Center (IC SCC) deployed a capability—the Intelligence Community Analysis and Signature Tool (ICOAST)—to increase sharing of cybersecurity threat intelligence at the top-secret security level - The National Security Agency (NSA) receives and disseminates information relevant to cybersecurity at	**Main goal(s) of the policy instrument** Prevention, Detection **Main government resource(s) used to implement this instrument** Information/Organisation **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** EU institutions gather and share publicly available information on threats, and use open-source intelligence (OSINT) to analyse threats. The EU Hybrid Fusion Cell within the existing EU Intelligence Analysis Centre (INTCEN) structure can receive and analyse classified and open-source information on hybrid threats. **Examples of Implementation** - CERT-EU ongoing threats publicly available on website. - The ENISA Threat Landscape (ETL) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. - Georgian authorities sign new MoUs on information and experience sharing in the field of cybersecurity with different countries. Georgian technical security community is also part of European and international cyber-incident-sharing platforms (CERT.EU, Trusted Introducer, Team Cymru, etc.). **References** https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

the top-secret, secret and unclassified levels.
- The Cyber Information Sharing and Collaboration Program (CISCP) enables information exchange and the establishment of a community of trust between the federal government and critical infrastructure owners and operators.

References

https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf

https://www.nextgov.com/cybersecurity/2020/01/survey-financial-sector-agencies-policies-sharing-cyber-threats-inconsistent/162560/

https://www.oversight.gov/sites/default/files/oig-reports/CIGFO-2020-01.pdf

https://www.dodig.mil/Reports/Audits-and-Evaluations/Article/2048074/unclassified-joint-report-on-the-implementation-of-the-cybersecurity-informatio/

https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability

Limitation(s) for joint implementation

Resources, Lack of Capability (for classified intelligence)

Potential to address the following joint goals (ranked):

Common understanding of threats and vulnerabilities

4.7. Political/strategic threat assessment

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** Internal Actors **Description of Implementation** The US intelligence community presents assessment of threats to US national security to members of the US Senate Select Committee on Intelligence (sometimes referred to as the Intelligence Committee or SSCI), which is dedicated to overseeing the intelligence community. The statements reflect the collective insights of that community. **Examples of Implementation** - Statement for the record worldwide threat assessment of the US intelligence community presented in Congress and published. It includes a section on cyber matters. **References** https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Authority/Information/Organisation **Main target stakeholders** Own Institutions; Internal Actors **Description of Implementation** In the Council Decision of 24 June 2014 for the arrangement for implementation of the solidarity clause, it was decided that in order to regularly assess the threats facing the Union, the European Council may request the Commission, the High Representative for Security Policy and other EU agencies to produce reports on specific threats that can include cyber threats; under the EUINTCEN process, 'finished intelligence' material from the member states may be shared. INTCEN's products include 'intelligence assessments', 'strategic assessments' and 'special reports and briefings'. The Hybrid Fusion Cell, created inside the European External Action Service (EEAS) also provides strategic analysis to EU decision-makers. **Examples of Implementation** - Reports are not public. **References** https://ccdcoe.org/uploads/2018/11/EU-140624-Solidarity.pdf https://digit.site36.net/tag/hybrid-fusion-cell/

Note: Cooperation happens not bilaterally but via NATO's MISP; however, that does not constitute joint implementation.

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Common understanding of threats and vulnerabilities

4.8. Provision of guidelines/frameworks for standardisation and taxonomy

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** Internal Actors, External Actors **Description of Implementation** The NIST Cybersecurity Framework provides a policy framework on how private-sector organisations in the US can assess and improve their ability to prevent, detect and respond to cyberattacks. Organisations that lack a formal cybersecurity risk management programme could use the guidance to establish risk-based cyber priorities. Promoting international alignment and engaging with the international community has been an increasingly important focus for the Cybersecurity Framework effort. The NCCIC Cyber Incident Scoring System (NCISS) is designed to provide a repeatable and consistent mechanism for estimating the risk of an incident. **Examples of Implementation** - The Transportation Systems Sector Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for transportation systems sector owners and operators to apply the tenets of the NIST Cybersecurity Framework to help reduce cyber risks. - CISA Cyber Incident Scoring System. - Dams Sector Cybersecurity Framework Implementation Guidance. - Translations of the NIST Framework in various languages as well as adaptations of the frameworks by governments and industries across the globe, starting with the Japanese translation produced by Japan's Information-technology Promotion Agency (IPA), and translations in Italian, Hebrew, Spanish, Arabic and, most recently, Portuguese. - NIST Framework website 'International Resources' lists all translations and adaptions. **References** https://www.nist.gov/cyberframework https://www.nist.gov/cyberframework/picking-frameworks-pace-internationally https://us-cert.cisa.gov/sites/default/files/c3vp/framework_guidance/dams-framework-implementation-guide-2015-508.pdf	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information, Organisation **Main target stakeholders** Internal Actors **Description of Implementation** ENISA has issued this report to assist member states and digital service providers (DSPs) in providing a common approach regarding the security measures for DSPs. This initiative has been achieved by examining current information and network security practices for the DSPs across the EU. It has brought to light some important findings that can add to existing security objectives and measures in information technology infrastructures in Europe. Taxonomies result from collaboration initiatives, such as the annual ENISA/EC3 Workshop which involved CSIRTs, Law Enforcement Agencies, ENISA, and EC3 and created the incident classification taxonomy. **Examples of Implementation** -Technical guidelines for the implementation of minimum-security measures for DSPs. - Reference Incident Classification Taxonomy. **References** https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Limitation(s) for joint implementation
Resources
Potential to address the following joint goals (ranked):
Assisting each other in improving resilience, improving cybersecurity workforce, common understanding of threat and vulnerabilities, improving response mechanisms and cooperation among a diverse set of stakeholders.

4.9. Crisis response plan

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Detection, Mitigation/Response **Main government resource(s) used to implement this instrument** Organisation/Authority/Information **Main target stakeholders** Own Institutions; Internal Actors **Description of Implementation** US federal agencies have set up coordination and cooperation platforms for responding to cyberattacks. Those can be ad-hoc coordination groups such as the Cyber Unified Coordination Group, which develops during a significant incident. The National Cyber Incident Response Plan (NCIRP) reflects and incorporates lessons learned from exercises, real-world incidents and policy and statutory updates, such as the Presidential Policy Directive/PPD-41: US Cyber Incident Coordination and the National Cybersecurity Protection Act of 2014. **Examples of Implementation** - Through the ESSA Initiative, the Information Sharing Architecture (ISA) developed. - The National Cybersecurity Center within DHS coordinates and integrates information from six centres to provide cross-domain situational awareness, analysing and reporting on the state of US networks and systems, and fostering inter-agency collaboration and coordination. **References** https://us-cert.cisa.gov/ais https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/DOD-DHS-Cyber_Article-2016-09-23-CLEAN.pdf	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority/Information/Organisation **Main target stakeholders** Own Institutions; Internal Actors **Description of Implementation** The setting-up of a crisis response process with guidelines on how to respond and coordinate. **Examples of Implementation** - Blueprint European coordinated response to large-scale cybersecurity incidents and crises was established in 2017 and integrates existing mechanisms into one defining what certain stakeholders do and what responses look like on technical, operational and political/strategic levels. It includes Integrated Political Crisis Response (IPCR), the ARGUS rapid alert system and the EEAS Crisis Response Mechanism for the Common Security and Defence Policy (CSDP). **References** https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience, improving cybersecurity workforce, common understanding of threat and vulnerabilities, improving response mechanisms and cooperation among a diverse set of stakeholders.

4.10. National and international exercises, competitions and training of responses

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Mitigation/Response **Main government resource(s) used to implement this instrument** Organisational/Authority **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** Cybersecurity exercises: competitions may be mandated by Congress or established in response to Executive Order 13870. The President's Cup Cybersecurity Competition is a national cyber competition aiming to identify, recognise and reward the best cybersecurity talent in the federal executive workforce. NCCIC's National Cybersecurity Exercises and Training conducts a full spectrum of exercises in cooperation with the public and private sectors and international partners, particularly those who support US critical infrastructure. It has developed a comprehensive, adaptable and scalable cyber tabletop exercise package (CTEP) as a toolkit for interested organisations. **Examples of Implementation** - Cyber Storm is a national-level cyber-exercise series. Congress mandated Cyber Storm to strengthen cyber-preparedness in the public and private sectors. Participation spans federal, SLTT, international, and public and private sector critical infrastructure stakeholders: the US and Taiwan co-hosted a cybersecurity exercise. - DHS offers voluntary cyber-exercises for Special Event Assessment Rating (SEAR) to non-federal government and non-governmental entities. SEAR events are voluntarily submitted special events, which are sent to the DHS Office of Operations Coordination (OPS) by state, local, and federal officials for a risk assessment. **References** https://www.cisa.gov/cyber-storm-securing-cyber-space https://www.cisa.gov/presidentscup https://www.ait.org.tw/remarks-by-ait-director-w-brent-christensen-at-hacking-for-good-ai-cybersecurity/ https://itlaw.wikia.org/wiki/International_Watch_and_Warning_Network	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Organisation **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** The EU provides training and exercises that would foster resilience and cooperation among the member states and stakeholders within the EU. it is seen as a preventative measure to malicious cyber-activities as it connects important governmental and private stakeholders and equips them with the relevant skills and capabilities to cooperate and handle a crisis situation. Cyber threat assessment capacity and threat information exchange with other EU stakeholders are tested, as is the capacity of the EU institutions and relevant EU agencies (including ENISA, EU-LISA, Europol and CERT-EU) to coordinate and to respond to large-scale cybersecurity incidents and crises at the operational and political/strategic levels. **Examples of Implementation** - Parallel and Coordinated Exercise 2018 (EU HEXML PACE 2018) Double exercise containing a CSDP planning (ML) and an event driven (HEX) crisis management exercise, coordinated with and conducted in parallel with NATO. - Cyber Europe 2020 is an exercise run by ENISA to test EU-level technical and operational cooperation during cyber-crises and to provide opportunities to test local-level incident response and procedures and train EU- and local-level technical capabilities. - Europol, CEPOL, ECTEG124 training programmes – including the Training Governance Model and Training Competency Framework (including certification). - European Judicial Training Network. **References** https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF https://www.enisa.europa.eu/events/5th-ehealth-security-conference/presentations/ENISA_Exercises_Cyber_Europe_2020.pdf https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation

Examples of joint implementation
- US–EU Working Group on Cybersecurity and Cybercrime did a transatlantic cyber-exercise and organised information exchanges on national and regional cyber-exercises. - CyberStorm is conducted with international partners, and member states are represented; information from 2010 includes 12 international partners: Australia, Canada, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Sweden, Switzerland and the UK (up from four countries that participated in Cyber Storm II).
Limitation(s) for joint implementation
Resources
Potential to address the following joint goals (ranked):
Improving response mechanisms and cooperation among a diverse set of stakeholders; improving the cybersecurity workforce.

4.11. Cyber dialogue

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** External Actors **Description of Implementation** Regular, mostly in-person exchanges with other countries on cybersecurity policy that may include discussions on potential cooperation. **Examples of Implementation** - Japan–US Cyber Dialogue - EU–US Cyber Dialogue **References** https://www.mofa.go.jp/press/release/press4e_002646.htmlhttps://translations.state.gov/2020/01/22/the-third-u-s-france-cyber-dialogue/	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Organisation **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** The need for closer engagement with key international partners, as a way to promote 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 US, as well as other consultation venues where cyber issues are among the agenda items. EU cyber dialogues with other countries aim to improve understanding of the national policies of other states with regard to international peace and security, with a view to reducing risks of misperceptions or misunderstanding in the case of malicious cyber incidents that may be considered as originating in or transiting through their territory. **Examples of Implementation** - EU–US dialogue held on 24 May 2019 in Washington, DC. These dialogues could also help to identify possible other preventive or cooperative measures. **References** https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564374 https://eeas.europa.eu/headquarters/headquarters-homepage_me/64495/Joint%20Elements%20Statement%20on%20the%20Sixth%20EU-U.S.%20Cyber%20Dialogue

Examples of joint implementation

- EU-US Cyber Dialogue

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Common understanding of threats and vulnerabilities.

4.12. Cyber capacity building in third countries

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Treasure/Organisation **Main target stakeholders** External Actors **Description of Implementation** Capacity building (or capacity development) is the process by which individuals and organisations obtain, improve and retain the skills, knowledge, tools, equipment and other resources needed to do their jobs competently. **Examples of Implementation** - Digital Connectivity and Cybersecurity Partnership initiative. **References** https://www.usaid.gov/sites/default/files/documents/1861/USAID_DCCP_Fact_Sheet_080719f.pdf	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Treasure/Organisation/Information **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** The importance of external cyber capacity building as a dimension of cyber policy is noted in the 2013 EU Cybersecurity Strategy, which defines it as a strategic building block of its international engagement. The 2015 Council Conclusions on cyber diplomacy also pointed to the need to strengthen cybersecurity and the fight against cybercrime through international cooperation and assistance in the field of cyber capacity building. This position was reaffirmed in the 2017 Joint Communication on resilience, deterrence and defence: building strong cybersecurity for the EU, which acknowledges that efforts to strengthen resilience in third countries contribute to meeting the EU's development commitments and to increasing the level of cybersecurity globally, with positive consequences for the EU. The Joint Communication further defined that a priority for capacity building will be 'the EU's neighbourhood and developing countries experiencing fast growing connectivity and rapid development of threats'. A set of Council Conclusions on EU External Cyber Capacity Building Guidelines were adopted in June 2018, offering political guidance on the scope, principles, priorities and approach for the EU's engagement in this field. **Examples of Implementation** - Many capacity building efforts in SADC have been directed towards strengthening institutions in regard to cybersecurity through training programmes and workshops. The Council of Europe, through the Global Action on Cybercrime (GLACY and its extension GLACY+), has conducted workshops on cybercrime and cyber policy for Mauritius, South Africa, Madagascar, Namibia, Tanzania and Zambia; this has been ongoing since 2013. - Regular report to the Horizontal Working Party on Cyber Issues on external cyber capacity building, and on Member States to share information on their respective efforts. - In specific regions, the Commission has also used other instruments, including the European Neighbourhood Instrument (ENI), to help countries of the Eastern Partnership (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) to define strategic priorities related to the fight against cybercrime. The Instrument of Pre-accession (IPA) finances a new action of €5 million to help countries in South-Eastern

Europe and Turkey to cooperate on cybercrime. The roll-out of more actions in these areas is foreseen in the next years, also through other financing instruments.

References

https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

https://www.iss.europa.eu/sites/default/files/Operational%20Guidance%20for%20the%20EU%E2%80%99s%20international%20cooperation%20on%20cyber%20capacity%20building%20%E2%80%93%20A%20Playbook.pdf

Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case

https://eucyberdirect.eu/content_knowledge_hu/eu-external-cyber-capacity-building-guidelines/

https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf

https://ec.europa.eu/information_society/newsroom/image/document/2017-

Examples of joint implementation

On the ground, e.g. in Georgia and Ukraine. 'The EU–US partnership is perhaps the only one sufficiently advanced to consider triangulated efforts for cyber capacity building in third countries, such as improving access to the internet and preventing cyber threats. Discussions for a coordinated approach have been initiated.' http://www.egmontinstitute.be/content/uploads/2018/01/EPS-EU-cyber-partners_RENARD_AM.pdf?type=pdf

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience, improving cybersecurity workforce.

4.13. Cybersecurity research and development

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Treasure/Authority **Main target stakeholders** Own Institutions, Internal Actors **Description of Implementation** Funding for cybersecurity-related research implemented by federal agencies **Examples of Implementation** - Approximately $4bn/year across 14 agencies, seven programme areas. - Department of Homeland Security's Transition to Practice (TTP) programme aims to help move federally funded cybersecurity technologies into broader use. **References** https://www.nitrd.gov/PUBS/ImplFedCybersecurityRDStrategy-June2014.pdf https://shareng.sandia.gov/news/resources/news_releases/cyber_ttp https://eucyberdirect.eu/content_research/1432/	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Treasure/Authority **Main target stakeholders** Internal Actors, External Actors **Description of Implementation** The EU aims to pool Europe's cybersecurity expertise and prepare the European cybersecurity landscape: hence the European Commission proposal for a European Regulation establishing a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Cybersecurity Coordination Centres in 2021.These projects will assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence. **Examples of Implementation** - The four Horizon 2020 pilot projects will develop a sustainable European cybersecurity competence network. They will implement a variety of tasks such as cybersecurity demonstration cases in eHealth, finance, telecommunications, smart cities, transportation, Cyber Range, trainings or programmes to tackle the cybersecurity skills gab in the EU and deliver innovative marketable solutions made in the EU to tackle future cross-domain cybersecurity challenges. The projects will closely cooperate and coordinate their activities. In addition, they are expected to work together with the European cybersecurity ecosystem in order to advance the way cybersecurity research, innovation and deployment is performed in Europe, and across sectors of our economy. - The mission and objectives of CONCORDIA, ECHO, SPARTA and CyberSec4Europe. - European centre of excellence for countering hybrid threats. - The EU and Japan have funded joint research projects on cybersecurity. **References** https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635518/EPRS_BRI(2019)635518_EN.pdf
Examples of joint implementation	
No joint implementation yet, but interest was voiced in funding a Cyber Policy Research Initiative in 2016.	

Limitation(s) for joint implementation
Resources
Potential to address the following joint goals (ranked):
Assisting each other in improving resilience, improving cybersecurity workforce, common understanding of threat and vulnerabilities.

4.14. Awareness activities

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Information/Nodality/Organisational/Treasure **Main target stakeholders** Internal Actors **Description of Implementation** Conferences, roundtables, campaigns for outreach and awareness that aim to increase the awareness about cybersecurity. **Examples of Implementation** - DHS's STOP THINK CONNECT. - Since 2004, October is designated as National Cybersecurity Awareness Month (NCSAM), a collaborative effort between government and industry that raises nationwide cybersecurity awareness and ensures that all Americans have the resources they need to be safe and secure online. - Learn how to avoid scams, protect your identity, and secure your computer with tips from the Federal Trade Commission's (FTC) OnGuard Online and visit their Protect Kids Online webpage. **References** https://www.stopthinkconnect.org/ https://www.cisa.gov/national-cyber-security-awareness-month	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Information/Organisational/Treasure/Authority **Main target stakeholders** Internal Actors **Description of Implementation** With the adoption of the Safer Internet Programme 2009–2013 by the European Parliament and the Council, the programme started into its third round and was extended for another four years. Since 2014 the programme is carried on via the Connecting Europe Facility (CEF). An awareness campaigns aims to edcuate a target audience about cybersecurity-related information. **Examples of Implementation** - ENISA, the European Commission DG CONNECT and Partners are deploying the European Cyber Security Month (ECSM) every October. - Co-funding of Klicksafe as part of the CEF Telecom Programme **References** https://www.klicksafe.de/ueber-klicksafe/die-initiative/project-information-en/

Examples of joint implementation

Jointly promoted National Cyber Awareness Month in the US and Europe.

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience, common understanding of threats and vulnerabilities, improving cybersecurity workforce, improving response mechanisms and cooperation among a diverse set of stakeholders.

4.15. Technical response teams

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, detect and react **Main government resource(s) used to implement this instrument** Authority/Organisational **Main target stakeholders** Own Institutions, Internal Actors **Description of Implementation** The Department of Homeland Security Cyber Hunt and Incident Response Teams Act of 2019 (bipartisan legislation) directs the DHS to maintain permanent 'cyber hunt and incident response teams' to assist both government and private entities in their efforts at prevention and, when necessary, to respond appropriately to cyberattacks. A computer security incident response team (CSIRT) is a concrete organisational entity (i.e. one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. Moreover, there is a requirement for federal departments to maintain computer incident response capabilities. Per PPD-41, each federal agency that regularly participates in the Cyber Response Group (CRG), including SSAs, ensures that it has the standing capacity to execute its role in cyber-incident response. **Examples of Implementation** - US-CERT. - Treasury Computer Security Incident Response Capability (TCSIRC): provides incident reporting with external reporting entities and conducts performance monitoring and analyses of CSIRCs within the Department **References** https://www.congress.gov/bill/116th-congress/senate-bill/315/text https://www.us-cert.gov/ https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf https://fas.org/irp/agency/dhs/nrp.pdf https://www.treasury.gov/about/organizational-structure/offices/Pages/-Cyber-Security.aspx	**Main goal(s) of the policy instrument** Prevention, detect and react **Main government resource(s) used to implement this instrument** Organisation/Authority/Information **Main target stakeholders** Own Institutions, Internal Actors **Description of Implementation** In the Digital Agenda for Europe adopted in May 2010 (see IP/10/581 and MEMO/10/200), the Commission committed itself to establishing a CERT for the EU institutions, as part of the EU's commitment to a reinforced and high-level EU Networking and Information Security Policy in Europe. After a pilot phase of one year and a successful assessment by its constituency and its peers, the EU institutions decided to set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies on 11 September 2012. The Digital Agenda also calls on all member states to establish their own CERTs, paving the way to an EU-wide network of national and governmental CERTs by 2012 (see IP/11/395). The EU's Council of Telecoms Ministers adopted conclusions on 27 May 2011 confirming this objective. Cyber Rapid Response Teams (CRRTs) were established by PESCO and are led and supported by seven member states on a voluntary basis. **Examples of Implementation** - The CRRTs established as part of the PESCO framework could be used to assist other member states, EU institutions, CSDP operations and partners. CRRTs will be equipped with commonly developed deployable cyber toolkits designed for detecting, recognising and mitigating cyber threats. Teams would be able to assist with training, vulnerability assessments and other requested support. CRRTs would operate by pooling participating Member States experts. - CERT-EU - The CERT for the EU institutions, bodies and agencies. The team is made up of IT security experts from the main EU institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the member states and beyond as well as with specialised IT security companies in order to respond to information security incidents and cyber threats. - CSIRTs by country: an interactive map by ENISA show how EU member states have implemented the suggestion of having a CERT. **References**

https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

https://www.easa.europa.eu/faq/24266
https://cert.europa.eu/cert/plainedition/en/cert_about.html CSIRTs by Country - Interactive Map

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience, common understanding of threats and vulnerabilities.

4.16. Early warning/public vulnerability or (attributed) threat alerts

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, detect and react **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** Internal Actors; External Actors **Description of Implementation** Alerts provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks. Alerts can also have a signalling function if used as a tool to publicly attribute activities to state or non-state actors. **Examples of Implementation** - An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks. - NSA cybersecurity advisory: Patch remote desktop services on legacy versions of Windows - Joint US–UK technical alert on malicious cyber-activity carried out by Russian government. **References** https://us-cert.cisa.gov/ics/alerts_CISA https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/ https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf	**Main goal(s) of the policy instrument** Prevention, detect and react **Main government resource(s) used to implement this instrument** Information **Main target stakeholders** Internal Actors **Description of Implementation** Alert (reactive): This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus or hoax and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT community and disseminated by ENISA, or may be redistributed from vendors, other CERTs or security experts or other parts of the constituency. Resources are solely informational. Announcements (proactive): This includes, but is not limited to, intrusion alerts, vulnerability warnings and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited. **Examples of Implementation** - ENISA published an alert with assessment of WannaCry Ransomware Outburst. **References** https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst
Limitation(s) for joint implementation	
Resources	
Potential to address the following joint goals (ranked):	
Common understanding of threats and vulnerabilities, improving response mechanisms and cooperation among a diverse set of stakeholders, Assisting each other in improving resilience.	

4.17. Accountability and evaluation of instruments

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Authority/Organisation **Main target stakeholders** Own Institutions **Description of Implementation** Assessment of the implementation progress of cybersecurity measures that were demanded by legislations and may result in recommendations for improvement. The 2019 Defense Authorization Act established the US Cyberspace Solarium Commission, which had to weigh the costs and benefits and evaluate the means for executing various strategic options, including for the political system, the national security industrial sector and the innovation base. Options to be assessed include deterrence, norms-based regimes and active disruption of adversary attacks through persistent engagement. Evaluate the effectiveness of the current national cyber policy and consider possible structures and authorities that need to be established, revised or augmented within the federal government. A final report with the Commission's findings is due September 1, 2019. **Examples of Implementation** - The US Cyberspace Solarium Commission report was published in March 2020. - the Office of Management and Budget (OMB develops and oversees the implementation of policies, principles, standards and guidelines on information security. This includes coordinating the development of standards and guidelines under the National Institute of Standards Technology Act and enforcing their adoption in federal agencies. - FISMA includes a provision for the Government Accountability Office (GAO) to periodically report to Congress on agencies' implementation of the act. GAO's objectives in this report were to (1) describe the reported adequacy and effectiveness of selected federal agencies' information security policies and practices and (2) evaluate the extent to which the OMB, DHS and NIST have implemented their government-wide FISMA requirements. - GAO categorised information security deficiencies as reported by 16 randomly selected agencies and their I inspectors general according to the elements of an information security programme; evaluated IG reports for 24 Chief Financial Officers (CFO) Act agencies; examined OMB, DHS and NIST documents; and interviewed agency officials.	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Authority/Organisation **Main target stakeholders** Own Institutions **Description of Implementation** As part of its better regulation agenda, the Commission continuously evaluates whether EU laws have met the needs of citizens and business, at minimum cost. The REFIT programme in particular, as well as tools such as evaluations and fitness checks, helps make existing EU laws simpler and less costly to apply. On 19 February 2020, the new European Commission published a Communication on shaping Europe's digital future. The white paper included that the Security of Network and Information Systems (NIS) Directive will be reviewed in Q4 of 2020. **Examples of Implementation** - Commission's Forward Planning of Evaluations and Studies 2017 and beyond. This document provides an overview of evaluations (including fitness checks) and studies as identified by the Commission Services in their 2017 Management Plans, which are part of the Commission's Strategic Planning and Programming cycle. The evaluation planning takes the form of a five-year indicative rolling programme, with evaluations in the first two years being broadly fixed while planning for the later years is more indicative. - 2017 Assessment of the 2013 Cybersecurity Strategy. - 2020 evaluation of NIS Directive. - Evaluation of research projects; for example, The Transport and Research and Innovation Monitoring and Information System (TRIMIS) supports the implementation and monitoring of the Strategic Transport Research and Innovation Agenda (STRIA) and its seven roadmaps by the Joint Research Centre on behalf of the European Commission. - Article 32 (1) of Regulation EU n. 526/2013 requires the Commission to 'commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency and its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification.' **References** https://ec.europa.eu/info/sites/info/files/20170504-studies-and-evaluations-2017-planning_en.pdf https://ec.europa.eu/info/law/law-making-process/evaluating-and-improving-existing-

References

https://us-cert.cisa.gov/ics/alerts CISA
https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government

https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices
CSC Final Report.pdf

https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

https://www.gao.gov/assets/710/700588.pdf

laws/evaluating-laws/planned-evaluations_en

https://trimis.ec.europa.eu/sites/default/files/documents/trimis_digest_issue_3_april_2018_4.pdf

https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience

4.18. Specific topical (cooperation) working groups

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority/Organisation **Main target stakeholders** External Actors, Internal Actors **Description of Implementation** Establishment of working groups on cybersecurity (policy) related topics with other countries. **Examples of Implementation** - the US–Japan Cyber Defense Policy Working Group (CDPWG) was established in October 2013. - ASEAN Defence Ministers Meeting-Plus (ADMM-Plus) Experts' Working Group on Cyber Security - NTIA Working Group on Software Transparency. - Cyber Solarium Commission, a bipartisan group created by the 2019 National Defense Authorization Act and chaired by Sen. Angus King (I-ME) and Rep. Mike Gallagher (R-WI), was tasked with creating a strategy for defending the US against cyberattacks and making recommendations for policies and legislation necessary to implement that strategy. **References** https://nsarchive.gwu.edu/news/cyber-vault/2019-05-15/cyber-brief-us-japan-agreement https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation https://www.lawfareblog.com/cyberspace-solarium-commission-makes-its-case-congress	**Main goal(s) of the policy instrument** Prevention, Mitigation/Response **Main government resource(s) used to implement this instrument** Authority **Main target stakeholders** Internal Actors, External Actors **Description of Implementation** Establishment of working groups on cybersecurity (policy) related topics. **Examples of Implementation** - US–EU Working Group on Cybersecurity and Cybercrime - NIS Cooperation working group **References** https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation http://www.egmontinstitute.be/content/uploads/2018/01/EPS-EU-cyber-partners_RENARD_AM.pdf?type=pdf

Examples of joint implementation

- The US–EU Working Group on Cybersecurity and Cybercrime that was established in the context of the 2010 Lisbon US–EU Summit serves as a framework for US–EU collaboration to enhance cybersecurity and cybercrime activities and contribute to countering global cybersecurity threats. The Working Group focuses on four areas where cooperative approaches add significant value to both regions: cyber-incident management, public–private partnership on critical infrastructure cybersecurity, cybersecurity awareness raising, and cybercrime. It identifies clear priority areas for cooperation, as well as concrete deliverables, following a specific roadmap.
- The EU and the US are establishing an Executive Working Group (EWG) to consider, inter alia, regulatory initiatives to reduce unnecessary administrative obstacles and costs, while at least preserving the levels of protection of each side.

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience, improving response mechanisms and cooperation among a diverse set of stakeholders, common understanding of threats and vulnerabilities, improve cybersecurity workforce.

4.19. Multi-stakeholder consultations

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Prevention **Main government resource(s) used to implement this instrument** Organisation/Information **Main target stakeholders** Internal Actors, External Actors **Description of Implementation** Establishment of multi-stakeholder consultations to draw in information from different sectors and perspectives. Since 2015, the National Telecommunications and Information Administration has sought public comment on several matters around cybersecurity. Many stakeholders emphasised the importance of community-led, consensus-driven and risk-based solutions to address cybersecurity challenges, highlighting the role NTIA should play in convening multi-stakeholder processes. **Examples of Implementation** - NTIA has convened two multi-stakeholder processes to address these challenges, one on vulnerability disclosure and another on IoT security updates. - NTIA's cybersecurity multi-stakeholder process focused on Software Component Transparency, not limited to US citizens. **References** https://www.ntia.doc.gov/SoftwareTransparency https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency	**Main goal(s) of the policy instrument** Prevention **Main government resource(s) used to implement this instrument** Organisation/Information/Treasure **Main target stakeholders** Internal Actors **Description of Implementation** Establishment of multi-stakeholder consultations to draw in information from different sectors, perspectives that can be online or in person. Supporting multi-stakeholder participation in consultation processes financially. The results of public consultation feed into the ex-post European Commission evaluation and can serve as input to prepare the ground for a possible revision of the mandate or legislation. **Examples of Implementation** - In order to strengthen the multi-stakeholder engagement at the first intersessional consultative meeting of the Open-ended Working Group, the EU established the Engagement Support Programme (ESP). - 2017 Public consultation on the evaluation and review of ENISA. **References** https://eucyberdirect.eu/content_events/oewg2019/df https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-european-union-agency-network-and-information

Examples of joint implementation

EU–US: Call for proposals for regulatory cooperation activities to inform the Executive Working Group (EWG) to consider how to reduce unnecessary administrative obstacles and costs, while at least preserving the level of protection of each side in terms of cybersecurity.
EU Stakeholder Consultation: Synopsis Report EU-US: Call for proposals for regulatory cooperation activities http://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158068.pdf

Limitation(s) for joint implementation

Resources

Potential to address the following joint goals (ranked):

Assisting each other in improving resilience, improving response mechanisms and cooperation among a diverse set of stakeholders, common understanding of threats and vulnerabilities, improve cybersecurity workforce.

4.20. Personnel exchanges, e.g. cyber liaison officer

US (federal government)	EU (EU institutions)
Main goal(s) of the policy instrument Mitigation/Response **Main government resource(s) used to implement this instrument** Authority, Organisation **Main target stakeholders** External Actors, Internal Actors **Description of Implementation** Generally a liaison officer is a person who is employed to form a working relationship between two organisations to their mutual benefit. An example is the Memorandum of Understanding (MOU) between the Department of Defense (DoD) and the Department of Homeland Security (DHS), which sets forth the terms and conditions under which liaisons are exchanged between the two departments on a non-reimbursable basis. **Examples of Implementation** - The Joint Cybercrime Action Taskforce (J-CAT), hosted by Europol's EC3, brought together cyber liaison officers from various EU member states and non-EU law enforcement partners from Australia, Canada, Colombia and the US (which is represented by a liaison officer from the FBI and the US Secret Service). At the international level, EC3's J-CAT provides a focal point that allows the various liaison officers to exchange strategic information quickly, facilitates cross-border cooperation and serves as an information hub on any given action day. - CyberCommand provides liaison officers to key interagency partners to provide information exchange, e.g. at DHS. - US Coast Guard Cyber Command provides a liaison officer to DHS NCCIC. **References** https://www.jcs.mil/Portals/36/Documents/Doctrine/Interorganizational_Documents/doj_mou_liaisons_cap_region2013.pdf http://onlinepubs.trb.org/onlinepubs/conferences/2012/hscamsc/presentations/6b-rouzer.pdf	**Main goal(s) of the policy instrument** Mitigation/Response **Main government resource(s) used to implement this instrument** Authority, Organisation **Main target stakeholders** Internal Actors, External Actors **Description of Implementation** Generally a liaison officer is a person who is employed to form a working relationship between two organisations to their mutual benefit. When used in cybercrime, 'liaison officer' means a representative of one of the member states posted abroad by a law enforcement agency to one or more third countries or to international organisations to establish and maintain contacts with the authorities in those countries or organisations with a view to preventing crime or investigating criminals. Internally, ENISA created in 2004 a network of liaison officers from all member states to exchange information between ENISA and the member states, and support ENISA in disseminating its activities, findings and recommendations to the relevant stakeholders across the EU. **Examples of Implementation** - The Joint Cybercrime Action Taskforce (J-CAT), hosted by Europol's EC3, brought together cyber liaison officers from various EU member States and non-EU law enforcement partners from Australia, Canada, Columbia and the US (which is represented by a liaison officer from the FBI and the United States Secret Service). At the international level, EC3's J-CAT provides a focal point that allows the various liaison officers to exchange strategic information quickly, facilitates cross-border cooperation and serves as an information hub on any given action day. Within the MLAT context, the J-CAT works as a coordinating hub to exchange strategic information and provides a face-to-face platform to discuss and facilitate MLAT requests. - The National Liaison Officers Network facilitates the exchange of information between ENISA and the Member States, and supports ENISA in disseminating its activities, findings and recommendations to the relevant stakeholders across the Union. The Network is composed of representatives of all member states and will be set up by the Management Board in the course of 2019. ENISA is in the process of implementing a new regulatory framework. **References** https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf NLO Network

https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/nlo-network/

Examples of joint implementation
EC3 has an embedded liaison officer from the FBI who is stationed in the headquarters on a full-time basis.
Limitation(s) for joint implementation
Resources
Potential to address the following joint goals (ranked):
Improving response mechanisms and cooperation among a diverse set of stakeholders, common understanding of threats and vulnerabilities.

About the author

Julia Schuetze works on cyber diplomacy of the European Union with the United States and Japan as part of the EU Cyber Direct project. She alsoworks as project manager of the "Transatlantic Cyber Forum" which deals with internationalcyber security policy. Her research focus is on cyber operations against electoral processes, comparative cybersecurity policy and governance. As part of her role at SNV she has spoken at the Congressional Cybersecurity Caucus in the United States, has facilitated workshops on Germany's cybersecurity architecture with the foreign office, has organized the cybersecurity conference with the Bundesakademie für Sicherheitspolitik as well as several other workshops and events with U.S. and German cybersecurity experts in Washington D.C. and Berlin. Her work has been published or cited by news outlets, such as WirtschaftsWoche Der Tagesspiegel, F.A.Z and the BBC. She is a Cybersecurity Policy Fellow at New America Foundation and volunteers for the OGP Civil Society Working Group and for the Steering Committee of the Internet Governance Forum Germany.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.