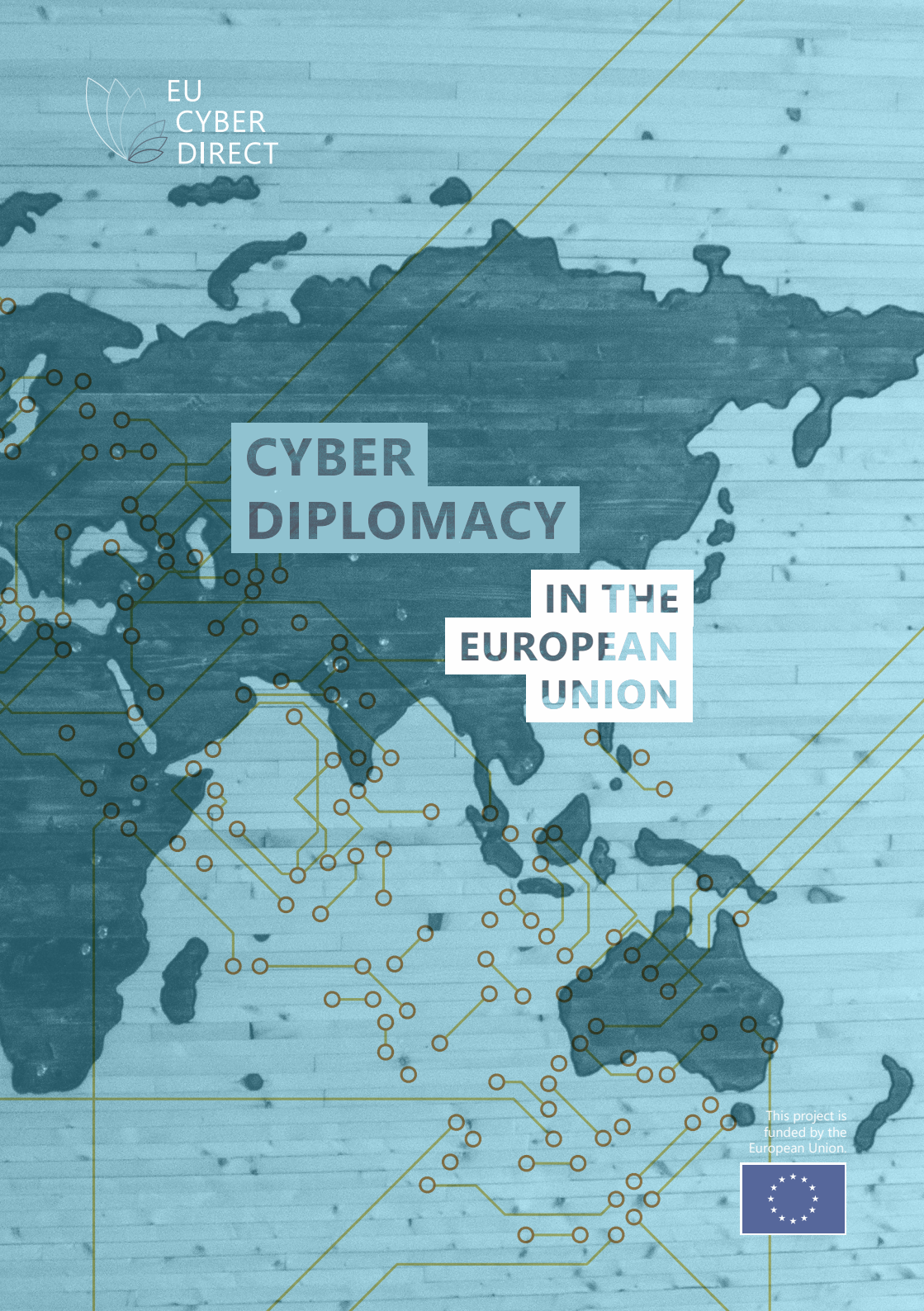
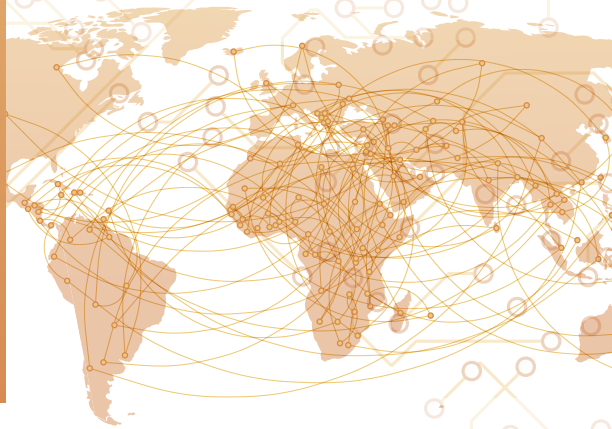

EU
CYBER
DIRECT
CYBER
DIPLOMACY
IN THE
EUROPEAN
UNION
This project is
funded by the
European Union.

WHAT IS CYBER DIPLOMACY?

The use of the internet to access information, communicate with people across the world, or deliver public services is often taken for granted. However, with the growing importance of cyberspace for pursuing their interests, governments are increasingly interested in ways in which citizens access and use different components of cyberspace.



Cyber diplomacy – a set of diplomatic practices concerned with the broadly defined governance of cyberspace – is a new dimension in international relations. Ministries of foreign affairs are usually the main actors responsible for pursuing a cyber diplomatic agenda in close cooperation with other parts of government, and in some cases under the guidance of a coordinator or ambassador serving as a cyber-diplomat-in-chief.

Cyber diplomacy is the main avenue for preserving and defending the open, free, secure, stable, and peaceful nature of cyberspace. Most of the time, this objective is pursued through international dialogue and cooperation with partner countries and organisations. However, protecting a rules-based international order means that sometimes it is necessary to impose consequences on state and non-state actors who violate existing international law or breach agreed-upon norms of responsible behaviour.

The EU's **strength** results from its clear commitment to adequate levels of cybersecurity as a precondition for economic and social growth, in line with the Sustainable Development Goals.

The EU's **legitimacy** stems from its adherence to the highest standards domestically as well as engagement with a wide range of actors, including governments, businesses, and citizens around the world. Ultimately, the key objective of the EU's cyber diplomacy is to provide a **secure and trusted digital environment** in which citizens are free to pursue their ambitions.

Access to and use of an open and secure cyberspace enables economic growth and innovation, accelerates progress and drives political, social, and economic development globally.

Free – Citizen's human rights and fundamental freedoms are protected both online and offline

Open – Citizens enjoy universal, affordable and equal access to the internet

Secure – Citizens can access and use cyberspace in a safe and trusted way

Peaceful – Citizens benefit from a stable digital environment in which all actors behave responsibly

The EU's cyber diplomacy is focused on ensuring that governments, the private sector, civil society organisations, and end users around the globe understand the impact of an open, free, and secure cyberspace on their lives and that they are capable of taking actions to protect it.

The EU's cyber diplomacy aims to...

- strengthen **resilience**
- build **trust**
- prevent **conflicts**
- protect **human rights and freedoms**
- promote **multilateralism**

It does so through...

- **cyber dialogues** with specific partner countries
- **capacity building** and **technical assistance**
- **engagement** with civil society and the private sector
- **outreach** and **awareness campaigns**
- **diplomatic démarches, statements,** and **declarations**
- **restrictive measures** or other forms of restraint, coercion, or signalling

DIGITAL RISKS AND THE EU'S RESPONSES

With its potential to galvanise growth and increase prosperity, the digital economy is now high on the global agenda. Internet-enabled platforms, data-driven innovation, and digital applications are changing how all sectors work, whether transportation, health, education, or agriculture. But these benefits are not always enjoyed equally around the world, not least due to the digital divide but also cybercrime or malicious activities undertaken in cyberspace by state and non-state actors.

ELECTION PROCESS

In 2015 and 2016, computer hackers infiltrated the Democratic National Committee (DNC) computer network, leading to a data breach.

PORT SECURITY

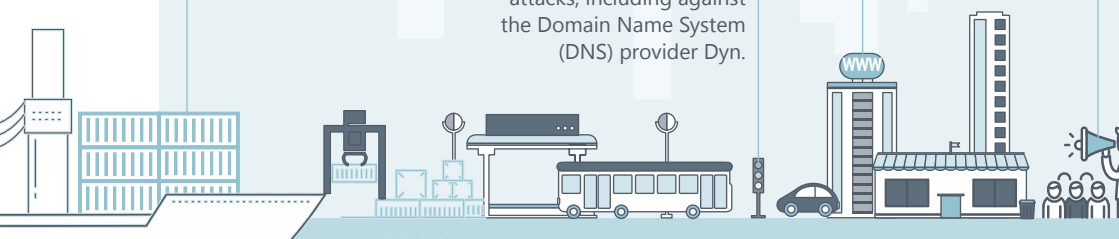
In 2017, NotPetya ransomware attacks against Maersk, the world's largest cargo shipping company. The attacks cost the company over $300 million in damages, and the company had to reinstall 4,000 servers, 45,000 PCs, and 2,500 applications.

DATA BREACHES

In 2016, Yahoo! announced it had suffered a cyberattack that affected 3 billion user accounts.

INTERNET OF THINGS

In 2016, the Mirai botnet was used in the largest and most disruptive distributed denial of service (DDoS) attacks, including against the Domain Name System (DNS) provider Dyn.



SATELLITE INFRASTRUCTURE

A hacking group gained electronic access to two U.S. government satellites in 2007 and 2008.

TRANSPORTATION INFRASTRUCTURE

A 2018 cyberattack on Atlanta Airport caused cancellation of flights, passenger delays, and overall airport disruption, costing the city millions of dollars.

ESPIONAGE

In 2019, it was reported that a coordinated cyberespionage campaign had targeted UN relief agencies, the International Red Cross, and other non-governmental organisations.

In order to mitigate the risks, the EU has adopted specific **policy and regulatory frameworks**, **strategic documents**, and institutional solutions aimed at enhancing cooperation between the member states and between the EU and partner countries.

- Digital Single Market Strategy for Europe — 2015
- European Agenda on Security
- Internet governance
- Cyber diplomacy
- Cyber resilience — 2016
- NIS Directive
- Mainstreaming digital solutions in EU development policies
- EU–NATO joint declaration
- Communication on resilience, deterrence, defence — 2017
- Cyber diplomacy toolbox
- Resilience in the EU's external actions
- Blueprint for coordinated response
- External capacity building
- Malicious activities in cyberspace — 2018
- General Data Protection Regulation (GDPR)
- EU Cybersecurity Act — 2019
- Cyber sanctions regime

STRENGTHENING RESILIENCE

Cybersecurity is a shared responsibility. The EU takes concrete steps to ensure that all stakeholders – both across the EU and globally – are adequately equipped to enjoy full benefits of digital society without unnecessary risks.

The EU sets good practices for strengthening cyber resilience and shares lessons with the rest of the international community. It builds its domestic resilience by setting standards, promoting cooperation among stakeholders, and building a culture of cybersecurity across all sectors.

EU Cybersecurity Act

The EU Cybersecurity Act revamps and strengthens the EU Agency for Cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services, and processes.

The EU's cybersecurity architecture

NIS Directive

The Security of Network and Information Systems Directive provides legal and institutional measures to boost the overall level of cybersecurity and preparedness in the EU.

It creates a **culture of security** across vital sectors of the economy and society (energy, transport, water, banking, healthcare, financial markets, digital infrastructure);

It increases **national cybersecurity capabilities** by requiring all member states to have a national cybersecurity strategy, national Computer Emergency Response Team, NIS national competent authorities, and a Single Point of Contact;

It enhances EU-level **cooperation and information sharing** through establishing the CSIRT Network (a network composed of EU member states' appointed CSIRTs and CERT-EU) and the NIS Cooperation Group (a platform for EU member states, the European Commission and the EU Agency for Cybersecurity).

Crisis response

The **EU Blueprint for Coordinated Response** to large-scale cyber incidents and crises sets out the objectives and modes of cooperation between the member states and EU Institutions in responding to such events. It explains how existing crisis management mechanisms can make full use of existing cybersecurity entities at the EU level.

Capacity building

The EU promotes sustainable digital development in partner countries. It implements projects aimed at **capacity building** for cyber resilience and the fight against cybercrime. The EU is one of the world's biggest donors in cyber capacity building projects focused on developing national cybersecurity strategies, establishing CERTs, and fighting cybercrime – all while respecting human rights and fundamental freedoms.

Research and innovation

In order to better prepare for future challenges and improve policymaking, the EU invests in cybersecurity research, innovation and deployment. In 2018, building on the Cybersecurity Act, the European Commission proposed the creation of a **Network of Cybersecurity Competence Centres** and a **new European Cybersecurity Industrial, Technology and Research Competence Centre** to invest in a stronger and more pioneering cybersecurity capacity in the EU.

BUILDING TRUST

Trust in the digital environment is the foundation on which competitive, prosperous, free and open, modern societies are built. This is why the European Union aims to improve online security, trust and inclusion.

Fighting cybercrime

The EU is constantly adapting its capacity to fend off attacks on information systems, combat the sexual exploitation of children online and child pornography, prevent fraud and counterfeiting, and facilitate cross-border access to electronic evidence.

To facilitate cooperation between law enforcement and judicial authorities, the EU is modernising its rules for obtaining the **electronic evidence** needed to investigate and eventually prosecute criminals and terrorists (e.g. **European Production Order, European Preservation Order**).

The **European Cybercrime Centre (EC3)** at Europol works to strengthen the law enforcement cooperation against cybercrime across the EU. The **European Judicial Cybercrime Network**, supported by Eurojust, facilitates cooperation between the competent judicial authorities.

The **Data Protection Police Directive** protects individuals when their personal data are processed by authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or for the execution of criminal penalties.

Protection of personal data and privacy online

Europeans have set high standards for data protection that ensure digital privacy for citizens and provide better cybersecurity. The EU promotes robust data protection rules globally and is prepared to share lessons and good practices that may inform similar legislative efforts around the world.

- **General Data Protection Regulation (GDPR)** provides new rules to give citizens more control over their personal data.
- **ePrivacy Directive** ensures the confidentiality of communications and defines rules regarding online tracking and monitoring.
- **eIDAS Regulation** introduces safe ways for individuals and companies to perform transactions online.

Standards and certification frameworks

The **EU Cybersecurity Act** revamps and strengthens the EU Agency for Cybersecurity (ENISA) and establishes an EU-wide **cybersecurity certification framework** for digital products, services and processes, including:

- a common European approach to cybersecurity certification;
- a modern, dynamic, and risk-based certification scheme with an emphasis on the use of globally relevant international standards;
- an open, inclusive, and transparent governance framework.

International cooperation

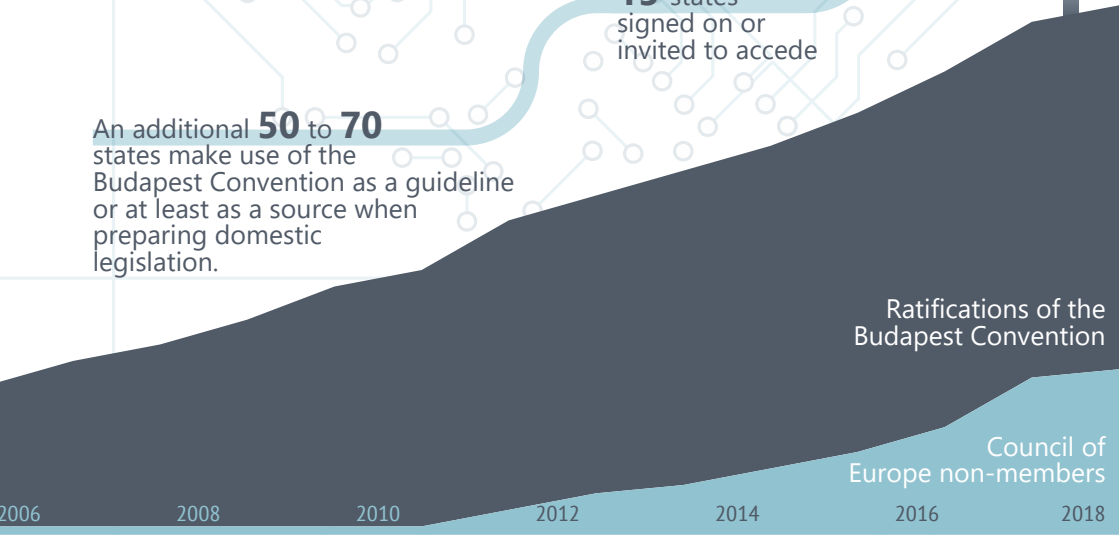
Given the transnational nature of cybercrime, the EU supports and promotes the **Budapest Convention on Cybercrime**, the only regional document with a global reach. The Convention provides technology-neutral definitions, lays out procedures for international cooperation against cybercrime, and sets out rule-of-law safeguards. Through various projects and initiatives, the Council of Europe also provides concrete support for legislative or institutional reforms in line with the Budapest Convention.

At least **two-thirds** of all states worldwide already make use of the Budapest Convention.

An additional **50** to **70** states make use of the Budapest Convention as a guideline or at least as a source when preparing domestic legislation.

15 states signed on or invited to accede

64 parties



EU CYBER DIPLOMACY IN ACTION

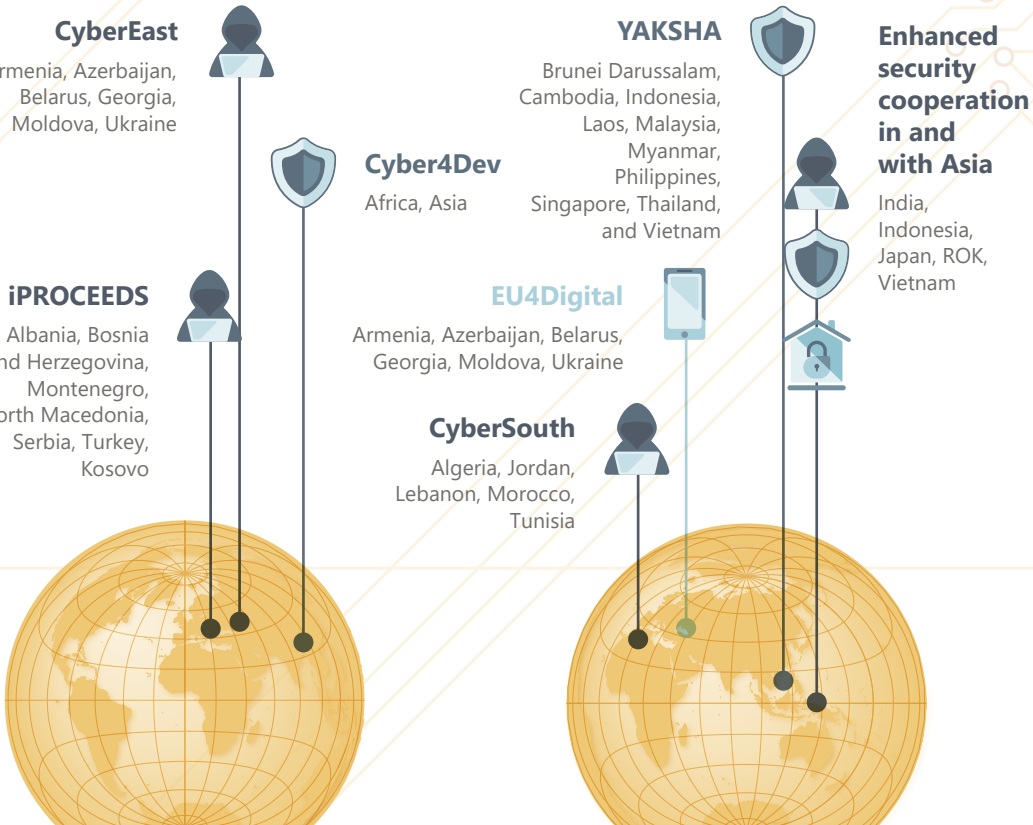
Diplomacy is not only words. The EU takes concrete actions and implements projects to support the efforts of partner countries and international organisations, while promoting its own values and interests.

CRIME

The EU supports states in strengthening their legal and institutional capacities to fight cybercrime including by enhancing their abilities for effective international cooperation.

PEACE AND STABILITY

The EU engages with stakeholders around the world to provide policy support and promote better understanding of EU policies.



SECURITY

The EU works with partner countries to increase the resilience of their critical information infrastructure and networks through comprehensive policies, organisations and technical measures.

RIGHTS

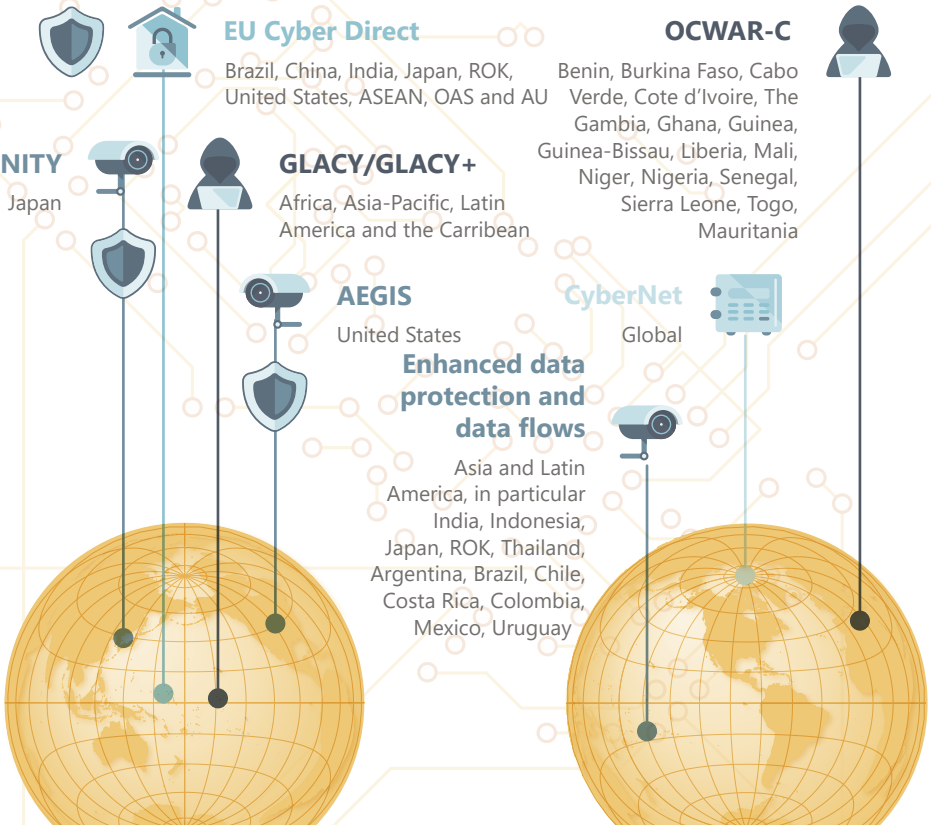
The EU works to build awareness about importance of the right to privacy and promotes greater regulatory convergence on data protection.

DIGITAL

The EU strengthens cooperation on digital policies, including telecom rules, trust and security of e-government, eTrade, eHealth, ICT innovation and digital skills.

HUMAN CAPACITIES

The EU takes steps to strengthen global delivery, coordination and coherence of the EU's external cyber projects.



PREVENTING CONFLICTS

Malicious activities in cyberspace undermine the rules-based international order, raise the risk of conflict, and consequently pose a risk to citizens' safety and well-being. For this reason, the EU's cyber diplomacy is committed to settling international disputes by peaceful means.

To prevent the adverse effects of malicious activities in cyberspace, the EU advances an inclusive strategic framework for conflict prevention through bilateral, regional, and multi-stakeholder engagement.

The EU works to **strengthen global cyber resilience**. Global cyber resilience reduces the ability of potential perpetrators to misuse technology for malicious purposes and strengthens the ability of states and societies to effectively respond and recover from cyber threats.

The EU works with partner countries and organisations to build **individual and/or joint capacities** to prevent, detect, deter, and respond to malicious cyber activities.

The EU promotes **responsible behaviour in cyberspace**:

- It strongly advocates that existing international law applies in cyberspace and emphasises that respect for international law, in particular for the UN Charter, is essential for maintaining international peace and security.
- It acknowledges that compliance with voluntary, non-binding norms of responsible behaviour in cyberspace contributes to an open, secure, stable, accessible, and peaceful cyberspace.

The **EU's cyber sanctions regime** in a nutshell:

Established on 17 May 2019;

Adopted to deter and respond to cyberattacks constituting an external threat to the EU or its member tates;

Allows the EU for the first time to impose sanctions on persons or entities responsible for cyberattacks or attempted cyberattacks, or who provide financial, technical, or material support for such attacks or who are involved in other ways;

Concrete measures include a ban on persons travelling to the EU and an asset freeze on persons and entities. EU persons and entities are forbidden from making funds available to those listed.

The EU **builds trust to reduce the risk of misperception**, escalation, and conflict. It has actively supported the development of **confidence-building measures** adopted by the OSCE as well as similar processes in Latin America and the Asia Pacific.

The **Cyber Diplomacy Toolbox** is at the core of the EU's joint diplomatic response to malicious cyber activities. Its focus is on preventing conflicts, mitigating cybersecurity threats, and contributing to greater stability in cyberspace through five sets of measures.

Stability measures

> Political statements: declarations by the HRVP on behalf of the EU, HRVP statements, spokesperson statements, local EU statements
> EU Council conclusions
> Diplomatic demarches
> Political and thematic dialogues

EU support to member states

> Solidarity Clause (Art. 222 TFEU)
> Mutual Defence Clause (Art. 42.7 TEU)

Cooperative measures

> EU démarches
> Technical assistance
> Political and thematic dialogues

Preventive measures

> Confidence-building measures
> Public diplomacy and awareness campaigns
> External cyber capacity building

Restrictive measures

> Targeted sanctions against individuals and entities

PROTECTING HUMAN RIGHTS

The EU's international engagement in cyber issues is guided by its core values of human dignity, freedom, democracy, equality, the rule of law, and respect for fundamental rights. Cybersecurity can only be sound and effective if it is based on a respect of fundamental rights and freedoms.

Supporting human rights defenders around the world

Support for **human rights defenders** (HRDs) is an integral part of the European Union's external policy on human rights. HRDs represent natural and indispensable allies in the promotion of human rights and democratisation in their respective countries. Through the **European Instrument for Democracy and Human Rights** (EIDHR), the EU provides small grants on an ad-hoc basis and supports projects designed to protect HRDs, individuals, and organisations.

Free and fair democratic processes

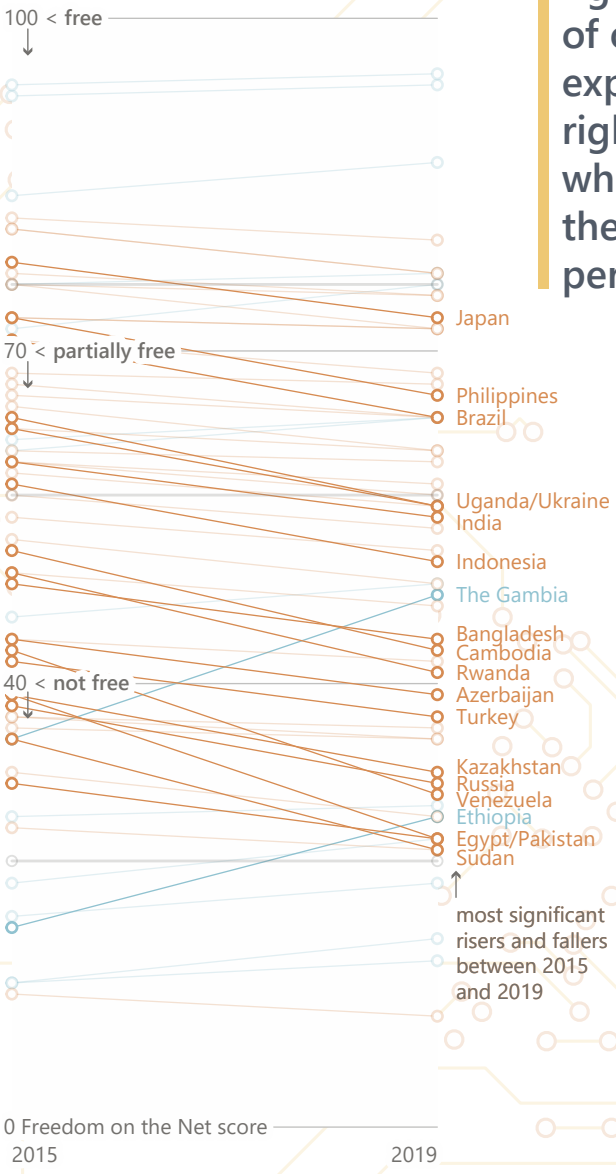
Exercising the right to vote in a well-informed and safe manner is one of the foundations of democratic societies. The instances of disinformation and malicious cyber activities around the world have reinforced the EU's focus on protecting **democratic processes and institutions** from manipulation and interference.

Preventing the misuse of new technologies

The EU is committed to strengthening **controls on exports** of certain goods and technologies that may be used for human rights violations, terrorist acts, or the development of weapons of mass destruction. For instance, the EU's export controls aim to prevent human rights violations associated with certain cyber surveillance technologies.

> “All human rights that exist offline must also be protected online, in particular the right to freedom of opinion and expression and the right to privacy which also includes the protection of personal data.

EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014)



47 countries (out of 65) experienced a deterioration in internet freedom between 2015 and 2019.

Freedom House (2019)

PROMOTING MULTILATERALISM

The EU's interest lies in a multilateral system that is rules and rights-based, which protects the global commons, promotes shared public goods, and delivers benefits for citizens in Europe and across the globe.

Cooperation through an effective multilateral system – one that delivers results in tackling today's and tomorrow's global challenges – remains the best way to advance national and collective interests.

To strengthen the multilateral system, the EU has three main areas of focus:

- **upholding international norms and agreements** and respect for existing international law and norms of responsible behaviour in cyberspace;
- **extending multilateralism to new global realities**, including cooperation and coordination with regional partners, such as ASEAN, the OAS, the AU, the OSCE, and NATO;
- **making multilateral organisations fit for purpose** through bilateral cyber dialogues with other regional bodies and international organisations and by shaping global debates on the future of cyberspace, in particular at the UN.

Multilateral cooperation and multi-stakeholder partnerships are at the core of the EU's global engagement on cyber issues.

- **WePROTECT Global Alliance** - an international movement dedicated to national and global action to end the sexual exploitation of children online as part of the UN Sustainable Development Goals.
- **Freedom Online Coalition** - a group of over 30 governments committed to work together to support Internet freedom and protect fundamental human rights worldwide.
- **Global Forum on Cyber Expertise** - a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building.
- **Global Internet Policy Observatory (GIPO)** is an online platform for crowd-sourcing knowledge and expertise to develop a tool helping users understand and monitor Internet-policy regulatory and technological developments around the world.

The EU's multilateral and multistakeholder engagement takes many shapes and forms.

Global level

UN system

UNGA Main Committees

- Disarmament & International Cooperation
  - Group of Governmental Experts (GGE)
  - Open-ended Working Group (OEWG)
- Economic & Financial
- Social, Humanitarian & Cultural

Agencies and bodies

- ITU
- Human Rights Council
- UNDP
- UNODC
- IGF and IGF regional and national initiatives

Specialised platforms

- Global Forum on Cyber Expertise
- Meridian
- Interpol

Multistakeholder initiatives

- The Paris Call
- Global Commission on Stability in Cyberspace
- Tech Accord
- Charter of Trust

Regional organisations

- African Union and RECs
- ASEAN and ASEAN Regional Forum
- Organisation of American States
- Council of Europe
- G7/G20
- NATO

HOW TO ENGAGE WITH THE EU?

The European Union and its member states play an active role in shaping the global cyber diplomacy agenda. Through its presence and actions around the world, the European Union is a global leader in strengthening and protecting the free, open, secure, and peaceful nature of cyberspace.

The EU has some **140 delegations and offices around the world**. Representatives in your country are the first point of contact for any information about concrete EU activities and programmes.

The EU conducts **six specific cyber dialogues** with Brazil, China, India, Japan, the Republic of Korea, and the United States.

You can learn more about the EU's cyber diplomacy and its digital policies by visiting the websites of:

> **the European External Action Service**
www.eeas.europa.eu

> **the European Commission**
www.ec.europa.eu

Numerous **EU institutions, agencies and bodies** are engaged in international engagements of strategic or operational nature. You can contact them directly or visit their websites to learn more about their activities:

> **EU Agency for Cybersecurity (ENISA)**
www.enisa.europa.eu

> **European Cybercrime Centre (EC3)**
www.europol.europa.eu

> **EU Institute for Security Studies (EUISS)**
www.iss.europa.eu

> **CERT-EU**
www.cert.europa.eu

> **“[…] we depend on a rules-based international order and need commonly agreed rules and effective and inclusive global institutions, within and beyond the United Nations (UN) system, to ensure peace, security, human rights, prosperity and sustainable development for all. International law, agreements and rules establish a level playing-field for large and small countries alike.’**

Council conclusions on EU action to strengthen rules-based multilateralism (2019)

EU CYBER DIRECT

Supporting EU Cyber Diplomacy

Print
ISBN 978-92-9198-908-9
CATALOGUE NUMBER QN-01-20-008-EN-C
DOI:10.2815/686538

Online
ISBN 978-92-9198-909-6
CATALOGUE NUMBER QN-01-20-008-EN-N
DOI:10.2815/71385

Published by the EU Institute for Security Studies.
Cover image credit: Brett Zeck/unsplash