

Information integrity online and the European democracy shield

SUMMARY

In recent decades, the digital information sphere has become the public space for debate: the place where people access information, and form and express opinions. Over the past 10 years, global information ecosystems have also increasingly become geostrategic battlegrounds. Authoritarian state actors are testing and fine-tuning techniques to manipulate public opinion and foment divisions and tension, to undermine democratic societies and open democracy as a system.

At the same time, the geostrategic rivalry overlaps more and more with corporate geopolitics: the digital information sphere has become a contested territory for large corporations competing fiercely to lead the development and roll-out of new technologies – with artificial intelligence (AI) as a game changer in this quest. These innovations come with risks: information manipulation campaigns facilitated by generative AI magnify threats to democratic information ecosystems.

Strategic and systemic pressures on the open information environment are set to increase. This makes efforts to uphold universal values in the digital information environment – values such as human rights and, in particular, freedom of expression – even more essential.

The increased focus on information integrity by multilateral organisations makes room for coordinating actions to boost the resilience of information ecosystems more broadly, safeguarding human rights. This concept ties in with key parts of the work planned under the future 'European democracy shield'. The broad scope of information integrity covers a number of activities that are already under way in the EU – including measures and legislation launched in recent years – and offers new paths for coalitions and partnerships.



IN THIS BRIEFING

- Introduction: Evolving principles, practices and priorities
- Principles: Information integrity in a multilateral context
- Selected approaches



Introduction: Evolving principles, practices and priorities

The notion of **information integrity** has been gaining ground in international and multilateral forums in recent years. Used by the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD) as a positive approach to a safely navigable information sphere with access to trustworthy information for all, the concept as understood by the UN and the OECD emphasises protecting freedom of expression. This is in line with the EU Charter of Fundamental Rights, Chapter 2, [Article 11](#), which stipulates that freedom of expression includes freedom to hold opinions and to receive and impart information and ideas without interference. It is also in line with [Article 19](#) of the UN Universal Declaration of Human Rights on the right to freedom of opinion and expression, and Article 19 of the International Covenant on Civil and Political Rights ([ICCPR](#)).

In the EU, the broad concept of information integrity falls within the scope of the evolving European democracy shield idea. First announced in July 2024, the democracy shield initiative links existing work to counter **foreign information manipulation and interference (FIMI)** with the implementation of key legislation and initiatives to boost the health of the information sphere. This includes regulation of online platforms and search engines in the [Digital Services Act \(DSA\)](#), including the 2022 strengthened code of practice to make online platforms do more to curb information manipulation and hate speech, and the work of the [European Digital Media Observatory \(EDMO\)](#) and its regional hubs. It also includes the [AI Act](#), with its risk-based approach to regulating AI, including generative AI-facilitated information manipulation such as deepfakes, the [European Media Freedom Act](#), and the [Regulation on Transparency and Targeting of Political Advertising](#).

The terminology used by the EU and the European Parliament to capture the challenges to the democratic information sphere – including information manipulation and interference – continues to evolve. In 2018, the Commission [defined disinformation](#) as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public and may cause public harm'. **Misinformation**, on the other hand, refers to unintentionally false information. However, identifying intent to deceive can be challenging, and mis- and disinformation often overlap. The 2024 European Parliament elections saw [no major](#) last-minute disinformation campaigns targeting the elections directly, but rather a trickle of deceptive narratives linked with geopolitical tension, benefiting authoritarian actors seeking to erode trust in democracy.

Growing awareness about authoritarian threats to democracy, including in the information space, previously prompted Parliament to set up its first Special Committee on foreign interference in all democratic processes in the EU, including disinformation (INGE) in September 2020, followed by a second (ING2) in 2022. In line with this focus, the European External Action Service (EEAS) [pioneered](#) the term foreign information manipulation and interference (FIMI) in 2021. FIMI is defined as behaviour 'that threatens or has the potential to negatively impact values, procedures and political processes', is 'manipulative in character' and 'conducted in an intentional and coordinated manner', involving 'state or non-state actors, including their proxies inside and outside of their own territory'. FIMI reflects the EEAS' external mandate, with a focus on authoritarian state actors such as Russia and China.

The concept of information integrity is not a fixed analytical framework, and still lacks a clear definition, as [Yadav, Wanless and Lai](#) point out. Nevertheless, this evolving concept could offer a positive framework within which the EU can further expand its push to support healthy and sustainable information ecosystems – as a key pillar of the future European democracy shield – within and beyond the EU. Parliament used the concept of information integrity in resolutions by the two Special Committees on foreign interference in [2022](#) and [2023](#). These resolutions called for a centre for information integrity, to act as a knowledge hub to facilitate and foster operational exchange between Member States, EU institutions and EU agencies. As detailed below, the EEAS has a team dedicated to Information Integrity and Countering Foreign Information Manipulation and Interference ([SG.STRAT.4](#)).

Principles: Information integrity in a multilateral context

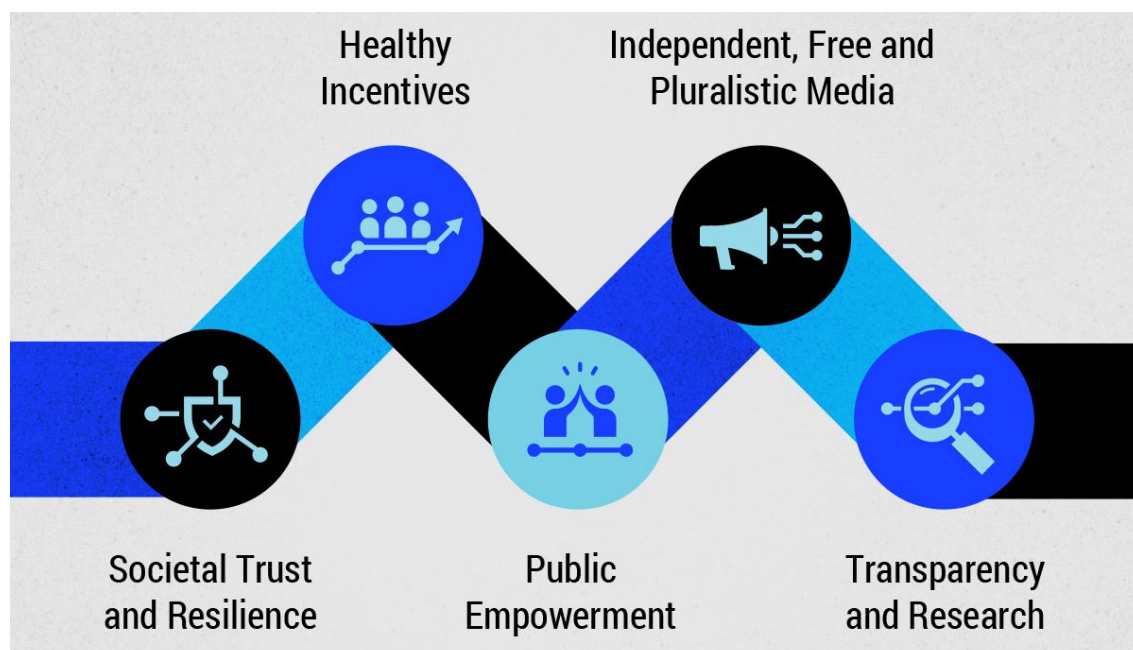
Information integrity has become a core concept for multilateral cooperation to tackle the wider challenges to the information space. Although there is no uniformly agreed definition of information integrity, the information integrity approaches detailed below take the complexity of the challenges into account and focus on positive actions in the efforts to boost the entire information ecosystem. They emphasise the importance of sustainability and upholding human rights in the information ecosystem, with a focus on cooperation among all actors in the information sphere. Key stakeholders include large tech companies, which help shape the way information is created, disseminated and received, including using new and emerging technology, such as generative AI (GAI).

Whereas international and multilateral approaches, as listed below, emphasise the importance of safeguarding human rights, authoritarian state actors – notably Russia and the People's Republic of China (PRC) – are working to assert their state-driven approach in the global information ecosystem, weakening rights-centred frameworks for governance and standard-setting. Significant PRC [investment](#), in particular, in influencing the multilateral system, is a source of concern among human rights experts and watchdogs. The PRC is seeking to insert its own initiatives, terms and conditions to govern emerging technologies, to [protect itself](#) from criticisms relating to human rights. Further US disengagement from the multilateral system under the second Trump administration may [create a vacuum](#) for China to push its own system and replace the Washington-led world order.

The United Nations global principles for information integrity

On 24 June 2024, the UN published its five [global principles for information integrity](#), which are: societal trust and resilience; healthy incentives; public empowerment; independent, free, and pluralistic media; and transparency and research. The document served as a resource for Member States ahead of the September 2024 [Summit of the Future](#). The global principles stress that building up information integrity is essential to keep working towards the Sustainable Development Goals, and that this means fighting misinformation, disinformation, and hate speech while protecting human rights such as freedom of expression.

Figure 1 – UN global principles for information integrity



Source: United Nations Global Principles for [Information Integrity](#), Department of Global Communications, © (2024) United Nations. Reprinted with the permission of the United Nations.

A 2023 UN policy brief on [information integrity on digital platforms](#) built on the 'Our Common Agenda' proposal outlined principles for a code of conduct to 'make the digital space more inclusive and safe for all, while vigorously defending the right to freedom of opinion and expression, and the right to access information'.

The outcome documents from the Summit of the Future – the [Pact for the Future, Global Digital Compact and Declaration on Future Generations](#) – included a commitment in the Global Digital Compact to 'work together to promote information integrity, tolerance and respect in the digital space, as well as to protect the integrity of democratic processes'. It recognised that digital and emerging technologies can enable information manipulation and interference and thereby harm societies and individuals, erode human rights, fundamental freedoms and the Sustainable Development Goals (SDG). It pledged to boost international cooperation to address mis- and disinformation and online hate speech and mitigate the risks 'in a manner consistent with international law'.

The [Global Digital Compact](#) includes the following commitments, to be fulfilled by 2030:

- roll out digital media and information literacy curricula to increase resilience against mis- and disinformation (DSG 3 and 4);
- promote diverse and resilient information ecosystems, including via independent and public media and supporting journalists (SDGs 9 and 16);
- independent, fact-based, timely, targeted, clear, accessible, multilingual and science-based information to counter mis- and disinformation (SDGs 3, 4, 9 and 16);
- promote access to relevant, reliable and accurate information in crises (SDG 10);
- encourage UN entities, together with governments and stakeholders, to assess the impact of mis- and disinformation on the Sustainable Development Goals (SDG 17).

Against this backdrop, the Global Digital Compact urgently called on

- digital tech companies and social media platforms to improve transparency and accountability, including on terms of service, content moderation, recommendation algorithms and handling of personal data in local languages, enabling users to make informed choices, for example on consent (SDGs 9 and 10);
- social media platforms to grant researchers access to data, ensuring transparency and accountability and build evidence on mis-, disinformation and hate speech, informing government and industry policies, standards and best practices (SDGs 9, 16 and 17);
- digital tech companies and developers to continue to develop solutions and publicise actions to counter potential harms from AI-enabled content, including hate speech and discrimination. Measures include safeguards in AI model training processes, identification of AI-generated material, authenticity certification for content and origins, labelling, watermarking and other techniques (SDGs 10, 16 and 17).

Information integrity and elections

The importance of information integrity is particularly apparent in the context of elections. In 2022, the [United Nations Development Programme](#) (UNDP) – as the main provider of electoral support within the UN framework – launched the [Action Coalition on Information Integrity in Elections](#), supported by the Danish Government's [Tech4Democracy](#) initiative. Led by the UNDP's [Global Policy Centre for Governance](#), the Action Coalition was launched against a backdrop of new and emerging challenges from information pollution worldwide, facilitated by a fast-evolving toolbox used by malicious actors seeking to disrupt the information ecosystem around elections. Key objectives of the cooperation include:

- improving information sharing and coordination among key stakeholders in electoral assistance and support, to include representatives from the technology sector;
- assessing and understanding impacts of disinformation on electoral integrity;

- analysing best practice and case studies to develop effective recommendations and guidance; coordinating responses to threats to information ecosystems if relevant;
- assessing emerging analysis, approaches and recommendations to feed into new thinking and positions on relevant issues.

OECD: Boosting information integrity, democracy and trust

Information integrity is a cornerstone of the OECD's [Reinforcing Democracy initiative](#), which was launched in 2022 at the OECD Global Forum and Ministerial on Building Trust and Reinforcing Democracy. In this context, OECD member countries established the Information Integrity Hub as a forum for analysing public governance measures to boost the integrity of the information space. The OECD describes its hub as a peer-learning platform where countries can exchange data and best practice, and that offers resources to address global information challenges, such as foreign information manipulation and interference.

In its 2024 report [Facts not fakes: Tackling disinformation, strengthening information integrity](#), the OECD emphasised the urgency of boosting 'the integrity of information spaces and combating disinformation' to reinforce democracy and strengthen the fabric of open societies. Not unlike the considerations behind the EU's all-of-society approach, the OECD recommended a 'multi-stakeholder approach' with governments playing a 'constructive, yet not intrusive' role in reinforcing information integrity. Governments would also protect the independence and variety of content production, with all actors in the information ecosystem taking responsibility. The recommendations included three complementary policy aims:

1. enhancing transparency, accountability, and plurality of information sources;
2. fostering societal resilience to disinformation; and
3. upgrading governance measures and institutional architecture to uphold the integrity of the information space.

Linking trust and resilience of democracies with information integrity

The work of the Information Integrity Hub is a key element in the broader focus of the OECD on challenges to democracy, and the links between polarisation, distrust in online spaces and within democratic societies, and vulnerabilities to foreign interference and disinformation.

In November 2024, the OECD invited stakeholders from all countries – media representatives, journalists, private sector players, civil society organisations, academics, citizens, international organisations and government experts – to comment on a [draft recommendation on information integrity](#). The goal of the draft recommendation is to guide policy makers to promote information integrity 'in line with the universal human rights of freedom of opinion and expression'. Recommendations include:

- a coherent, comprehensive approach to boosting information integrity and upholding universal human rights by developing and implementing strategic frameworks;
- transparent mandates for relevant agencies, offices, units, or coordination mechanisms, including via technical advice on policies on AI, foreign interference, and electoral interference;
- deterring and mitigating risks to electoral processes; maintaining a safe and enabling environment that helps citizens exercise their right to participate in public affairs;
- increased international cooperation to strengthen the collective response to information integrity challenges, including efforts to reinforce local, pluralistic, independent, and public interest media via official development assistance and media development agencies;
- capacity-building and sufficient resources at local, national, and international levels for public officials who analyse and respond to information manipulation threats.

The final draft recommendation will be submitted to the Public Governance Committee for approval. Once approved, it will be presented to the OECD Council for adoption.

Selected approaches

According to Freedom House's [Freedom on the Net 2024](#) report, governments in more than half of the 41 countries that held or prepared for national elections during the reporting period invested in making their information space more reliable. Some of the commonly used steps included: cooperating with tech companies to boost authoritative information from election commissions; countering false or misleading information; supporting fact-checking initiatives by local media or civil society; and laying down rules for the use of GAI in political campaigns. The increasing focus on information integrity at multilateral and international levels offers a framework to link digital diplomacy, knowledge diplomacy and initiatives to promote democracy and capacity-building.

Canada

Canada is engaging in or leading a number of initiatives to boost information integrity, often in cooperation with EU Member States. For example, Canada and Latvia, together with the Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States, co-led the [Cohort on Information Integrity](#) that resulted from US President Joe Biden's first [Summit for Democracy](#) in 2021. The cohort included four thematic working groups focusing on: taxonomy, literacy, international cooperation on resilience to disinformation, and political microtargeting. In addition to [recommendations and reports](#) from the four working groups, the cohort also produced a [global mapping project](#), tracking over 500 organisations from across the world working to counter disinformation in the areas of fact-checking and verification; media literacy and training; research and mentoring; policy and standards.

Building on the work of the cohort and complementing existing UN efforts, Canada and the Netherlands launched the [Global Declaration on Information Integrity Online](#) in September 2023. Endorsed by 36 states at the time of writing, including 18 EU Member States as well as the US and the UK, the declaration defines information integrity as 'an information ecosystem that produces accurate, trustworthy, and reliable information, meaning that people can rely on the accuracy of the information they access while being exposed to a variety of ideas'. It aims to 'offer a positive vision of a broader information ecosystem that respects human rights and supports open, safe, secure, prosperous and democratic societies'. Participating states commit to respect, promote and fulfil freedom of opinion and expression, promote pluralistic media and journalism and protect access to media. They also pledge to 'abstain from conducting or sponsoring disinformation campaigns, domestically or transnationally'. The declaration includes recommendations for online platforms to improve content moderation, empower users, and improve algorithmic auditing. It urges 'responsible, human rights-based and human-centric design, development, implementation, and use of existing, new and emerging technologies, notably generative artificial intelligence, in a manner that upholds and safeguards information integrity online'.

United States

In addition to incorporating the notion of information integrity into [democracy assistance work](#), as mentioned above, the concept of information integrity is built into US executive digital diplomacy. The May 2024 [US international cyberspace and digital policy strategy](#), published by the Department of State (DoS), lists defending information integrity as a priority. It highlights the EU-US Trade and Technology Council (TTC), OECD and G7 as key forums for cooperation. This follows the 2023 launch by the DoS Bureau of Cyberspace and Digital Policy (CDP) of a [democratic roadmap](#) for building civic resilience to the global digital information manipulation challenge. It includes the following steps for global policymakers, civil society, and the private sector:

1. highlight the importance of the digital information manipulation challenge as a threat to the functionality and vitality of society;

2. recognise that building information integrity can be consistent with freedom of opinion and expression;
3. reinforce private sector digital platforms' ability to strengthen civic resilience to promote information integrity;
4. prioritise efforts to address generative AI, notably in the context of global 2024 elections.

Following the EU-US Trade and Technology Council April 2024 ministerial meeting, the US DoS and the EEAS launched a joint [US-EU coordination mechanism on information integrity in the Western Balkans](#). It seeks to 'empower like-minded partners to become self-sufficient in addressing the FIMI threat and to work together to reduce Russia's and the People's Republic of China's ability to employ propaganda and information manipulation campaigns in the region'.

European Union

Over the past decade, the EU has been developing a holistic, all-of-society approach to challenges in the information sphere. Triggered by Russia's illegal annexation of the Crimean peninsula and its hybrid war against Ukraine, the [European External Action Service](#) created the [East StratCom Task Force](#) in 2015, with a mandate from the European Council to counter Russia's ongoing disinformation campaigns. Since then, the EEAS has continued to expand its work to counter foreign information manipulation and interference (FIMI). Combining policy and methodology development, analysis and responses to FIMI, EEAS work includes cooperation with partners on democracy promotion as well as support of delegations, civilian and military missions and operations. Central to the work is strategic communications, support of independent media and awareness-raising, notably under the [EUvsDisinfo](#) brand. In addition, a [rapid alert system](#) (RAS) facilitates cooperation with other EU institutions and Member States on the FIMI file. Additional task forces have been added to East StratCom, covering the EU's southern neighbourhood, the Western Balkans, China, sub-Saharan Africa, and common security and defence policy military and civilian missions. A dedicated team of data analysts is also now part of the operation.

The EEAS is also working with the Commission and the Member States to expand and tailor the [EU Toolbox](#) to tackle FIMI. The EU has stepped up [cooperation with NATO](#) and in the framework of the G7 rapid response mechanism to counter disinformation. In addition, the EEAS is leading the work to build an information-sharing and analysis centre ([FIMI ISAC](#)), a platform to facilitate the sharing of experience, knowledge, analysis and information between stakeholders, including civil society, about root causes, incidents and threats. The work is being carried out by the EEAS Information Integrity and Countering Foreign Information Manipulation and Interference Division ([SG.STRAT.4](#)), in cooperation with the EEAS strategic communications and public diplomacy divisions ([SG.STRAT.3](#) and [SG.STRAT.2](#)).

In addition to the evolving work of the EEAS, the EU's whole-of-society approach to boosting information ecosystems encompasses broad policy areas such as digital regulation, education, and media freedom and pluralism (see above).

European democracy shield: Joining up the dots

Building on the EU's expanding toolbox to counter foreign information manipulation and interference, in July 2024 European Commission President Ursula von der Leyen proposed a 'European democracy shield'. Reflecting the all-of-society approach of the EU to boosting shared information ecosystems, a number of Commissioners will be tackling various aspects of the planned European democracy shield when it comes to information integrity aspects. Responsibility for the European democracy shield lies primarily with the Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, [Michael McGrath](#), building on the European democracy action plan and the defence of democracy package. Key tasks relating to information integrity include:

- stepping up the fight against foreign information manipulation and interference;

- coordinating the work on disinformation and working with other Commissioners to boost the work on digital and media literacy and on prevention through pre-bunking;
- protecting integrity of elections;
- working with Parliament and the Council to reach agreement on proposals still on the table, such as on European political parties and foundations;
- implementing the European Media Freedom Act and putting forward proposals to further support and protect independent media and journalists, building on the work done to protect them from abusive lawsuits (SLAPPs).

McGrath reports to [Henna Virkkunen](#), Executive Vice-President for Tech Sovereignty, Security and Democracy, who is responsible for:

- enforcing the Digital Services Act and the Digital Markets Act, establishing long-term compliance dialogues with the regulated entities, and contributing to the work on disinformation, as part of the European democracy shield;
- promoting EU digital norms and standards internationally and ensuring a leading role for the EU in global digital governance, in particular for AI and cybersecurity;
- with the Commissioner for International Partnerships, supporting Global Gateway projects in partner countries, for instance trustworthy digital communications networks.

The European External Action Service (EEAS) has been spearheading the EU's efforts to counter disinformation from Russia since 2015. This includes the current focus on information integrity and countering foreign information manipulation and interference. This work is mentioned only implicitly in the [mission letter](#) for the High Representative/Vice President (HR/VP) Kaja Kallas, and includes:

- strengthening the EU-NATO partnership, covering all security threats, including new dangers linked to cyber, hybrid and space;
- working with the Commission to ensure that the EU can react flexibly to new threats, including cyber- and hybrid attacks;
- leading the work on a new horizontal set of restrictive measures against hybrid threats against the EU, complementing existing sanctions;
- ensuring that Europe plays a leading role in strengthening and updating multilateralism and in reforming the international rules-based system.

The [mission letter](#) for the Commissioner for Defence and Space, Andrius Kubilius, tasks him with:

- working to address vulnerabilities to cyber-attacks and hybrid attacks and building up resilience and capacity to counter them more robustly and effectively.

The work planned under the European democracy shield already includes previously envisaged priorities that tie in with the broad concept of information integrity. The enforcement of the EU's digital regulations, for example, is arguably the strongest step ever to be taken at governmental level to hold online platforms accountable. However, the bolstering of the relevant acts, which will be a focus of the new Commission, could face challenges from the new Trump administration and its close ties with parts of the tech industry. This could bring the underlying friction between the rights-driven EU approach to digital regulation and the [US market-driven model](#) to the fore.

Role of the European Parliament

Over the past two legislative terms, Parliament has used a [mix of tools](#) to address challenges to the democratic information sphere: legislative work, non-legislative resolutions, hearings, and its budgetary powers. The latter were key to the evolution of the EEAS StratCom team, with Parliament's [2016 resolution](#) on strategic communication to counteract anti-EU propaganda by third parties calling for the StratCom Task Force to be turned into 'a fully fledged unit ... with proper staffing and adequate budgetary resources, possibly by means of a dedicated budget line'.

The creation of the first Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation (INGE) in 2020 helped increase the EU's focus on FIMI. After its mandate expired, Parliament created a new Special Committee (ING2) in 2022 to follow up; it operated until 2023. In resolutions adopted in [March 2022](#) and [June 2023](#) respectively, Members of Parliament (MEPs) called for a common EU strategy to tackle foreign interference and disinformation. As well as calling for support for independent media, fact checkers and researchers, MEPs urged the Commission and the EEAS to consider creating a 'European centre for information integrity' as a knowledge hub to facilitate and foster operational exchange between Member States' authorities, EU institutions and EU agencies. Parliament is currently working to determine how to follow up on the mandates of INGE and ING2, and engage with the planned European 'democracy shield' in the Commission.

In addition to the external focus of the two Special Committees on Foreign Interference, Parliament's work to counter information manipulation has cut across policy areas, reflecting the EU's whole-of-society approach. This includes work of the Committee on Civil Liberties, Justice and Home Affairs ([LIBE](#)) on the Media Freedom Act; the Committee on the Internal Market and Consumer Protection ([IMCO](#)) on the DSA, the General Data Protection Regulation, copyright and political advertising; in addition to the Subcommittees on Defence ([SEDE](#)) and Human Rights ([DROI](#)) and the Special Committee on Artificial Intelligence in a Digital Age (AIDA).

The concept of information integrity lends itself to connecting the abovementioned work with other activities and responsibilities of the European Parliament, as well as expanding existing efforts linked with strengthening information ecosystems and defending democracy at home and abroad. This includes global democracy support activities through the Democracy Support and Election Coordination Group ([DEG](#)). This group has an official consultative role for the High Representative (HR/VP) when selecting priority countries for [EU election observation missions](#), and when appointing chief observers for those missions. Every EU election observation mission is headed by an MEP.

The DEG also engages in human rights activities, including the annual Sakharov Prize for Freedom of Thought, the EU's most prestigious human rights award. Moreover, the Triangle for Democracy programme brings together legislators, civil society and media actors to tackle disinformation while protecting freedom of expression. In addition, the European Parliament's external offices play a key role in establishing parliamentary democracy partnerships across the world, including by engaging with international organisations and forums, such as the [Global Parliamentary Forum](#) of the Global Parliamentary Network on World Bank and the International Monetary Fund. Via its external offices – as well as its European and international parliamentary networks and partnerships – Parliament can contribute to fostering global coalitions and multi-stakeholder cooperation to boost information integrity, within the framework of the evolving European democracy shield.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2024.

Photo credits: © Suriya / Adobe Stock.

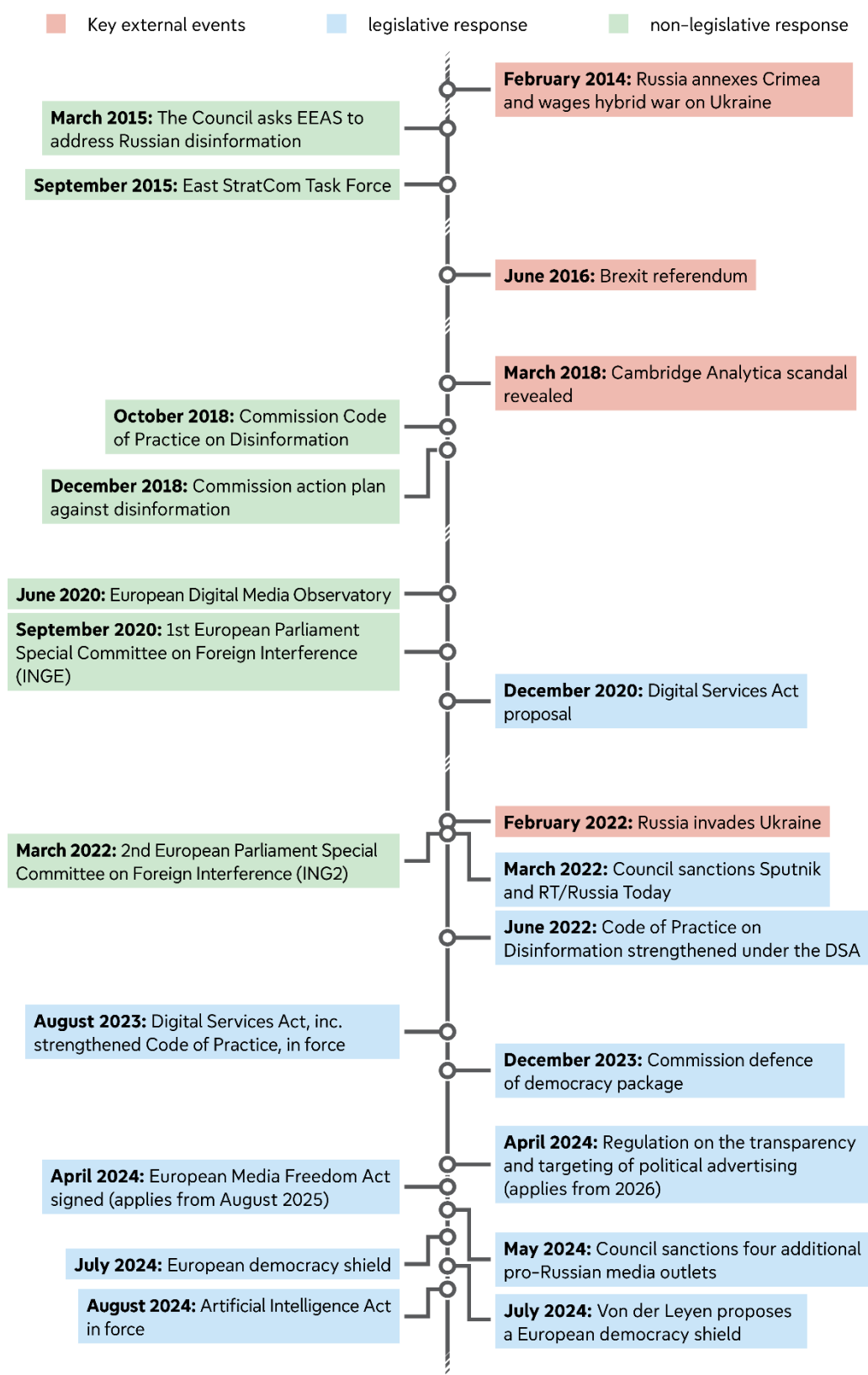
eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

<http://epthinktank.eu> (blog)

Annex – Timeline: Information manipulation and the EU response



Source: EPRS, European Parliament, 2024, based on the [Official Journal of the EU](#), [European Commission](#), [the Council](#), and [The Guardian](#).