BRIEFING

European Parliament

Foreign interference in democracies

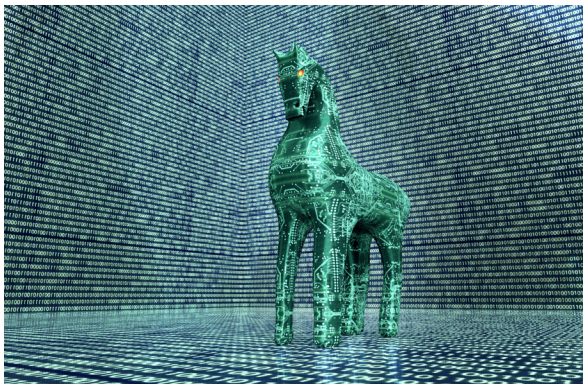
Understanding the threat, and evolving responses

SUMMARY

Across the world, democratic societies, institutions, processes and values are under increasing external and internal attack. The coronavirus crisis has, meanwhile, exacerbated the systemic struggle between democracy and authoritarianism, prompting authoritarian state and non-state actors to deploy a broad range of overt and covert instruments in their bid to destabilise their democratic counterparts.

Against this backdrop, and following a string of examples of hostile meddling by authoritarian actors to undermine democratic governing processes in countries such as Ukraine, the United Kingdom, the United States (US), Canada and Australia, the focus on foreign interference continues to sharpen.

Among the EU's institutions, the European Parliament – arguably the flagship of European democracy – is pushing the policy response to foreign interference to the top of the political agenda. Among other initiatives and actions, in October 2019 it passed a resolution on countering foreign interference and has set up a special committee on foreign interference, whose constituent meeting is scheduled to take place in September 2020.



In this Briefing

EPRS | European Parliamentary Research Service

Author: Naja Bentzen
Members' Research Service

PE 652.082 – September 2020

EN

Background: The authoritarian threat

While democratic societies, institutions, processes and values around the world have been under growing attack in recent years, the pandemic has further prompted authoritarian state and non-state actors – often under pressure to deflect blame for their own (mis-)handling of the crisis – to deploy a range of overt and covert instruments. These actors' attempts to turn the strengths of liberal democracies into weaknesses are increasingly well documented. As the Finnish Institute of International Affairs (FIIA) argued in a September 2019 working paper, 'the four cornerstones of Western democracy – state restraint, pluralism, free media and economic openness – provide openings for hostile external actors to interfere in democratic society through a host of covert, non-military means calibrated to undermine their internal cohesion and accelerate political polarization'. The sharpening focus on these challenges – not least in the European Union (EU) – is also drawing growing attention to discussion of definitions, as shown below, with a specific focus on three major, consolidated liberal democracies – the US, Australia and Canada – that have stepped up their responses to foreign interference in recent years. The multifaceted threats call for a whole-of-society response, requiring close (international) cooperation and coordination across policy areas, within and among institutions and democratic governments (including NATO and EU Member States), as well as with all stakeholders, notably media, the tech industry and civil society.

Responses of selected democratic actors

United States

US legislative steps to counter modern era foreign propaganda date back to the interwar years.[1] After the Cold War, however, countering propaganda by foreign actors declined as a US priority, until the 9/11 attacks reignited the need to respond to the propaganda of foreign actors such as Al-Qaida and, more recently, ISIL/Da'esh. Following the investigation into Moscow's meddling in the 2016 Presidential election, there is mounting concern that the Kremlin could interfere in the 2020 election. In 2018, the Department of Homeland Security (DHS) set up the 'countering foreign influence task force' as part of the National Risk Management Center within the Cyber and Infrastructure Security Agency (CISA). CISA – the lead federal agency responsible for national election security – defines foreign interference as 'malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies'.

In a July 2019 awareness-raising infographic, published as part of a national call for action to protect the 2020 elections (Protect2020), CISA explains foreign interference in the following five steps:

- Targeting divisive issues: 'Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States. They don't do this to win arguments; they want to see us divided'.
- Moving accounts around: 'Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user'.
- Amplifying and distorting the conversation: 'Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online'.
- Making the mainstream: foreign influencers 'fan the flames' by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.
- Taking the conversation into the real world: 'In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create

event pages and ask followers to come out. What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference'.

On 1 September 2020, CISA stated that they had seen no evidence of attacks on voting infrastructure (apart from disinformation targeting mail-in voting). The Director of National Intelligence also said that there had been no signs of foreign governments attempting to interfere in mail-in voting processes. A 3 September intelligence bulletin by the DHS warned that Moscow would likely increase its efforts to promote allegations of US election system corruption, failures, and foreign interference to reduce public confidence in the upcoming election.

Australia

Australia's approach to foreign interference has been shaped by its work to counter the Chinese Communist Party (CCP), whose activities in Australia in recent years have prompted increasing concern and a correspondingly decisive response. In December 2019, the prime minister announced the establishment of a 'counter foreign interference taskforce' to strengthen the Australian government's ability to 'discover, track and disrupt foreign interference' in the country.

Australia's Department of Home Affairs (DHA) makes a clear, explicit distinction between foreign influence and foreign interference. It defines **foreign influence** as open and transparent attempts by governments to influence discussions on issues of importance. By contrast, **foreign interference** is defined as activities going beyond routine diplomatic influence practised by governments, that may take place in isolation or alongside espionage activities, and that are:

- carried out by, or on behalf of a foreign actor;
- coercive, corrupting, deceptive and clandestine; and
- contrary to Australia's sovereignty, values and national interests.

The DHA further explains that foreign actors, including foreign intelligence services, 'are creating and pursuing opportunities to interfere with Australian decision makers at all levels of government and across a range of sectors', including:

- democratic institutions;
- education and research;
- media and communications;
- culturally and linguistically diverse communities; and
- critical infrastructure.

Australia's definition of and approach to foreign interference go far beyond electoral processes. The counter foreign interference (CFI) strategy is aimed broadly at protecting the country's sovereignty, values and national interests. It focuses on five pillars:

- enhancing capability to meet current and future needs;
- engaging at-risk sectors to raise awareness and develop mitigation strategies;
- deterring the perpetrators by building resilience in Australian society;
- defending directly against foreign interference activity through a coordinated government response; and
- enforcing Australia's CFI laws, by investigating and prosecuting breaches.

Correspondingly, the National Counter Foreign Interference Coordinator, appointed in 2018, works with the Home Affairs Department and Australian government and state and territory agencies to coordinate the whole-of-government approach to countering foreign interference. The following legislation to deter and counter foreign interference is relevant in this context:

- the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, which criminalises covert and deceptive activities of foreign actors that intend to interfere with Australia's institutions of democracy, or support the intelligence activities of a foreign government;

- the Foreign Influence Transparency Scheme Act 2018, which shows the nature and extent of foreign influence in government and political processes;
- the Security of Critical Infrastructure Act 2018, which includes a register of critical infrastructure assets providing visibility of who owns and controls the assets; an information-gathering power; and a ministerial directions power;
- the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Act 2018, which restricts the receipt of donations from foreign donors; and
- the Telecommunications and Other Legislation Amendment Act 2017, which imposes security and notification obligations on regulated entities to 'do their best' to protect networks and facilities from unauthorised interference.

In an illustrative example of Australia's holistic approach and response to foreign interference, in August 2020 – following growing concern over the CCP's influence on the Chinese diaspora in Australia – Canberra announced that it would provide migrants with free and unlimited English-language courses to reinforce Australian values and boost social cohesion. Australia's multicultural affairs minister, Alan Tudge, stated that, in the face of 'unprecedented high' foreign interference, the government was developing a broad campaign emphasising national identity and democratic values. He expressed particular concern that 'Members of our diverse communities have been both victims of interference and used as vectors to engage in foreign interference'.

Canada

According to the Government of Canada, foreign interference poses an increasing threat to the country's democratic institutions: 'New technologies and advances in how we consume information may potentially allow adversaries to use cyber-enabled means to influence Canada's democratic processes'. The 'security and intelligence threats to elections task force' is leading the work to combat foreign interference campaigns, and is made up of the following Canadian security and intelligence organisations:

- the Canadian Security Intelligence Service (CSIS);
- the Royal Canadian Mounted Police (RCMP);
- the Communications Security Establishment (CSE); and,
- Global Affairs Canada (GAC).

The G7 Summit in Charlevoix in June 2018 established a rapid response mechanism (RRM) to coordinate identification of and responses to evolving threats to democracies, under Canada's lead. In addition to this work, the Canadian organisations involved have continued their efforts to combat foreign interference by:

- protecting government systems and networks, as well as offering Elections Canada and political parties cyber advice and guidance (CSE);
- actively monitoring and reporting threats to the government and providing political parties with classified briefings on potential threats (CSIS),
- detecting and disrupting attempted foreign interference activity and investigating criminal activity related to interfering with or attempting to influence Canada's electoral processes (RCMP).

Furthermore, the December 2018 Elections Modernization Act (Bill C-76) prohibits the use of funds from foreign entities and includes heightened transparency measures, such as with regard to the use of foreign funds by third parties for partisan advertising and activities. It also clarifies offences related to false statements and foreign interference. Platform operators or owners can be prosecuted for knowingly selling election advertising to non-Canadians.

Think-tanks: Working towards common definitions

In a March 2019 briefing published by the **Alliance for Securing Democracy** (ASD) – dedicated specifically to conceptualising foreign interference in Europe – the authors argue that intent and

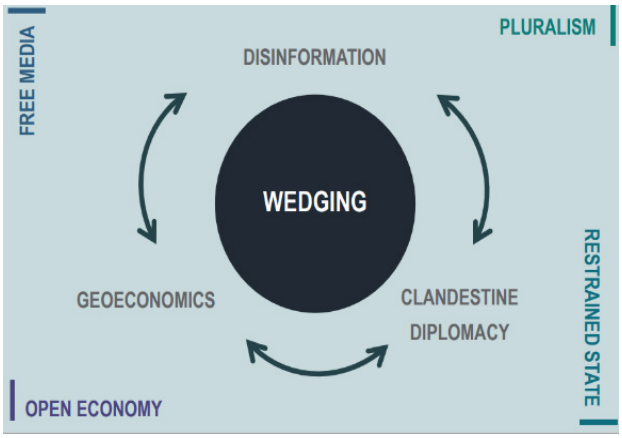
transparency are 'common threads in existing approaches to defining interference', providing a 'useful starting point for setting a definition for interference' when assessing 'unacceptable nation-state activity'. As interference tactics, ASD lists cyber-attacks, information operations, malign financial influence, the subversion of political and social organisations, and strategic economic coercion. According to the authors, the use of a qualifier such as 'malign' (G7 Charlevoix Commitment) or 'malicious' (Commission communication, September 2018) before the word 'interference', is 'problematic', as it 'suggests there is a form of interference that is not malign'.

The authors assert that the 'European Union and EU Member States are at the forefront of global efforts to counter interference by authoritarian states in democracies', and that the way the EU defines foreign interference in the future has the potential to carry significant weight, as 'global democracies will be looking to the European definition process as a standard setter'. The authors point at alleged inconsistencies by EU institutions regarding the usage of 'external', 'foreign' and 'third country'. The EU's terminology database IATE ('Interactive Terminology for Europe') notes that the term 'third country' – used in the EU Treaties – means 'a country that is not a member of the European Union', in the sense of a country not party to an agreement between two other countries. The term is used synonymously with 'non-EU', 'external' and 'foreign' country.

Alex Joske from the **Australian Strategic Policy Institute** (ASPI) argues that all aspects – including soft 'influence' tactics – should be taken into account when responding to the CCP's efforts to boost its influence by co-opting representatives of ethnic minority groups, religious movements, and business, science and political groups, speaking on behalf of these groups and using them to boost its own legitimacy. The challenge lies in connecting the deceptive dots: Joske says that diplomats might view the CCP's 'united front' system – 'a network of party and state agencies responsible for influencing groups outside the party, particularly those claiming to represent civil society' – as 'public diplomacy' or 'propaganda', without fully appreciating the scope of related covert activities. At the same time, 'Security officials may be alert to criminal activity or espionage while underestimating the significance of open activities that facilitate it. Analysts risk overlooking the interrelated facets of CCP influence that combine to make it effective'.

In a September 2019 working paper published by the **Finnish Institute of International Affairs** (FIIA), Mikael Wigell uses the notion of 'hybrid interference' to mean 'non-military practices for the mostly covert manipulation of other states' strategic interests'. Wigell makes a clear distinction with hybrid warfare, 'which is essentially a military approach to conducting "indirect war" under special circumstances'. Focusing not only on actions by the CCP and the Kremlin, but also by Erdogan's Turkey and the Islamic Republic of Iran, Wigell explains that 'the idea is not to confront the target head-on, but to weaken its resolve by more subtle means of interference calibrated to undermine its internal cohesion'. This 'wedge strategy' fosters divisions or aggravates existing tensions among target populations, weakening the target's cohesion and its potential to take counter-actions. He argues that hybrid interference is deliberately designed to exploit the key cornerstones of liberal democracy: state restraint, pluralism, free media, and open economy. The openness provides loopholes for interference through the tactical combination of covert action that involves cultivating local subversive organisations and fostering counter-elites; geo-economics to interfere strategically in target countries; and disinformation. Wigell also introduces the concept of

Figure 1 – Hybrid interference as strategic practice



Source: FIIA, 2019.

democratic deterrence to counter hybrid interference, suggesting that liberal democratic values are not per se security vulnerabilities, but can be used as 'tools for a credible deterrence response against hybrid aggressors, all the while making our Western democracies more robust and resilient'.

EU and European Parliament response

In recent years, the EU has stepped up its response to growing hybrid threats and disinformation in the Union and its neighbourhood (with Ukraine as a highly visible target and testing ground for the Kremlin's hybrid attacks since 2014), while also making efforts to boost its cybersecurity. The EEAS East StratCom task force was launched in September 2015 to counter ongoing disinformation campaigns by the Kremlin, marking a milestone in the battle against disinformation. Since then, two additional task forces have been set up, focusing on the western Balkans and on the southern neighbourhood, respectively. Parliament has consistently supported this work.

The EU's focus on protecting democratic processes – notably elections – grew significantly in the wake of the 2016 UK referendum on EU membership, the US presidential elections the same year, the 2018 Facebook/Cambridge Analytica scandal, revelations about election interference around the world, and also with a view to the 2019 elections to the European Parliament.

In April 2018, the European Commission presented the communication 'Tackling online disinformation: a European approach'. This was followed by a Code of Practice on Disinformation – with leading social networks, online platforms and advertisers agreeing to self-regulate in order to combat disinformation. An action plan against disinformation meanwhile helped to strengthen the EU's capability to counter disinformation ahead of the European elections, with initiatives such as the Rapid Alert System (RAS), set up in March 2019 to enable common situational awareness of disinformation campaigns across EU Member States and facilitate common responses to them.

The European Commission's September 2018 communication on securing free and fair European elections stated that 'Protecting democracy in the Union is a shared and solemn responsibility of the European Union and its Member States. It is also a matter of urgency. All actors involved have to step up their efforts and cooperate to deter, prevent and sanction malicious interference in the electoral system.' The resilience of the EU's democratic system is part of the security union, and measures to protect elections focus on five inter-related areas:

- data protection: improving the protection of personal data in the electoral context;
- transparency: guaranteeing the transparency of online political advertising;
- cybersecurity: protecting elections from cyberattacks;
- cooperation: improving national and European cooperation on potential threats to European Parliament elections;
- appropriate sanctions: guaranteeing that electoral rules are respected by all.

In her 2019 agenda for Europe, the President of the European Commission, Ursula von der Leyen stated that, amid increasing attack 'from those who wish to divide and destabilise our Union'… 'We need to do more to protect ourselves from external interference'.

In its December 2019 conclusions on 'Complementary efforts to enhance resilience and counter hybrid threats' the Council of the EU stated that it 'recognises that a comprehensive approach at all levels is needed to address the challenges of disinformation, including interference seeking to undermine free and fair European elections, making best use of all available tools online and offline. This must include monitoring and analysis of disinformation and manipulative interference, enforcement of European data protection rules, application of electoral safeguards, efforts to enhance pluralistic media, professional journalism and media literacy as well as awareness among citizens'. The Council recognised 'the potential of the rapid alert system (RAS) regarding the fight against disinformation, in particular on election interference'. It urged the Commission, the EEAS and the Member States 'to further develop the RAS towards a comprehensive platform for Member States and EU institutions to enhance cooperation, coordination and information exchange, such as

research and analytical insights, best practices, and communication products, to support addressing disinformation campaigns as part of a range of European and national efforts'.

In January 2020, the Vice President of the European Commission for Values and Transparency, Věra Jourová, mentioned Russia and China explicitly as 'specific external actors' that are 'actively using disinformation and related interference tactics to undermine European democracy'.

In its July 2020 Security Union Strategy, the Commission proposed improved cooperation between intelligence services, EU INTCEN, and other organisations involved in security, as part of efforts to enhance cybersecurity and combat terrorism, extremism, radicalism and hybrid threats. It also announced that the Commission and the High Representative will set out an EU approach to hybrid threats that 'integrates the external and internal dimension in a seamless flow and brings the national and EU-wide considerations together', covering the full spectrum of action – from early detection, analysis, awareness, building resilience and prevention to crisis response and consequence management. The focus on mainstreaming hybrid considerations into policy-making aims to ensure that new developments and relevant initiatives are taken into account. Education, technology and research will be included in this framework, which aims to ensure regular, comprehensive intelligence-based reporting on the evolution of hybrid threats, to underpin decision-making. The EU Hybrid Fusion Cell remains the focal point for hybrid threat assessments.

In addition, a large number of EU Member States and stakeholders, and also EU agencies and bodies, support the 'Paris Call' for trust and security in cyberspace, launched by France in 2018. The initiative aims at developing common principles for securing cyberspace, including boosting the shared capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities. The call reaffirms that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by states.

The **European Parliament** held a debate on foreign electoral interference and disinformation in national and European democratic processes on 17 September 2019. On 10 October 2019, the European Parliament adopted a resolution on foreign electoral interference and disinformation in national and European democratic processes by 469 votes to 143, with 47 abstentions. Members underlined that foreign interference in elections, by compromising citizens' right to participate in their country's government, was part of a broader strategy of hybrid warfare, and that addressing it therefore remained a core security and foreign policy issue. They pointed out that free and fair elections were at the heart of the democratic process and called on the EU institutions and Member States to take decisive action in this regard. Highlighting the global trend of far-right groups using large-scale disinformation on social media platforms, Members voiced concern that evidence of interference, often with indications of foreign influence, is constantly being uncovered in the run-up to all major national and European elections, with much of this interference benefiting anti-EU, right-wing extremist and populist candidates and targeting specific minorities and vulnerable groups, to serve the wider purpose of undermining the appeal of democratic and equal societies.

Parliament invited the Commission to:

- monitor the impact of foreign interference across Europe and fulfil von der Leyen's commitment to 'address the threats of external intervention' in European elections;
- assess legislative and non-legislative measures that can result in intervention by social media platforms to systematically label content shared by bots, review algorithms to make them as unbiased as possible, and close down accounts of persons engaging in illegal activities to disrupt of democratic processes or instigate hate speech, without compromising on freedom of expression;
- provide funding and support for public awareness campaigns to increase the resilience of European citizens to disinformation.

Members also called for a discussion with Member States on foreign funding of political parties.

In its December 2019 resolution on the implementation of the common foreign and security policy, the Parliament stated that 'disinformation and other forms of foreign interference from external forces poses serious risks for European sovereignty and a serious threat to the stability and security of the Union'. It expressed concern that 'foreign interference from autocratic regimes through disinformation and cyber-attacks on the upcoming general elections threaten Asian democracies and regional stability'. Stressing that 'foreign interference in EU affairs poses a great risk to the EU's security and stability', Members voiced strong support for boosting the EU's strategic communication capabilities and lending further support to the three strategic communication task forces (east, south and western Balkans). They also called for the EEAS Strategic Communications Division to be made a fully fledged unit within the EEAS with responsibility for the eastern and southern neighbourhoods, with proper staffing and adequate budgetary resources, 'possibly by means of an additional dedicated budget line'.

In June 2020, the European Parliament decided by 548 votes to 83, with 56 abstentions, to set up a special committee on foreign interference in all democratic processes in the EU, including disinformation. With 33 members and a term of office of 12 months as of the constituent meeting planned for September 2020, the committee will analyse investigations showing that key electoral rules have been breached or circumvented, especially regarding the transparency of campaign financing. It will also look into the EU's dependence on foreign technologies in critical infrastructure supply chains, including internet infrastructure, such as hardware, software, apps and services, and into the action needed to strengthen capabilities for countering strategic communication. It will suggest coordinated action at EU level for tackling hybrid threats, and countering information campaigns and strategic communication of malign third countries that are harmful to the EU.

ENDNOTE

[1] In his recent book 'Active Measures: the secret history of disinformation and political warfare' (Macmillan 2020), Thomas Rid outlines four big waves of modern era disinformation; the first in the interwar years; the second after World War II; the third in the late 1970s (when disinformation was 'lifted to an operational science of global proportions, administered by a vast, well-oiled bureaucratic machine'; and a fourth emerging in the 2010s, with disinformation 'reborn and reshaped by new technologies and internet culture'.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

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

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

http://epthinktank.eu (blog)