BRIEFING

European Parliament

Foreign influence operations in the EU

SUMMARY

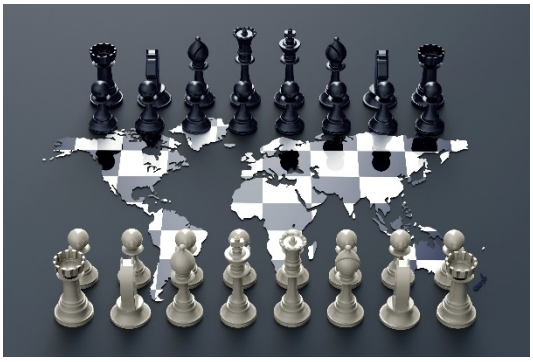
Attempting to influence political decision-making beyond one's own political sphere is not a new phenomenon – it is an integral part of the history of geopolitics. Whereas hard power relies on military and economic force, the soft power of a state involves public diplomacy and dialogue on values, cultures and ideas, which should normally correspond with its behaviour abroad.

Although the extent is hard to measure, democratic states whose values match the prevailing global norms – pluralism, fundamental rights and freedoms, the rule of law as a principle within states and in international relations – and exert this influence by contributing to the prevention and resolution of conflicts, traditionally appear more attractive, thus having more soft power leverage.

However, influence can also serve purposes of interference and destabilisation. Authoritarian state actors struggle to project soft power while engaging in disruptive or destructive behaviour. Instead, some state actors see a means of reaching their goals by making democratic actors, systems and values appear less attractive, through a number of overt and covert instruments.

The tools are constantly evolving. Today, social media combines the oral tradition with new electronic means of dissemination, enabling (potentially disruptive) messages to spread instantaneously. Disinformation can be, and is being, combined with other instruments in an increasingly diverse, hybrid 'toolbox' that authoritarian state actors have at their disposal.

In recent years, awareness in the research community of online disinformation by state actors has increased around the world, not least in the context of the United Kingdom referendum on EU membership and the US presidential election in 2016. Although their visibility increases in the context of elections and referendums, influence campaigns are not limited to democratic processes.



In this Briefing

EPRS | European Parliamentary Research Service

Author: Naja Bentzen
Members' Research Service

PE 625.123 – July 2018

EN

Definitions

Misinformation is information that is erroneous or incorrect, but not intentionally so.

Disinformation is deliberately false information, in particular that supplied by a government (agent).

Hybrid threats are coordinated and synchronised actions that deliberately target democratic states and institutional vulnerabilities, through political, economic, military, civil, and information-related means.

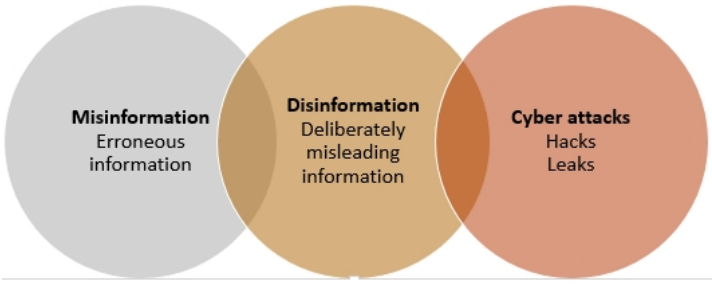
Projecting power: the soft and the sharp approach

Efforts to influence opinion and political decisions beyond one's own territory are an integral part of the nature of power and geopolitics. Genghis Khan and his men planted rumours about their cruelty and the number of their horsemen to spread fear and to weaken the enemy's resilience, long before the printing press made it possible to mass-produce information. Today, social media combines traditional oral communication with new electronic means of dissemination, and enables messages (including false news and disinformation) to spread at the speed of light.

The success of soft power (defined by Joseph S. Nye as 'the ability to affect others through the co-optive means of framing the agenda, persuading and eliciting positive attraction in order to obtain preferred outcomes')[1] as opposed to military power, hinges on communication. Via public diplomacy, a country or an entity 'seeks to build trust and understanding by engaging with a broader foreign public beyond the governmental relations that, customarily, have been the focus of diplomatic effort'. It has been argued that states whose ideas and dominant culture correspond with the prevailing global norms (democracy, pluralism, international rule of law), and whose credibility is underpinned by their values and policies, are most likely to be attractive. By contrast, authoritarian states struggle to balance attraction with disruptive behaviour and/or operations.

Having had limited success with their soft power efforts, both Russia and China – according to a 2017 study by the National Endowment for Democracy – recognise the potential for reaching their goals by making democracy, human rights and fundamental freedoms appear less attractive through 'sharp power' (which some researchers see as 'forced attraction' based on coercion, as opposed to soft power, which is based on attraction and persuasion). At the same time, the focus of leading democratic public diplomacy state actors, such as the US, on countering third-country propaganda, has declined since the Cold War ended (whilst the 9/11 attacks sparked new measures to counter propaganda from non-state actors such as Al-Qaida and, more recently, ISIL/Da'esh).

Figure 1 – Overlapping information disruptions



Source: EPRS, adapted from the Council of Europe, 2017.

'Sharp' influence efforts aiming to undermine the adversary are not new; but the information disruption 'toolbox', which includes a number of often overlapping covert and some overt instruments, keeps growing. New technologies have increased the speed at which disinformation can be spread, for example, often in combination with cyber-attacks (including hacks and selective leaks). The expanding hybrid toolbox also includes assaults, corruption, energy coercion, and ideological and religious influence.

Online platforms as facilitators for 'polarisation entrepreneurs'

Online platforms facilitate the high-speed, large-scale and targeted spreading of conspiracy theories, disinformation and junk news. The attention-based business models often encourage

polarised, emotional debates in which users are automatically fed information confirming existing cognitive biases. The resulting fragmented information sphere inadvertently assists actors who benefit from exploiting wedge issues. The disclosure that user data from Facebook, including that of 2.7 million EU citizens, was improperly shared with consultancy company Cambridge Analytica (which used the data to micro-target and mobilise UK and US voters) reignited the debate on the compatibility of online platforms' business models with the principles of democracy.

Active measures then and now: the case of the Kremlin

History of Soviet/Russian propaganda

It is well documented that the Soviet Union combined covert and overt influence techniques. Soviet leaders saw the conflict with the West as a continuum and did not differentiate between peacetime and war. Active measures, (a translation of the Russian term *активные мероприятия*), disinformation, agents of influence, reflexive control (feeding an opponent selected information to elicit the desired decision), forgeries, propaganda and controlled international front groups were used to target key elite and public audiences to promote Soviet goals. The long-term aim was to stimulate already existing opinion, define the terms of the political debate, 'provide significant ammunition' in that debate, or 'deposit an ideological residue that eases the path for subsequent influence operations'. The intelligence budget for active measures and disinformation was US$3-4 billion annually, involving over 15 000 personnel.[2] In recent years, Moscow has revived and boosted its toolbox, adding new cyber techniques among other means. It has also developed a new ideology to restore 'Russian greatness', including by protecting Russian speakers abroad. According to some analysts, this 'empire of diaspora' relativises borders and creates an 'imagined community' of Russian-speakers seen as an organic part of the Russian cultural nation.

Hybrid attacks on Russia's neighbours

Russia's neighbouring countries have witnessed Moscow's revamped active measures for over ten years. In April 2007, Estonia (a member of both the EU and NATO) was one of the first countries to witness massive cyber-attacks, following the decision of the Estonian government to move a Soviet monument. Protests among Russian speakers were exacerbated by false Russian media reports alleging that the statue, as well as Soviet war graves, were being destroyed. Soon after, Estonia experienced large-scale cyber-attacks for weeks, affecting banks, media outlets and government authorities. One year later, ahead of the conflict in Georgia in 2008, Moscow granted citizenship to a number of Abkhazians and South Ossetians, preparing a 'Russian population' to protect. Moscow justified the incursion as a 'peace operation' to protect Russian soldiers and civilians under attack in Georgia, whereas Georgia asserted that it attacked the city of Tskhinvali in response to shelling from South Ossetia into Georgia, as well as to Russian arms shipments into South Ossetia. Russia's military operation was accompanied by cyber-attacks and disinformation campaigns. Five years later, Moscow responded to Ukraine's Euromaidan revolution and the ousting of Ukrainian pro-Kremlin President Viktor Yanukovich by sending unmarked Russian soldiers to take control of Crimea in March 2014 (President Putin later admitted to deploying troops in Crimea) and launching a hybrid war against the country. In response, the EU has progressively imposed restrictive measures on Russia. Since then, Moscow has used Ukraine as its biggest testing field abroad for disinformation.

Disinformation and cyber-attacks in the European Union

Analysts point out that contemporary Russian propaganda is responsive to events, adapting to the targeted country's local circumstances, narratives and audiences. Russian state media, such as Sputnik and RT, show little commitment to objectivity. As a result, they get a head start in persuading audiences: first impressions are resilient; repetition creates familiarity, and familiarity leads to acceptance. The messages can then be amplified by Kremlin-sponsored trolls and bots, as well as by pro-Kremlin civilians. Narratives that may not resonate with Scandinavians may work well

in Slovakia or other countries with traditionally closer linguistic and cultural ties to Russia. A recent report by the Hague Centre for Strategic Studies notes that Russia's strategic communications have been 'effective in shaping people's perceptions of the EU inside Russia, in the Eastern Partnership (EaP) countries, as well as in the EU itself; particularly among native Russian speakers'.

The EU's East StratCom task force, the Atlantic Council's Digital Forensic Research Lab, and Ukrainian fact-checkers StopFake, are documenting the on-going pro-Kremlin disinformation campaigns. In Ukraine, following the Euromaidan revolution, disinformation campaigns included: denials of Russia's involvement in the illegal annexation of Crimea and Eastern Ukraine; undermining of Ukraine's credibility as an independent state; false news about alleged cruelty by Ukrainians, such as the falsified crucifixion of a three-year old boy by a Ukrainian soldier; and conspiracy theories about the Orange and Euromaidan revolutions being Western plots and the pro-Western government in Kyiv a 'puppet regime'. The 2014 downing of the MH17 passenger jet over Ukraine sparked a wave of conspiracy theories to distract from Russia's involvement. When a Dutch-led investigation in May 2018 concluded that the weapon used to down MH17 had been provided by a Russian military unit, Kremlin and pro-Kremlin actors and outlets launched a new counter-offensive, not only denying Russian involvement, but also dismissing the investigation, calling it 'openly biased and lopsided' and claiming that it solely used 'images from social networks that have been expertly altered with computer graphic editing tools'. However, digital forensic experts in 2016 detected that the Russian Ministry of Defence had itself published altered photos to claim that Ukraine was responsible.

While narratives may differ from country to country, analysts agree that Moscow seeks to undermine unity, destabilise democracies and erode trust in democratic institutions. This pattern has been repeated in the EU: from the influence operations in the run-up to the 2016 referendum in the Netherlands about the EU-Ukraine Association Agreement; continued cyber-attacks to further reduce trust in the wake of the UK EU membership vote; Kremlin-affiliated media promotion of polarising issues during the 2017 German election; and pro-Kremlin bots engaging in a coordinated 'disruption strategy' over Catalonia in 2017, along with Kremlin-backed news platforms. EU Security Commissioner Julian King has openly called the pro-Kremlin disinformation campaign an 'orchestrated strategy' and said that disinformation poses a 'serious security threat to our societies'.

As already noted, disinformation and cyber-attacks often go hand in hand. The Danish Defence Minister in April 2017 said that ATP or Fancy Bear, a group that also gained access to email accounts of US Democrats during the US presidential election, had hacked the emails of select Danish defence staff for two years. He said the hacker group was 'tied to the intelligence services' and 'the Russian regime'.

(Attempted) assassinations accompanied by information campaigns

Disinformation campaigns often accompany violent actions, such as 'wet affairs' including assassinations and kidnappings. A British government inquiry into the poisoning of former Russian intelligence officer Alexander Litvinenko, who was killed in London in 2006 by radioactive polonium-210, concluded in 2016 that President Putin probably approved his assassination. The conclusion was met with a Russian-language Twitter campaign mocking its wording, *#ПутинВозможноОдобрил* ('PutinPossiblyApproved'). The attempted murder of a former Russian spy, Sergei Skripal, and his daughter, on UK soil in March 2018, quickly sparked accusations of Russian state involvement. Prime Minister Theresa May called it 'highly likely' that Russia was responsible for the attack. Reacting to the alleged involvement of Russia's Intelligence Services (RIS) (an important instrument in Moscow's hybrid toolbox and in peace-time most often used in a non-violent way), some 150 Russian diplomats were expelled from Western countries, including 18 EU Member States. In May 2018, British intelligence agency MI5 Director Andrew Parker pointed to the Skripal case as the most recent example of the Russian state's 'now well-practised doctrine' of blending different tools. The attack, he noted, was followed by a 'cynical' information campaign to sow confusion and doubt: Russian state-sponsored media have propagated 'at least 30 different so-

called explanations in their efforts to mislead the world and their own people'. Parker explained that two-thirds of social media output at the peak of the Salisbury story came from Russian government-controlled accounts.

Weaponising migration

Shortly after the migrant crisis started in summer 2015 in southern Europe, waves of third-country nationals without documents began crossing the border between Russia and Norway (the most peaceful Russian border since 1945) on bicycles. In total, 5 465 people entered the country, compared with five asylum seekers in the previous years. The pattern was repeated in Finland, where Russian border guards let a wave of third-country nationals, most of whom had been living in Russia for a long time, leave the country. Traffickers flew them to Murmansk and directed them to the border. This textbook hybrid operation fuelled anti-immigration sentiments and undermined traditional cross-border trust, signalling that Moscow is able and willing to be disruptive.

NATO's Supreme Allied Commander in Europe, General Philip Breedlove, in 2016 accused Russia and Syria of using continuous mass migration as a weapon against Europe. Russia's air campaigns and the Syrian regime's use of barrel bombs against civilians, he said, served the mere purpose of 'deliberately weaponising migration in an attempt to overwhelm European structures and break European resolve'. The migration waves were accompanied by waves of polarising disinformation. In Germany, a false story about a 13-year old Russian-German girl, identified as Lisa, reportedly raped by Arab migrants, was spread in January 2016 from a small website for Russian expats in Germany. It was picked up by Russian-language Kremlin-sponsored mass media as well as by Russian foreign media such as RT and Sputnik. Social media and right-wing groups amplified the story; demonstrations were organised via Facebook, involving representatives of German-Russians and neo-Nazis. Foreign Minister Sergey Lavrov in a public address alleged that information about the case was covered up, warning German authorities not to 'paint over reality with political correctness'. The pro-Kremlin channel NTV claimed that residents in Germany and Sweden 'are regularly raped by refugees … but the local authorities and police hide these facts and do not open criminal investigations'.

Other state and non-state actors are also weaponising migration. The head of the UN World Food Programme has warned that ISIL/Da'esh is conspiring with terrorist groups in Africa (such as Boko Haram and al-Qaida) to create a new migration wave towards Europe, infiltrated by terrorist recruits.

Energy coercion

Scholars have shown that Moscow's use of energy as an offensive or defensive tool of foreign policy dates further back than the collapse of the Soviet Union in 1991 – the Kremlin is said to have interrupted oil supplies to the Baltic States as far back as 1990 in a bid to quash their independence aspirations. By contrast, Moscow has rewarded 'friendly' leaders in Belarus, Ukraine before 2005, and the breakaway regions of Abkhazia, North Ossetia and Transnistria with cheap gas and oil. Moscow's use of its 'petro-stick' has been particularly visible not only in Ukraine, but increasingly also in Belarus. A recent study has found that 15 EU Member States remain dependent on Russia for over half of their gas supplies and that ties with Moscow have discouraged some from supporting more stringent EU sanctions on Russia's gas sector over the illegal annexation of Crimea and its actions in eastern Ukraine. There is concern that the proposed Nord Stream 2 pipeline could make Europe vulnerable to energy coercion. Other energy-rich authoritarian states, such as Azerbaijan, Iran, Libya and Saudi Arabia, are also using energy as a tool of foreign policy.

'Outsourced' influence operations

Moscow's influence operations are, according to experts, often outsourced to an 'adhocracy' of oligarchs, trolls, criminal networks and hackers to minimise or delay the risk of exposing the involvement of the Kremlin. For example, trolls from the Internet Research Agency in St Petersburg are thought to be directly controlled not by the Kremlin but by Yevgeny Prigozhin, who has close

ties to President Putin and is involved in a number of pro-Kremlin projects. Despite this and the trolls' task to flood the internet with pro-Kremlin messages, Putin maintains that the Russian state has 'nothing to do' with the agency and that Prigozhin (who in February 2018 was indicted by the US for his role in the US presidential elections) is acting as a private citizen. Similarly, Putin continues to downplay the role of hackers in cyber-attacks and election meddling, describing them as 'Russian patriots' who 'fight against those who say bad things about Russia', and whom he does not control[3].

Think-tanks and GONGOs

This pattern can also be seen in a more subtle layer of influence, namely the use of academic experts and spiritual leaders to further Moscow's foreign policy objectives. According to a 2017 report published by the Swedish Defence Research Agency (FOI), Russia seeks to influence expert communities, in line with the 2016 Foreign Policy Concept, which encourages the involvement of Russia's academic community, cultural and humanitarian associations in Moscow's public diplomacy efforts. The report analyses the efforts to influence expert communities and public opinion in the West through think tanks and government-organised non-governmental organisations (GONGOs). Institutes specifically targeting English-speaking expert audiences include the Valdai Club (launched in 2004), the Russian International Affairs Council (launched in 2010) and Rethinking Russia (founded in 2015). FOI explains that experts from these think tanks are in high demand as speakers at conferences across the world; their access to Moscow 'adds to their attraction as cooperation partners'. The report concludes that explicitly propagandistic think tanks create networks with 'less mainstream' experts, organisations and institutes in the West.

The power of religion: instrumentalisation of 'spiritual-moral values'

Even during the Soviet era, the Kremlin attempted to influence international religious organisations and further Soviet policy goals through a religious propaganda apparatus. The actions and statements of the regional heads of the local Committees on Religious Affairs were expected to adhere to official Kremlin positions. The oversight process involved the KGB and the Soviet foreign policy structure, such as the Soviet Academy of Sciences Institutes abroad. In recent years, the Orthodox Church has played an increasingly visible role in the Kremlin's narrative. Mass demonstrations in Russia in the winter of 2011-2012 highlighted the need to renew the 'base of support' for the Kremlin. In response, the Kremlin strengthened its ties with the Orthodox Church, promoting a patriotic narrative involving conservative values, according to which the Kremlin protects all Russians against Western moral threats. In 2015, spiritual-moral values were explicitly defined as a matter of Russian national security. The 2015 Russian National Security Strategy suggested building Russia's 'spiritual potentiality … in the polycentric world', and labelled the 'destruction of traditional Russian spiritual and moral values' as a key security threat.

Following the illegal annexation of Crimea in March 2014, Russian forces took control of churches affiliated with the Ukranian Orthodox Church – Kyivan Patriarchate (UOC-KP), which was set up after the Soviet Union collapsed in 1991 and rivals the Ukrainian Orthodox Church – Moscow Patriarchate (UOC-MP). In Crimea, some churches were looted, and UOC-KP leaders were called 'Nazis' (in line with the Kremlin's disinformation narrative about Ukraine) and 'those who broke away'. In April 2018, Ukraine's parliament adopted a resolution to ask the spiritual leader of the world's Orthodox Christians to recognise the autocephaly of the UOC-KP. President Poroshenko hopes that the independent UOC-KP may emerge by the 1030th anniversary of the Christening of Rus celebrated in July 2018. The Kremlin continues to oppose the independence of the UOC-KP.

European responses to disinformation campaigns

Ukraine: lessons from the front line

Striking a balance between countering online disinformation to defend democracy while at the same time protecting freedom of expression appears to be the key challenge facing the EU – a dilemma that is familiar to Ukraine. For example, Kyiv has faced heavy international and domestic

criticism for blocking major Russian websites on the territory of Ukraine in 2017, including internet group Mail.ru and social networks VKontakte and Odnoklassniki, as well as the search engine Yandex and a number of other Russian websites. Council of Europe Secretary Thorbjørn Jagland on 17 May 2017 stated that the 'blocking of social networks, search engines, mail services and news web sites goes against our common understanding of freedom of expression and freedom of the media. Moreover, such blanket bans are out of line with the principle of proportionality'.

Ukraine's move seemed to backfire, not only because it gave Moscow the opportunity to accuse Kyiv of violating human rights, but also because criticism by international human rights watchdogs taint Ukraine's image among its allies, thus playing into the Kremlin's hands. However, international experts argued that – in the light of the on-going Russian disinformation campaigns and cyber-attacks – metadata from the related sites could be used to map political and social preferences. These could be exploited to further destabilise Ukraine and interfere in future elections. The March 2018 disclosure that user data from 87 million Facebook users were improperly shared and used to micro-target and mobilise US and UK voters seems to confirm Kyiv's initial concerns.

The role of civil society in fact-checking and media literacy projects

In terms of civil society engagement in the battle against online disinformation, Ukraine has been a clear front-runner. The fact-checking initiative StopFake, for example, launched in March 2014 by students of Mohyla School of Journalism, has debunked over 1 000 fake news stories. With an audience of more than 180 000 followers on social media and active in 11 languages, StopFake is also analysing data to identify principles, mechanisms and instruments of Russian disinformation. In addition, StopFake is involved in media literacy projects in schools across Ukraine as well as the newly launched international myth-busting portal DisinfoPortal.org.

European Union Member States

A number of EU Member States have responded to recent disruptions in the information sphere by updating and/or increasing their counter-disinformation efforts. For example, the United Kingdom and the Czech Republic have set up separate units to counter disinformation. The Netherlands took significant steps to secure its electoral processes ahead of the 2017 general elections, including abolishing the electronic counting of ballots as well as the use of USB drives and email by election officials, over concern about potential hacking attempts. Similarly, France moved to prevent an election cyber-attack ahead of the 2017 presidential election. In addition, several media outlets, some in cooperation with Google, have launched fact-checking platforms. Attacks on Emmanuel Macron's campaign (spread by Sputnik France, RT, and a network of bots; some of which had been active in the US election campaign) were immediately exposed as an illegitimate effort to sway the election.

Lessons from the US, Germany, France and the United Kingdom have prompted Sweden to take significant measures to counter foreign interference ahead of its general election in September 2018. The Swedish Civil Contingencies Agency has been assessing the threats, and in January 2018 Stockholm announced plans to create a new 'psychological defence' authority to preserve its 'open society's free exchange of knowledge and information' and to identify, analyse and confront influence operations. In a different move, the British House of Commons in May 2018 acknowledged London's role as a 'laundromat' and 'top destination' for Russian oligarchs to hide their wealth, and the direct link between this wealth and the ability of President Putin to execute his 'aggressive foreign policy and domestic agenda'. This prompted a call for a ban on Russian sovereign Eurobonds in London.

The key dilemma: balancing protection and fundamental rights

The debate on legislative responses in Member States reflects the ethical dilemma of protecting the information ecosystem without compromising fundamental rights. A French law to stop manipulated information (passed by the French Parliament on 4 July 2018 and to go into force before the 2019 European elections) will enable authorities to block false information. Also, online

social networks must assume greater responsibility for content and increase their cooperation with authorities. Moreover, the law will authorise the state to close down foreign broadcasters attempting to destabilise France. The law has sparked concern about the impact on freedom of expression, and potential censorship. Germany's Network Enforcement Law came into force on 1 October 2017, enabling the government to fine large social media platforms up to €50 million if they fail to remove unlawful content (including hate speech and fake news) within 24 hours. Despite concern over over-blocking (removal of more content than necessary), no cases have been reported.

EU and NATO: coordinated efforts to counter hybrid threats

In accordance with the July 2016 Global Strategy for the European Union's foreign and security policy, which envisaged stronger ties and cooperation with NATO, as well as the July 2016 EU-NATO joint declaration, EU-NATO cooperation is increasing. In line with the April 2016 joint communication on a joint framework on countering hybrid threats, Finland initiated a new European Centre for Countering Hybrid Threats (Hybrid CoE), inaugurated in October 2017. The decision by 10 EU Member States, Norway and the US to open the centre jointly is in itself seen as a sign that tensions with Russia over its influence campaigns in the West can no longer be ignored. Whereas other centres of excellence have been established under NATO auspices in EU Member States Estonia, Latvia and Lithuania, the Hybrid CoE is the first to link NATO and the EU. The unprecedented level of cooperation between the EU and NATO to address hybrid threats is in line with the July 2017 joint report on the implementation of the joint framework on countering hybrid threats. The Hybrid CoE maintains close contact with the EU Hybrid Fusion Cell, set up within the EU Intelligence and Situation Centre structure and fully operational since May 2017.

Table 1 – EU Member States' participation in key counter-disinformation structures*

EU28	EEAS East StratCom	NATO StratCom CoE	NATO Cyber Defence CoE	EU/NATO Hybrid CoE
Austria			Contributing	
Belgium			Sponsoring	
Czech Republic	Seconded national expert		Sponsoring	Participating
Denmark	Seconded national expert			Participating
Estonia		Sponsoring	Sponsoring	Participating
Finland	Seconded national expert	Partner country	Contributing	Host country
France		Joining	Sponsoring	Participating
Germany		Sponsoring	Sponsoring	Participating
Greece			Sponsoring	
Hungary			Sponsoring	
Italy		Sponsoring	Sponsoring	Participating
Latvia	Seconded national expert	Founding and hosting nation	Sponsoring	Participating
Lithuania	Seconded national expert	Sponsoring	Sponsoring	Participating
Netherlands		Sponsoring	Sponsoring	Participating
Poland		Sponsoring	Sponsoring	Participating
Slovakia			Sponsoring	

Spain			Sponsoring	Participating
Sweden	Seconded national expert	Partner	Future contributing participant**	Participating
United Kingdom	Seconded national expert	Sponsoring	Sponsoring	Participating

* As of 29 May 2018. Sources: the Kremlin Watch; StratCom CoE; Cyber Defense CoE; Hybrid CoE.

** According to the CCDOE's website, 'Sweden is well on its way' to becoming contributing partner.

East StratCom task force

In 2015, the European Council asked EU High Representative/Vice-President, Federica Mogherini, to submit an action plan on strategic communication to address Russia's ongoing disinformation campaigns. As a result, the East StratCom task force was set up in September 2015 under the European External Action Service. However, the (now 14-strong) team has to date been working without its own budget, drawing on the existing EU strategic communication budget and mostly seconded staff. At present, three people are working to collect the disinformation stories (more than 3 800 examples in 18 languages in May 2018), which it analyses, debunks and publishes in its weekly newsletter. Other team members explain and promote EU policies in the Neighbourhood. The European Parliament has consistently supported the East StratCom task force. In its 23 November 2016 resolution on EU strategic communication to counteract propaganda, it called for the task force to be reinforced through 'proper staffing and adequate budgetary resources'. The Parliament has consistently reiterated these calls.

Strengthening efforts to tackle online disinformation

In the EU, responses to foreign disinformation and related influence campaigns fall within a number of different policy areas, including communications networks, (cyber) security and culture.

In a June 2017 resolution, the European Parliament urged the European Commission to analyse the situation and legal framework regarding fake news, and to verify the possibility of legislating to limit its spread. In October 2017, Mariya Gabriel, European Commissioner for the Digital Economy and Society, launched a public consultation on 'fake news and online disinformation' and set up a high-level expert group (HLEG) representing academia, online platforms, media and civil society. In its 26 April 2018 communication on online disinformation, the European Commission issued an action plan and proposed self-regulatory tools to counter online disinformation. The measures include:

- a code of practice on disinformation by online platforms to ensure transparency of sponsored content and clarity about algorithms; close down bots and fake accounts;
- a new European fact-checking network covering factual corrections across the EU;
- an online platform on disinformation to support fact-checkers and researchers;
- media literacy efforts – a European week of media literacy;
- support for resilience of Member States' elections against cyber threats;
- promotion of voluntary online identification systems to improve traceability and identification of information suppliers and boost trust and reliability online;
- action by Member States to boost support for quality journalism. The Commission will launch a call for proposals in 2018 for quality news on EU affairs;
- a coordinated strategic communication policy to counter false narratives about Europe and tackle disinformation within and outside the EU.

The Commission plans the following next steps:

- Following the first meeting of a new multi-stakeholder forum to boost efficient cooperation among online platforms and advertisers, the code of practice on disinformation is expected to be adopted by July 2018. The Commission expects 'measurable impact' by October 2018.
- By December 2018, the Commission will report on progress and examine the need for further action to ensure the continuous monitoring and evaluation of measures taken.

Strengthening cybersecurity in the EU

In September 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) Federica Mogherini published a joint communication on cybersecurity for the EU. The package includes new initiatives to boost EU cyber resilience and response in three key areas: 1) cyber-attacks and the EU's cybersecurity capacity; 2) criminal law response, and 3) strengthening global stability through international cooperation. In order to boost EU resilience to cyber-attacks, a legislative proposal to strengthen the European Union Agency for Network and Information Security (ENISA) was published in September 2017. The 'Cybersecurity Act' proposes expanding ENISA into a fully operational EU Cybersecurity Agency. Other measures include a toolkit for implementing the Network and Information Security (NIS) Directive, a blueprint for effective response in the event of cyber-attacks affecting several Member States, boosting research capacity and developing effective cyber-defence, cyber-hygiene and skills, in Europe and with global partners. In October 2017, the European Parliament adopted a resolution on the fight against cybercrime, urging the EU to invest more in cybersecurity to prevent attacks aimed at critical infrastructure and destabilising societies; to improve information exchange via Eurojust, Europol and ENISA; and to invest in education to address the lack of qualified cybersecurity professionals.

Strengthening the European narrative and identity

In its 2017 communication on strengthening European identity through education and culture, the European Commission called for a political decision on Euronews, with the European Parliament 'closely involved' in the process. In a 2014 resolution on the role of broadcasting media in projecting the EU and its values, the Parliament called for a robust EU media broadcasting strategy to promote freedom of expression, media pluralism, democracy and human rights in and beyond Europe.

The 2019 European elections: preparing responses to disinformation

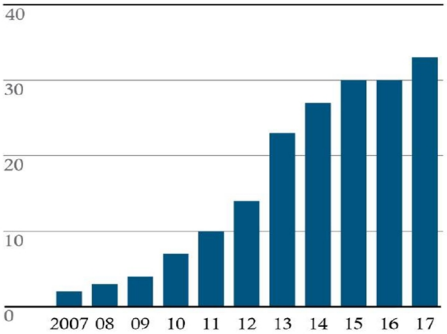
In a January 2018 debate on the influence of Russian propaganda on EU countries, Members of the European Parliament warned that the upcoming EU elections in May 2019 are likely to be the next big target for Russian disinformation. The Parliament has set up a special unit to respond to fake and incorrect information about the institution, in anticipation of the expected increase in such activities. Also with a view to the 2019 European elections, the Commission has encouraged national authorities to identify best practices for identifying, mitigating and managing risks to the electoral process from cyber-attacks and disinformation. In the Cooperation Group established under the NIS Directive, Member States are mapping existing initiatives on the cybersecurity of network and information systems used for electoral processes. European Commission support for Member States in managing risks to the electoral process, not least with a view to the European elections, includes:

- all necessary support, together with ENISA, for the work of the NIS Cooperation Group on cybersecurity of elections. By the end of 2018, the group will deliver a set of recommendations and measures to be implemented by Member States;
- a high-level conference with Member States on cyber threats to elections in late 2018.

Focus on evolving tools and actors

New artificial intelligence-driven techniques such as manipulated sound, images or video ('deep fakes') are on the rise. In the hands of unpredictable actors with substantive cyber capabilities (see Figure 2), increasingly challenging scenarios could emerge.

Figure 2 – Countries with cyber-attack capabilities



Source: DNI world threat assessment 2018.

At the same time, existing tools are (re-)activated. Turkey has repeatedly mobilised its diaspora for political gains. Prior to Germany's 2017 general election, President Erdogan discouraged German Turks from voting for Angela Merkel's Christian Democratic Union, the Socialists and the Greens, calling them 'enemies of Turkey'. He urged Turks to vote for 'parties who are not enemies of Turkey'. Ahead of the presidential election in in June 2018, Erdogan was banned from holding rallies in EU Member States Germany, Austria and the Netherlands, home to large Turkish diasporas. Instead, he held a rally in Sarajevo, Bosnia-Herzegovina (BiH), in May 2018, bringing in some 10 000 supporters from EU Member States and attracting another 10 000 Bosniaks. The move to rally in BiH reignited concern over Erdogan's ability to reactivate Turkey's deeply rooted influence efforts in the Balkans. Russia has long used ethnic Russians abroad as an influence tool and a pretext for military action. Experts recommend supporting Russian-language media outlets to engage with these minorities.

China's influence efforts in and beyond Europe

Under Chinese President Xi Jinping, Beijing has expanded its global information strategy, increasing its efforts to influence political and economic elites, media, public opinion, civil society and academia in liberal democracies across the world. According to a February 2018 report by the Global Public Policy Institute and the Mercator Institute for China Studies, Beijing (like Moscow) is seeking to weaken Western unity. China – promoting its own political and economic system as a 'viable alternative to liberal democracies' – is attempting to build global support on specific policy issues via 'layers of active support' in academic, political, media and business circles. The report warns that EU Member States are increasingly adjusting their policies to 'curry favour with the Chinese side'. China's divide and rule tactics have borne fruit in the area of liberal values and human rights, the report asserts, as European elites are increasingly embracing Chinese rhetoric and interests.

The 16+1 format (a group of 16 central and eastern European countries launched in 2012, initiated and led by China) has sparked concern over the strategy behind Chinese investments in poorer European countries. China allegedly views central Europe as 'an avenue through which it might influence EU decision making', to secure compliance with the One China policy through pressure to limit contact with Taiwan, the Dalai Lama and Uyghur groups in return for infrastructure projects such as the Hungary-Serbia railway and similar investments in the Western Balkans as part of Beijing's Belt and Road Initiative. Further south, Greece has become a key Chinese investment target since the financial crisis, with the port of Piraeus as a hub for an 'informal web of Chinese companies'. Some see the decision of Greece, Hungary and Croatia to oppose criticism of China in a 2016 EU statement on the South China Sea Dispute as dictated by China in return for investments. In June 2017, Greece blocked an EU statement to the UN that criticised China's human rights record.

Media and academic activities

In 2015, Reuters mapped a list of radio stations worldwide, including in Finland, Italy, Hungary, Romania, and the Western Balkans, that are part of networks backed by the Chinese government and broadcast pro-Beijing programming. In addition, Chinese state broadcaster China Global Television Network (CGTN) is reportedly working to recruit over 350 journalists in London, as part of its plans to establish a European hub of operations. In one job advertisement, CGTN said it aimed to report on 'nations, regions, and stories often ignored by western media' from a Chinese perspective.

In the 'soft' academic sphere, China has established 516 Confucius Institutes (CIs) in 142 countries around the world, including in the EU. The Office of Chinese Language Council International (Hanban) typically funds the establishment of the CI, providing teachers and material, whereas the local university provides infrastructure, administration and management. CIs promote Chinese language and culture, including the official Chinese narrative on Tibet and Taiwan, which often clashes with academic research at the hosting institutions. Some critics assert that CIs work to spread a favourable vision of the 'China model' of development, silence discussions about issues censored in China (such as the Tiananmen Square massacre) and 'correct' the perception of China as a hard authoritarian state that violates human rights. In Sweden, the Stockholm University CI (established in 2005 as the first CI in Europe) was closed in 2015 following criticism from staff and the public.

Asia-Pacific democracies seek stronger cooperation with the US on Chinese influence

Outside Europe, Western democracies such as the US, Australia and Canada are increasingly scrutinising Chinese influence operations and vehicles. The Canadian Association of University Teachers in 2013 urged Canadian universities and colleges to close down their Confucius Institutes. In 2014, the American Association of University Professors recommended the same for US universities. In 2017, the US National Association of Scholars urged all universities to close their Confucius Institutes. US lawmakers in January 2018 introduced a bill on Countering the Chinese Government and Communist Party's Political Influence Operations Act, requiring investigations and a subsequent unclassified report. The bill would require CIs to register as foreign agents. Australia (one of the first countries to recognise the challenges of Chinese influence) in 2017 announced a ban on foreign donations to political parties, and is scrutinising foreign investments with potential national security implications. A May 2018 report by the Canadian Security Intelligence Service said that Australia, Japan, New Zealand and the US are seeking stronger cooperation to address China's influence, as anxiety about the challenges is 'clearly deeper' in these countries than in the EU.

The European Parliament's Committee on International Trade (INTA) on 28 May 2018 adopted its first reading report (rapporteur: Franck Proust (EPP, France)) on the Commission's proposal for a regulation establishing a framework for the screening of foreign direct investments (FDI) into the EU, including in critical infrastructure and technologies (for example, election infrastructure). The INTA amendments seek to extend the scope of the Commission's proposal to include FDIs that might affect media independence or the EU's strategic autonomy, threaten security or public order, or lead to a monopoly. On 13 June 2018, plenary confirmed the decision to enter into interinstitutional negotiations.

Outlook

The multifaceted nature of the challenges of foreign disinformation and related influence efforts require correspondingly multifaceted responses. The growing visibility in the EU of mainly pro-Kremlin online disinformation has produced a range of different solutions and proposals. With an increasing number of state and non-state actors attempting to impact and/or undermine decision-making in the EU – paired with the rapid evolution of means and methods – a growing number of Member States, sectors and policy areas will likely be affected by these developments. These evolving foreign influence operations call for a broader European and interdisciplinary approach.

ENDNOTES

[1] J.S. Nye, *The future of power*, PublicAffairs, 2011, pp. 20-21.

[2] K.N. McCauley, Russian influence campaigns against the West, 2016, p. 3.

[3] See also T. Maurer, 'Cyber proxies and their implications for liberal democracies', *The Washington Quarterly*, 2018.

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)