Russia's Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies?

Eugene Kondratov and Elisabeth Johansson-Nogués

PhD program in Politics, Policies, and International Relations, Universitat Autonoma de Barcelona, Cerdanyola del Valles, Spain; Institut Barcelona d'Estudis Internacionals, Campus UPF, Ramon Trias Fargas, 25-27, 08005 Barcelona, Spain.

yevgeniy.kondratov@autonoma.cat; ejohanssonnogues@ibei.org

This research was supported by project "Visions and practices of geopolitics in the European Union and its neighborhood" (VISIONS) [grant number CSO2017-82622-P]; Ministerio de Ciencia, Innovación y Universidades, Spain

Russia's Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies?

Abstract: *This article examines the Russian government's use of the cyber and information domains as arenas to challenge liberal democracies. Previous studies have examined the technical or military-strategic aspects of Russian cyber activity or (dis)information. This article builds on these efforts and extends the scope of analysis to examine the socio-political challenge of Russian 'hybrid interference' for liberal Western democracies such as France, Germany and the UK. Our case studies highlight Russia's growing use of cyber operations combined with (dis)information to foment or exacerbate tensions between government and society and/or among different societal groups. Our findings suggest that while Russia utilises hybrid interference to create or augment inter-societal turbulence in the short-term, the longer-term effect might serve to erode horizontal and vertical trust in such societies.*

Keywords: Russia, cyber-attacks, (dis)information, trust, France, Germany, the UK

Introduction

Western countries have become increasingly concerned about new developments in the cyber and information domains. During the last decade, the number of cyber-attacks and malicious cyber practices coordinated by foreign actors has been on the rise in many Western democracies worldwide. Commercial espionage, for example, as well as hacking into governmental websites or email communication flows, have become areas of growing activity and thereby apprehension. More recently, negative information- or disinformation campaigns against determined Western political leaders or democratic institutions have also occurred with periodic frequency. The intensification of such (dis)information efforts has caused some to quip that Western countries appear to be gripped by an 'infodemic' (European Commission 2020).[1] These developments in the cyber and information spaces are perhaps not new phenomena (Rid 2020). However, the volume, sophistication, and channels of such foreign interference in recent years have decidedly changed their scope, form, method, and, consequently, their associated socio-political challenge for Western countries (European Parliament Policy Department 2021, Hague Center for Strategic Studies 2019, Monaghan 2019).

The reaction in the affected countries to the increased cyber- and (dis)information interference into their respective domestic contexts reveals a perception of heightened vulnerability. Western democracies have been quite unprepared for the onslaught of such activity by foreign actors, creating pressure on Western governments and societies only potentially comparable to that of the Cold War era. It has also been alarming for Western countries that analysts and official governmental inquiries have yielded trace events that indicate that the majority of hybrid interference activity is perpetrated by a mix of state and non-state actors based in or linked to two particular global actors: Russia and China (Estonian Foreign Intelligence Service 2018; Limnell

[1] (Dis)information is defined here as composed of a range of information typologies. The concept spans everything from correct and factual information, to propagandistic and negatively biased, all the way to outright false and deceptive information. The more sophisticated (dis)informers employ a mix of these at any given time.

2018; Vilmer et al. 2018; Karlsen 2019; UK Government 2020). Hence, rather than being a diffuse threat committed by small, socially marginal groups or individual anonymous hackers, as had been the norm in previous decades, today's cyber actions appear to follow clear and concerted methods as part of a more aggressive foreign policy and/or military strategy issued by determined state actors (Bechis 2021, Thomas 2019, Vilmer 2018). The dilemma that such interference poses for targeted Western societies is that the activity is frequently challenging to attribute, control and/or counter in contexts where freedom of expression and unregulated access to social communication networks are highly valued. For some Western governments or societies, the insidiousness of (dis)information or malicious cyber activity also lies in foreign actors' attempts to establish direct contact with target Western audiences by informal means of communication as well as their active attempts to shape public opinion to sow or exploit social divisions (Dowling 2021; Henschke, Sussex, and O'Connor 2020). Their actions, therefore, have come to be viewed as an effort to undermine Western societies and institutions, which are based on democratic values, human rights, and the rule of law (European Parliament 2016).

This article will focus on the 'hybrid interference' of the Russian Federation's state and semi-state actors into three Western European countries: France, Germany and the United Kingdom, since 2014. We are particularly interested in the socio-political dynamics of cyber operations and (dis)information on targeted societies, and in our cross-case analysis, we unpack why such action is seen as a threat to Western European societies and their respective institutions. In the first section, we will map out and advance our understanding of hybrid interference by examining how Russia employs cyber operations combined with (dis)information against Western governments and/or societies. We will also introduce our conceptual framework based on 'trust.' In the second section, we will outline the various cases in which Russia has exerted hybrid interference in France, Germany and the United Kingdom. Finally, we will analyse the socio-political challenges created by Russian hybrid interference in these three Western European democracies and how that interference affects levels of trust within these societies.

Hybrid interference, Russia, and trust

Hybrid interference refers to a combination of economic, political, cyber and information means, which are overtly or covertly used to achieve strategic objectives without the extensive use of military power or physical violence. Such (c)overt means of interference can involve destabilising cyber operations, disseminating biased or false information, infiltrating opinion-makers, financing anti-government groups, or discrediting political actors (Wigell 2019). Hybrid interference can also encompass selective targeting or grooming of determined social groups to curry favour with the foreign actor's point of view. Here we will employ hybrid interference in a more limited sense, as we aim to examine Russian activity in the spheres of cyber-attacks and (dis)information operations.

Russia's modern use of hybrid interference has its roots in the times of the Soviet Union. 'Active measures' – as it was known in this period – included several features, such as deception, the art of manipulation, and negative propaganda. Active measures were steadily refined throughout the Cold War and became professionalised in the 1970s (Abrams 2016). Then Soviet state security agency KGB's highest-ranking defector to the US, Maj. Gen. Oleg Kalugin described active measures as the 'heart and soul of Soviet intelligence' and stated that these practices were designed to 'weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies…' (Kalugin 1998). Before becoming President of the Russian Federation, Vladimir Putin was a career operative of the KGB. Every KGB agent of the First Chief Directorate (foreign intelligence) was reportedly required to devote 25% of their time proposing new ideas for false and negative information campaigns (Boghardt 2009). Since coming to power in 2000, Putin has continued to embrace active measures, first to suppress internal opposition (Zafesova 2021) and later used externally to meet his government's geopolitical objectives (Bechis 2021). However, such practices have been modified to fit the digital information age and new modes of popular social communication, morphing into what we now call hybrid interference (Ball 2017). Putin's support for hybrid interference is part of a multipronged Russian foreign and security policy, whereby indirect, non-lethal actions, partly based on information-psychological influence, have become an important pillar alongside traditional military or diplomatic means (Rzheshevsky 2005). Three consecutive Russian security doctrines mention the importance of cyber and (dis)information superiority for Russia as domains of global competition and urge the intensified use of hybrid interference as a means of foreign and security policy (President of the Russian Federation 2009, 2015 and 2021).

The importance of cyber and (dis)information operations to Russian foreign and security policy is echoed by the growing number of actors involved and the resources devoted to hybrid interference into Western democracies (UK Government 2020). One can conceptualise the involvement of different types of actors in Russia's hybrid interference operations as an ecosystem. The hybrid interference ecosystem relies on several state and semi-state actors (e.g., security or military intelligence agencies, state media and proxies, as well as privately-owned companies), which act in parallel to each other without much coordination, but with the explicit or implicit consent of the Russian political and military leadership (Bodine-Baron et al. 2018). The different actors of the hybrid interference ecosystem intervene in different ways. Some focus on extracting information through cyber-attacks or creating social media accounts and bots. Yet others produce content for (dis)information platforms and send it to various types of consumers, including ordinary citizens, journalists, and political decision-makers, whether inside or outside Russia. The output of this ecosystem reflects what Laruelle (2021) considers the ideological plurality of the Putin regime, whereby (dis)informational content sourced from varying ideological viewpoints is produced by competing Kremlin-linked political actors in the hope of having their agendas adopted at higher levels within the Russian presidential administration. This insight is consistent with the findings of Taylor (2018) on the role of competitive informal networks and their influence on the system of governance in Russia.

The ecosystem includes actors such as the Russian security services (the FSB and the GRU), which are central components in acquiring and manipulating information in Western societies through cyber operations (Aaltola 2017). The FSB was initially responsible for internal security. However, in the past several years, its role has expanded to include foreign intelligence collection and offensive cyber operations (Congressional Research Service 2021). The GRU is the Russian government's military intelligence agency and controls several institutes that develop hacking tools and malware. Besides these two agencies, the Russian government has an independent directorate, as part of the Presidential Staff of the Russian government, charged with coordinating countrywide (dis)information activities, including shaping Russia's favourable image abroad (Blank 2016). Russia Today (RT) and Sputnik are the two primary Russian state-funded media outlets serving content to non-Russian speakers outside Russia. Both outlets have television channels, websites, and social media accounts on all major platforms where they serve content in several languages, including English, French, and German (Global Engagement Center 2022).[2] Besides state-funded agencies, semi-state actors have also become involved. One of the more active entities is the Internet Research Agency (IRA), founded in 2013 by the prominent oligarch and Putin associate Yevgeniy Prigozhin (Vilmer 2018).[3] The IRA, based in St. Petersburg, is considered a 'troll factory,' i.e., a facility that employs hundreds of staff to write and diffuse false information across the internet. It does so with the assistance of software known as bots, whose role is to perform simple, repetitive work, such as rapid replication and deployment of messages.

Various explanations have attempted to clarify the political challenge and risk hybrid interference represents for Western democracies. Some analysts have focused on the alleged military or geopolitical challenges underlying Russian interference. It has been argued that Putin's strategy can be seen as retaliation for what some in the Russian regime perceive as the Western powers' encouragement, in the past decades, of anti-government protests and the fomentation of regime change in Eastern Europe as well as in Russia itself (Wigell 2019). Russia's Foreign Minister, Sergei Lavrov, has commented that EU member states are 'an elite club' using the extension of the liberal world order as an instrument of 'domination over everyone else' (Lavrov 2017). The Russian foreign and security policy towards the West is thus conditioned by a confrontational and zero-sum logic, where allegedly, anything the Russian Federation can do to damage the interests of the West is permissible (UK Government 2020). The Kremlin is perceived to act upon the belief that an undemocratic world order where relative military strength bestows great power legitimacy is in Russia's favour (*ibid.*). Such findings are corroborated by academics, such as Tsygankov (2019), who argues that Russian hybrid interference is a method to strengthen its global bargaining position, foment increased multipolarity, and reduce Western dominance in the current world order.

Another set of scholars has set about to explain Russian hybrid interference as a much more contained phenomenon and limited to specific objectives inside targeted countries within the West. Such Russian interference has, for example, been attributed to the goal of the manipulation of third

[2] Sputnik and RT primarily serve German-speakers via their YouTube channels due to their failure to meet the requirements to obtain German television broadcast licenses.

[3] Prigozhin can be described as an individual oligarch who acts as an 'entrepreneur of influence' by investing his own 'money or social capital to build influence abroad in hopes of being rewarded by the Kremlin' (Laruelle and Limonier 2021). Prigozhin is not only the main financier behind IRA, but also finances the private military company The Wagner Group which has operated in various conflicts around the world.

states' strategic interests (Wigell 2019) or to a will to impose the Russian worldview, values, and interests on a target society's audience through a variety of means (Bartosh 2018). Kallberg (2020; see also Meister 2016) claims that Russian influence operations are an attempt to make Russia seem relevant to citizens of target countries by presenting itself as a significant player able to influence domestic processes and contrasts it with a West that is naïve, weak, and full of socio-political cleavages that may be easily exploited. Yet another set of authors, Mahairas and Dvilyanski (2018; see also Hammond-Errey 2019), see the key objective of digital influence operations as contaminating and overloading the information space with so many perspectives that the audience becomes confused and consequently erodes the latter's sense of critical thinking. Aaltola (2020) interprets Russia's actions as an attempt to interfere within the West's political processes, thereby further weakening democracies and possibly fanning populist and/or autocratic tendencies. Building upon these studies, we aim to combine some of their insights and hone in on a specific subset of hybrid interference – cyber and (dis)information – with the ambition to obtain an analytically clearer explanation of Russian activity in determined Western countries.

We posit that Russia's hybrid interference into Western European democracies is fundamentally linked to the sense of increased vulnerability that such interference generates in the latter societies. Our conceptual framework is therefore centred on liberal democracy's fundamental touchstone – trust. Trust is one of the essential elements that allows democracies to function effectively (Nannestad 2008; Putnam 1993; Uslaner 2002) and allows pluralistic societies to resolve their differences peacefully (Putnam 1993).[4] Trust is considered to be essential for various actions supportive of a healthy democracy, including participation in informal social networks, voluntary associations, and civic acts, such as voting (Putnam 1993, 2000). Such acts are theorised as elements of what Putnam (2007) considers 'bridging capital'; they serve to overcome social cleavages, such as race, religion, and ethnicity, which are commonly found in heterogeneous Western democracies. Higher levels of trust are both a cause and effect of the development of these acts of bridging capital. As an example, a society that cultivates higher levels of trust may see the creation of more voluntary associations. In turn, these types of voluntary associations may themselves cultivate higher levels of trust. The concept of bridging capital is part of a larger concept known as social capital, which Putnam (2007) conceptualises as the cultivation of 'social networks and the associated norms of reciprocity and trustworthiness.' Trust may thus be considered 'the glue that joins society together and the oil that facilitates its smooth operation' (Newton, Stolle, and Zmerli 2018).

Here, we distinguish two types of trust inherent to liberal democracies: vertical and horizontal. *Vertical trust* refers to trust between citizens and their democratically elected institutions and is considered the basis for Western liberal and plural democracy (Delhey, Newton, and Welzel 2011). Vertical trust is likely to exist in contexts where citizens perceive government institutions as fair and functional (Berg and Johansson 2016). A further unpacking of vertical trust also reveals that

[4] However, we also recognize that both types of trust exist within a network of other variables and may also be affected by levels of corruption as well as cleavages surrounding class, education, ethnicity, national wealth, or income equality (Uslaner 2018).

citizens' confidence in institutions may vary. Trust toward more neutral institutions (courts, police, civil service) tends to be stronger, while trust in political institutions (legislature, political parties, leaders) tends to be weaker (Zmerli and Newton 2017; Rothstein and Stolle 2008). With *horizontal trust,* we refer to individuals of a society trusting each other in their coming together in the democratic marketplace of ideas and the functioning of their political community (Uslaner 2002). Horizontal social trust requires inhabitants (citizens and residents) to accept each other as rightful participants in the political process or community, regardless of individual characteristics (Griffin 2015).

Horizontal trust is linked to vertical trust in that if the public believes that their institutions do what they are supposed to do in a fair and unbiased manner, they may also tend to develop trust horizontally in their fellow citizens (Rothstein and Stolle 2008). Vertical and horizontal trust rely on each other, and thus, due to this link, eroding one risks negatively affecting the other. These links may be further eroded through a process known as 'truth decay.' This refers to a constant stream of (dis)information that prohibits citizens from being adequately informed and debating important topics in society (RAND Corporation 2018). This debilitating process is further augmented by foreign actors using cyber and technical means to disrupt the normal functioning of information and infrastructure systems, allowing truth decay to transform into declining trust for formerly respected sources of information (RAND Corporation 2018). When that happens, meaningful discourse and debate are not only degraded horizontally with other members of society but also vertically with government leaders, who these citizens are supposed to elect, communicate with, and monitor as they carry out their public duties. Together, the wedges created by eroding the bonds of horizontal and vertical trust risk undermining the essential foundations of a democratic society.

Scholars have regularly noted that the benefits of Western liberal democracies have become increasingly questioned in the last decade, and the vertical trust, or social contract, between government and its citizens has weakened. Studies by the OECD show that trust in governments has declined in most OECD countries in the last decade. In 2020, only 51% of people, on average, trusted their governments (OECD 2021). Persistently low election participation, voter turnout (Dalton 2004), polarisation and politicisation of public policy, as well as the rise of populist parties are some of the manifestations of the current perceived level of relative distrust in the traditional institutions of Western liberal democracy (Wike and Fetterolf, 2018). This echoes findings on sovereignty by Agnew (2017), who argues that power and space are today more networked rather than contiguous, grouping scattered hierarchies of polities rather than a single uniform state. The crisis of Western democracy has thus led to a certain erosion of vertical trust, creating friction between government and citizens and among different civil society groups. The 'effective sovereignty' or governance exercised by the state is thus undermined, as the former relies on the willing participation of state-based, corporate and societal actors, among others (*ibid*.). The disaffection for politics and/or traditional channels of information has turned the public toward direct democracy instruments, such as referenda and offline or online citizen initiatives (Setala and Schiller 2012), in their quest to satisfy their demands for more participation (Christensen 2017). The digitalisation of popular initiatives – whether in discussion forums or calls for street demonstrations – has created unmediated and instant communication channels among citizens, further supporting their alternative political organisation and their cause.

As informal and social media has increasingly become a key channel for public discourse in Western democracies, foreign actors have seen an opportunity for a possible means of influence over political activity in such countries (Norri-Sederholm et al. 2020). This has turned social media into a high-stakes environment where influence campaigns by foreign actors can impact the perception of how trustworthy democratic institutions are (Pamment et al. 2018) and/or act to erode not only weak ties among different groups in society but also strong ties, such as those of family and close friends (Asmolov 2018). Hybrid interference thus acts by applying further pressure on existing political pressure points—such as anti-government and anti-establishment sentiments or religious, economic, or ethnic intra-societal frictions — which in turn affects the credibility of the government (vertical trust) and/or promotes or exacerbates divisions among different groups of society (horizontal trust). The danger posed by (dis)information relates to its ability to distort the domestic preference formation and agenda-setting phases of democratic deliberation. Dowling (2022) concludes that such activity, or even the perception of interference, has the potential to undermine the trust that is indispensable for the functioning of a modern democratic political system. Cyberattacks, when used in conjunction with disinformation as part of hybrid interference campaigns, serve the purpose of undermining trust. According to Brangetto and Veenendaal (2016), cyberattacks have a dual nature in influence operations; technically, they may change, compromise, steal information from, or destroy various systems, and psychologically, they contribute to undermining trust and confidence in the governments of targeted states.

Methodologically our research relies on a cross-case study of three of the most prominent cases of Russian hybrid interference in Western Europe in the period encompassing 2014 to 2021: France, Germany and the UK. Our main data are sourced from reports compiled by independent and renowned data forensic laboratories, although we supplement with secondary literature. We would, however, like to echo the disclaimer from these same forensic laboratories of the difficulty of obtaining trace information from social media platforms, which in essence makes attributing actions with complete certainty in the digital domain difficult. Moreover, the fact that some of the incidents in the cases described below were detected long after they had happened and the hybrid interference actors were able to remove information that traced back to them, makes independent verification beyond the information supplied by the cited data forensic laboratories impossible.

Russian hybrid interference in the UK, Germany and France

This section outlines the Russian hybrid interference campaigns in France, Germany and the UK. The Russian cyber- and informational meddling in Western countries have noticeably increased since 2014. The year marked a particularly low point in Russian-Western relations as a consequence of the former's actions in Crimea and eastern Ukraine and the latter's diplomatic and economic sanctions against Russia (Casier 2020). The order of the country studies below responds to a chronological account of Russian hybrid interference in Western Europe, which began with the Scottish referendum on remaining in the UK. We observe that the modus operandi of the Russian interference has been very similar in all three countries. Russia primarily spread (dis)information through social media, with the assistance of automated botnets, and supplemented it with its traditional media and cyber-attacks on critical infrastructure, such as telecommunications.

United Kingdom

In the United Kingdom, there has been a pattern of Russian hybrid interference which has evolved significantly in sophistication since 2014. That same year, constituents in Scotland voted on whether to remain in the UK or not. In the aftermath of the vote, a video entitled 'Elite NWO Agenda' began circulating on YouTube, and after being shared by 671 users, a dozen of whom were confirmed to be pro-Kremlin trolls, it eventually went viral. The video received 800,000 views from people interested in the Scottish referendum. The video alleged that fraud had been committed in the Scottish referendum through vote-rigging, and the commentary also introduced doubts about the integrity of the electoral process (DFRLab 2017). In a similar video, widely circulated by a Russian troll network (Rose 2016), images were shared of vote-engineering purported to take place during the Scottish referendum, although the video had actually been filmed in Russia in 2012 (DFRLab 2017). In addition to the two videos, an opinion from a purported election observer and expert was disseminated in British media, appearing to lend credibility to the claims of a compromised vote. This expert, Igor Borisov, of the state-funded Russian Public Institute of Electoral Law, gave an interview to a relatively unknown publication stating that the Scottish referendum was not following international law. The story was then picked up by the British newspaper *The Guardian* and received widespread attention; it was read 790,000 times in just two days (Ostanin and Rose 2016). The fraud claim led to several online petitions, including one asking for recognition of Scottish independence, a call for a public judicial review, and two other calls for a revote, which appeared on the official UK Parliament's petitions page. One Facebook group, called 'Rally for a Revote,' posted invitations for local protest events in Scotland and collected more than 100,000 signatures for a petition demanding disqualification of the referendum result and a revote (Ostanin and Rose 2016). After the British government concluded that Russia had deliberately contributed to stirring public passions on the Scottish referendum (UK Government 2020), the defence spokesperson of the Scottish National Party, Stewart McDonald, stated that the UK's national security strategy must be updated to make defence against (dis)information a central priority (Percival 2021). He further elaborated that he believes this interference reveals how vulnerable society is to 'self-reinforcing feedback loops of distrust and disinformation that tug at the threads which hold our communities together' (McDonald 2021).

Two years later, in the context of the 2016 UK European Union membership referendum (Brexit), Russia utilised social media to spread (dis)information. Gorodnichenko, Pham, and Talavera (2021) analysed 28.6 million Brexit-related tweets and found that twenty percent of users in the sample were bots. Further, 45,000 tweets about Brexit were sent 48 hours before the election deadline, and 150,000 accounts based in Russia were involved in these actions (Mostrous 2017). In the 24 hours before the vote took place, Russian-affiliated accounts broadcasted messages overwhelmingly supportive of Britain leaving the European Union, with 1,102 posts using the hashtag 'ReasonsToLeaveEU' (Field and Wright 2018). These Russian-affiliated accounts continued to post immediately after the vote took place; the top retweets originating from these accounts included messages such as 'This is the simplest explanation. Just like UK we too want to stop globalist liberals from ruining us #BrexitVote', 'UK has no masters UK is free,' and 'Brits MADE UK Great Again.' In addition, some of these accounts attempted to introduce an element of racism and hostility toward those of North African and Muslim origin, with posts such as 'Algerian illegally in Britain attacked 8 women in ten days! Send the Muslim back to EU! #BrexitVote' and 'I hope UK after #BrexitVote will start to clean their land from muslim [sic] invasion!'. Further, whereas during the pre-Brexit period, these accounts produced content targeting specific societal fears of an influx of migrants, in certain post-Brexit tweets on the subject of Islam, they exploited societal tensions over the 2017 London and Manchester terror attacks, with tweets including 'Just a gentle reminder that the Mayor of London Sadiq Khan called moderate Muslims "Uncle Toms"' and '7 more dead in London because of climate change. Oh, wait, nope, it's Islamic terrorism again. #London Attacks' (Demos 2018).

The social media (dis)information campaigns were complemented by a hybrid strategy whereby Russia's traditional media echoed the social media (dis)information campaign's overwhelmingly right-wing sentiments, providing an additional voice of support for the Leave campaign. The Russian state-funded English-language stations, Russia Today (RT) and Sputnik, emitting in the open in the UK, conducted a 'systematically one-sided coverage' whose effect was to magnify the Leave Campaign and marginalise the Remain campaign (Nimmo 2016). The one-sided reporting included running overwhelming negative headlines of the Remain campaign's principles, quoting a disproportionate number of Leave campaigners, and stand-alone stories on comments by prominent British Eurosceptics such as Nigel Farage and Patrick Minford. The Broadcasters' Audience Research Board estimated that the weekly audience viewership of RT in Britain for the period during the Brexit referendum (20-26 June 2016) was 926,000 (BARB 2016).

In 2017, 90 email accounts belonging to various staff and members of the British parliament were hacked, and data were stolen (MacAskill and Syal 2017). Martin Ciaran, the head of the UK's National Cyber Security Centre, would late reveal that besides the attack on the British parliament, the country's media, telecommunications, and energy sectors were continuously being attacked, and Russia's GRU was attributed as the alleged perpetrator. Some examples of attacks include an August 2015 incident involving a UK-based television station, a March 2018 attempt to compromise the systems of the Foreign and Commonwealth Office, and an April 2018 attempt to gain access to the UK Defence and Science Technology Laboratory's computer systems (UK Government 2018). The combined cyber and (dis)information attacks led the British PM, Theresa May, to accuse Russia of interfering and planting stories to create discord in the West, and declared:

> I have a very simple message for Russia. We know what you are doing. And you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of western nations to the alliances that bind us (cited in Mason 2019).

In the 2019 UK General Elections, social media companies and investigators uncovered further evidence of ongoing Russian hybrid interference in Britain.[5] First, evidence suggests that Russia sought to spread (dis)information through social media to create divisions between Ireland and the United Kingdom, targeting the contentious negotiations over border controls in post-Brexit Northern Ireland. As part of the investigation into interference tied to Russia's hybrid campaign known as Operation Secondary Infektion, Facebook identified at least one account that belonged to the Russian (dis)information campaign. This account posted an article to Medium and fifteen other websites which falsely claimed that then-British Defense Secretary Gavin Williamson accused the Real Irish Republican Army (Real IRA), a paramilitary organisation fighting to unify Ireland, of assisting in the assassination attempt against a former Russian spy and British military informant, Sergei Skripal. In another attempt to inflame tensions between Ireland and the UK, an additional article used a forged leak, allegedly written by Arlene Foster of Northern Ireland's Democratic Unionist Party, to suggest that her party found the EU's position favourable and warned of a bloody confrontation in Ireland because of tensions over a possible hard border (Atlantic Council 2019). A third example of Russian interference in the elections was a set of – this time genuine – leaked documents which revealed correspondence between American and British officials in the context of the Brexit vote. The documents highlighted US pressure to change how drugs were priced through the UK's National Health Service and included discussions about drug patents, medical devices, and other politically sensitive topics. Both Reddit and the analytics firm Graphika detailed how the leaks and subsequent spread of the information were typical of Russian tactics (Reddit 2019; Nimmo 2019).[6] The leaked documents caused tension between the Conservative-led British government and the Labour opposition party as its leader, Jeremy Corbyn, used the revelations to accuse the government of a 'plot' to sell off part of the National Health Service to the United States (Hurst 2019). The Northern Ireland and US-UK correspondence incidents prompted UK Foreign Secretary Dominic Raab to declare that 'Russian actors sought to interfere in the 2019 general election through the online amplification of illicitly acquired and leaked government documents' (Sabbagh 2020). In their 2020 report, the Intelligence

[5] There is evidence that this British campaign was linked to a larger Russian global (dis)information campaign, Operation Secondary Infektion, a 'large scale influence operation that spanned nine languages, over 30 social networks and blogging platforms, [and] scores of fake user profiles and identities' (Atlantic Council 2019).
[6] According to Nimmo (2019) the leaked posts on Reddit were later amplified by at least 61 accounts linked to Russia.

and Security Committee of the British Parliament assessed that Russia's cyber capabilities and actions, in combination with their willingness to deploy them 'is a matter of grave concern and pose an immediate and urgent threat to our national security' (UK Government 2020). In response to Russian actions and other perceived harms toward democracy emanating from the digital domain, the British government created the Defending Democracy programme, which aimed to protect democratic discourse and processes from foreign interference (UK Government 2020).

Germany

Germany has been under a systematic campaign of Russian (dis)information since at least 2015. Compared with France and the United Kingdom, Germany has been the most targeted state, with over 700 documented cases between 2015 and 2021 (EUvsDisinfo 2021). Among the first cases that caught public attention was the cyber-attack committed by Unit 26165 of the GRU on the German Bundestag in 2015.[7] In the Bundestag attack, thousands of documents were extracted, including internal communications, reports, and working documents (Beuth et al. 2017). The stolen data, including over two thousand confidential documents, were then released by Wikileaks, a conduit regularly used by Russia's military intelligence to disseminate information obtained from its cyberattack targets (Bild 2016, ODNI 2017). This release included confidential and politically sensitive information detailing, among other topics, the secret cooperation agreements between the German and American intelligence agencies (Bild 2016, Barker and Stuchtey 2016). Stories about this release were published in international news and Russian-backed media outlets, emitting in the open in Germany, such as RT Deutsch and Sputnik. One particular Russian-financed German-language YouTube channel, Ruptly (a subsidiary of RT), had an audience reach in Germany comparable to that of the next two domestic outlets combined.[8]

In 2016, Russian hybrid interference successfully instrumentalised Germany's already controversial migrant issue with the so-called 'Lisa Case' (Federal Academy for Security Policy 2016). The fabricated story was first released by a minor media outlet serving the *Russlanddeutsch* community on 11 January 2016. It alleged that a 13-year-old German girl of Russian origin, Lisa, was the victim of kidnapping and sexual assault by several migrant men of Muslim origin. The 'Lisa Case' came at an especially vulnerable time for the German government. A few weeks earlier, tensions were raised after reports of migrant men attacking women during New Year's Eve celebrations in Hamburg, Cologne, and several other German cities (DW 2016). The Merkel government had already been reeling from accusations that it sought to cover up or downplay what had occurred. The 'Lisa Case' was initially picked up by Moscow-based Russian state television channels, NTV and Channel 1, and referenced publicly by Russian foreign minister Sergei Lavrov, but eventually found its way to RT Deutsch and Sputnik in Germany. After the story made its way through traditional Russian and German media outlets, it was further propagated by social media platforms and chain emails within Germany (Mankoff, 2020b). The (dis)information campaign

[7] Unit 26165 operated under various pseudonyms such as SOFACY, APT28, and Fancy Bear, and has been implicated in various international hacking incidents (US Department of Justice 2018).

[8] According to data published by Mankoff (2020b), in June 2020 Ruptly had 1,290,000 YouTube followers, while the top two German domestic outlets: Der Spiegel had 818,800 followers and Die Welt 583,000 followers.

created by the 'Lisa Case' was further distorted through Russian state television service Channel 1 with the publication of a false story claiming that Austria was setting up border checkpoints with Germany to prevent child-raping migrants from crossing the border and characterizing Germany as a lawless state (Channel 1 Russia 2016). The broadcast further stoked tensions by relaying a threat by the *Russlanddeutsch* that there would be consequences for the government and the perpetrators. They saw the latter as being protected by the state, to the detriment of the security of the *Russlanddeutsch* community (Mankoff, 2020a).

Before 2016 finished, a high-profile cyber assault on Germany's telecom infrastructure provoked an alarmed response from the government. On 27 November 2016, approximately 1 million German customers of Deutsche Telekom lost access to their internet and telephone services due to a cyber-attack, which the government attributed to Russia. The head of Germany's federal intelligence agency described the telecom attack as something that had no purpose other than provoking political uncertainty (Steinke and Prantl, 2016). The CEO of Deutsche Telekom, Timotheus Hottges, stated that the incident showed the need for states to band together and form a 'NATO for the Internet,' and in a later article, elaborated on how cyberattacks show the necessity of strengthening institutional vulnerabilities in Europe (Kleinz 2016, Hottges 2018). In addition to that incident, Germany that year suffered more than 70 cyberattacks which are held by experts as attributable to Russia's GRU, including an attack on the political party SPD's caucus in the German Parliament, on the Left Party, and the CDU's state chapter in Saarland (Beuth et al. 2017).

In 2021, with the impending parliamentary elections and a noticeable uptick in (dis)information and hacking attempts against government institutions, the German government released a statement about a suspected new Russian operation called 'Ghostwriter.' This campaign reportedly combined conventional cyberattacks with (dis)information in attempts to compromise Germany's legislature, including seven Bundestag members and 31 state parliamentarians in a phishing campaign. The attacks targeted parliamentarians' private email accounts rather than their official email addresses. Germany's Foreign Ministry stated they viewed such activity 'as a danger to the security of the Federal Republic of Germany and for the process of democratic decision-making, and as a severe strain on bilateral relations' (Moulson 2021). In addition, it was later revealed through the Council of the EU (2021) that the Ghostwriter campaign was part of a larger regional campaign that targeted 'numerous members of Parliaments, government officials, politicians, and members of the press and civil society in the EU by accessing computer systems and personal accounts and stealing data.' Further, the Council of the EU (2021) stated that the campaign '[sought] to threaten our integrity and security, democratic values and principles and the core functioning of our democracies'.

In an official study of the various Russian cyber-attacks and (dis)information activity, Germany's Federal Intelligence Service and Federal Office for the Protection of the Constitution concluded that the Bundestag cyber-attack and subsequent intrusions sought to 'exert influence, and presumably also to spread (dis)information and propaganda on a grand scale.' Further, they elaborated that the intrusions were likely 'directly authorized by the presidential administration in the Kremlin and left up to the security services to carry out' (Beuth et al. 2017). During the intrusions described above, the German government did not make too many public statements since they thought doing so would encourage Russia to increase their attacks, or at least provide some valuable intelligence that could be used against them in the future (Delcker 2017). Germany did, however, respond in 2020 through the framework of the European Union by imposing sanctions on the GRU military unit and individuals responsible for the 2015 Bundestag hack (Council of the EU 2020). In response to these activities, the German Public Prosecutors' Office opened a preliminary investigation based on a dossier compiled by the German Federal Office for the Protection of the Constitution. In addition, at a meeting with the German-Russian High Working Group on Security Policy, State Secretary Miguel Berger officially lodged a protest with Russian Deputy Foreign Minister Vladimir Titov (Soesanto 2021).

France

France is the second most targeted state after Germany (EUvsDisinfo 2021). The cyber-attack against French television network TV5Monde was one of the first noted actions of Russia's hybrid campaign. The attack began in January 2015 with reconnaissance of the television network's systems and escalated in April with the installation of malicious software, which destroyed the systems used to transmit television programs. The hackers claimed to be linked to Islamic State and posted inflammatory messages on the network's Facebook account warning of further attacks: 'Soldiers of France, stay away from the Islamic State! You have the chance to save your families take advantage of it' (Keslassy 2015). However, a team of investigators from France's cybercrime agency and TV5Monde's president found the reported culprits to be the Russian-affiliated APT28 (France24 2015; Paquette 2015).[9] The attack sought in part to exploit existing social tensions from the recently occurred Charlie Hebdo attacks when Islamist militants murdered seventeen people, including eleven journalists (BBC News 2015). Moreover, the attack was part of a more extensive hybrid interference campaign targeting the French state, its critical infrastructure, and its democratic processes, which began to intensify in 2016. That year, the French state would have to defend its institutions against 24,000 cyber-attacks, some of which originated from Russia. The defence minister, appraising the gravity of the threat, was quoted as saying, 'by targeting the electoral process of a country, we are undermining its democratic foundations, and therefore its sovereignty' (Le Journal du Dimanche 2017). In response to the threat, he announced the creation of a cyber army of 2,600 soldiers by 2019 (Gramer 2017).

In 2017, France's political institutions were tested by a coordinated, three-pronged hybrid interference campaign consisting of a (dis)information campaign, a hack of Emmanuel Macron's campaign headquarters, and the release (or leak) of approximately 21,000 emails two days before the final round of the second and final round of the presidential elections (Vilmer 2018). The campaign began when a Russian newspaper, *Izvestia*, published a story on February 3, 2017, entitled 'Assange will throw oil on the fire of the presidential campaign in France' (Kotsur 2017). The article referenced an interview conducted with the founder of Wikileaks, Julian Assange,

[9] This unit was later discovered to be a pseudonym of the same military team (Unit 26165 of Russia's GRU) implicated in the above-mentioned attacks in the United Kingdom and Germany.

wherein he stated that he would begin releasing memos from correspondence stolen from the Democratic National Committee headquarters in 2016 that was damaging to Macron (Kotsur 2017). That publication was followed by another from Russian state-sponsored Sputnik portraying Macron as allegedly beholden to the US and a 'gay lobby' (Sputnik 2017).[10] Attacks were both of a political and personal nature, including salacious remarks about his family (Vilmer 2018). Macron's campaign manager, Socialist MP Richard Ferrand, commented on the influx of (dis)information from Russia and alluded to its potential impact on trust in the election process and government leadership: 'False information from Russian media is weighing on our democratic life' (Vinocur 2017).

The (dis)information campaign intensified with the leaks, which began on 5 May 2017, hours before official campaigning was due to end for the 44 hours of election silence mandated by French law. They were timed strategically to prevent Macron and his campaign from being able to defend themselves and divert the conversation to Twitter. Several doctored documents, including two that suggested that Macron was a corrupt politician with secret offshore accounts, were posted to the website 4chan, along with an announcement that more would follow (Vilmer 2018). A link appeared between US-based and European-based accounts controlled by Russian actors, thus suggesting that the same GRU unit that was responsible for the US 2016 (dis)information campaign was also behind this one. The campaign to derail Macron's bid for the presidency used the hashtag #MacronLeaks and gained immediate traction with 500,000 tweets in the first twenty-four hours of its appearance (Vilmer 2018).

In late 2018, a nationwide protest began in France, known as the *gilet jaunes* (Eng. yellow vest) movement. Several studies suggest that Russia was responsible for spreading and amplifying (dis)information to this movement via its traditional and social media channels. According to a report by Avaaz (2019) '[W]hen taking into account all videos related to Yellow Vests (as measured by whether the term yellow vests was mentioned in either the video title or description), RT France accumulated more views than Le Monde, L'Obs, Le Huffington Post, Le Figaro, and FRANCE 24 combined (30M compared to 24M)'. RT's coverage of the *gilet jaunes* protests was marked by provocation and one-sided coverage, going so far as to film a crowd of protesters gathered in front of the news crew shouting 'Thank you, RT! Thank you, RT!' which was published on their YouTube channel. As an example of the (dis)information, during the protests, Sputnik and RT had falsely claimed that most French police no longer supported Macron and showed a video from the French town of Pau of officers removing their helmets, which they said was a sign of solidarity with protesters. After a denial from the authorities involved, one of the two stations, Sputnik, was forced to issue a correction. The (dis)information campaign was prominent enough to prompt a French government investigation into its links with the Russian government (Matlack and Williams 2018).

Russian hybrid interference as a challenge against trust in liberal democracies?

[10] The (dis)information campaign was intensified by media in the US working with the campaign of Marine Le Pen.

The Russian hybrid interference in France, Germany and the UK has, as we have seen, intensified in recent years (Bechis 2021, Hague Center for Strategic Studies 2019, Thomas 2019, Wigell 2019, Vilmer 2018). This fact has raised serious concerns among targeted governments and societies. The Russian action inserts itself in an already fragile socio-political landscape, where the current crisis of Western democracy reveals a certain erosion of the social contract and tension between government and citizens, as well as among different civil society groups (OECD 2021). Hence, it is worth noting that Russian hybrid interference is not responsible for the many crises we have seen in Western democracies in recent years, such as Brexit or social upheaval related to the *gilet jaune* movement. However, Russian cyber and (dis)information operations in Western Europe have found plenty of opportunities to exert leverage on existing socio-political pressure points.

The Russian (dis)information ecosystem appears to find elections or referendums particularly vulnerable moments for democratic states; hence, hybrid interference activity increases during such periods (Henschke, Sussex, and O'Connor 2020). Elections or referendums are critical moments for democratic systems; they allow leaders to engage with their citizens openly and inclusively and further allow communicative exchanges among citizens that inform their preferences and ground the legitimacy of public debate (Habermas 1996 and Young 2000 in McKay and Tenove 2020). Voting processes in Western democracies thus provide the ideal context where any actor can voice an opinion and where all types of information can proliferate largely unchecked (Rosenberger and Gorman 2020). Russia's use of hybrid interference may thus be of more concern in the periods around significant democratic processes such as referendums or elections, when more of the public may be seeking information, and emotions about political issues are more commonly expressed. The cases we have seen in the previous section demonstrate that with few initial participants, correct timing that coincides with democratic efforts and carefully produced content that plays on the emotions of that population may allow the (dis)information operations to reach a broad audience. Such conditions potentially provide a window of opportunity to target two types of trust: horizontal and vertical.

In terms of vertical trust, there were attempts in all three country-cases to delegitimise elections and referendums, and create distrust in the procedures, candidates, infrastructure, and institutions that supported them. Through (dis)information, efforts were made to paint government authorities as corrupt, beholden to foreign interests, or out of touch with their populations, to create a vertical trust wedge between the government and society. For example, in the British case, Russian hybrid interference managed to produce distrust in the UK and Scottish government's management of the 2014 Scottish Referendum and even provoked calls from some Scottish social groups for a revote. The 2016 Brexit Referendum was accompanied by cyber-attacks against technical infrastructure to further erode trust by demonstrating the lack of the British government's capability and preparedness to defend against such assaults. These events were assessed to be part of a possible Russian 'pre-positioning' strategy, which involves a 'process of exploring and securing an entry point in a network that now, or in the future, could be used to disruptive effect' (UK Government 2020).

Similarly, in the case of Germany, the hacking of the Bundestag revealed the German state's lack of preparedness and inability to protect its data and that of its citizens. The vertical trust wedge strategy was amplified by the 'Lisa Case,' which attempted to falsely portray the government as, on the one hand, unable to protect its citizens from attacks or unwilling to investigate appropriately and, on the other, as incapable of stopping irregular migrants from crossing its borders. In the French case, the hybrid interference campaign attempted to create wedges between the electoral candidates and voters by releasing forgeries and misleading information, prior to, and during the election period, as well as during the subsequent *gilet jaune* protests, which challenged the legitimate authority of Macron's government and the state institutions. The (dis)information campaign that flowed from Russia's hybrid interference ecosystem attempted to sow division in the vertical trust by falsely claiming that police had lost trust in the government and were siding with the *gilet jaune* protesters, leading to a challenge of legitimacy for the French state. As in the other two country cases, the (dis)information in France was accompanied by cyber-attacks. The attack against TV5Monde had crippled its ability to broadcast information and was designed to signal to the target, and the wider French public, that the government could not be trusted to defend them. These actions suggest that Russia utilized its hybrid interference to not only create or add to inter-societal turbulence and uncertainty in the short-term but also to target, as part of a longer-term campaign, the trust they had for their leaders and institutions.

Russia's hybrid interference into France, Germany and the UK has benefited from their liberal, open society set-up in terms of both freedom of expression as well as relatively lax internet regulation. Russian actors who seek to manipulate public discourse thus have taken advantage of the anonymity and openness of the internet, particularly on social media. In the cyberspace domain, democratic governments often find it challenging to balance their two primary responsibilities, i.e., the will to protect citizens from misleading and false information and the obligation to ensure the constitutionally enshrined freedom of expression in the form of a relatively unregulated democratic public discourse (Morgan 2018). Thus, Russia strategically applies pressure in this domain, knowing governments find themselves in a complex 'catch-22': they are faced with several options, all of which have the potential to erode the fragile trust between citizens and governments. First, by not responding to these campaigns, Russia is left to continue utilising techniques that would, in the longer term, erode vertical trust between citizens and their governments. Further, if governments do not respond promptly to hybrid interference campaigns, they may lose the opportunity to do so adequately and with the fuller consent of their constituents in the future. This is because building adequately intrusive cyber defences requires governments to draw on a 'considerable reservoir of trust' from the public (Abramson 2017), a reservoir that could be significantly eroded before they can take meaningful protective measures. Finally, if they do succeed in responsively building intrusive cyber defences or introducing limitations to digital expression, although these measures would potentially lessen the impact of Russia's interference, they would still serve its longer-term goal of eroding trust, as the measures would be seen as an infringement upon civil liberties.[11]

Equally, on the horizontal level, trust among citizens in Western democracies has been targeted by Russian hybrid interference. This, in part, is an intended consequence of creating turbulence at the societal level. For example, in the 2014 Scottish Referendum, the Russian government attempted to create horizontal distrust between supporters and opponents of Scottish independence. This process was repeated during the 2016 Brexit Referendum, where the hybrid interference campaign targeted the Leave and Remain camps, with additional rhetoric inserted to inflame tensions from right-wing Leave supporters and fringe party members, with favourable one-sided coverage for particular beneficiaries of the (dis)information campaigns. The Russian strategy continued even after the Brexit referendum through Operation Secondary Infektion to further sow horizontal divisions by focusing on anti-immigrant rhetoric and attempting to stoke tensions over the border issue in Northern Ireland. Michael Murphy, former deputy chief of the Irish Defence Force's military intelligence section, commented that Russia liked to exploit these wedge issues because they result in 'long-term division, no matter the result…in the UK they've created a division greater than ever before' (Gallagher 2020).

In Germany, attempts were made to create horizontal trust wedges between the *Russlanddeutsch* and Russian-speaking immigrants from post-Soviet states in one camp and migrants from Middle Eastern and North African states in the other, on the societal level. In the French case, a similar formula was used, which included a hybrid strategy of (dis)information and cyber-attacks to sow horizontal divisions. The attack on TV5Monde and the subsequent false posts purporting to be from Islamic militants were an attempt to stoke tensions between France's Muslim minority and other segments of its population, which was especially strategic as it happened after the Charlie

[11] An example of governmental response to some of the events documented in this study, is the UK government's Defending Democracy programme, which focuses on electoral integrity and online transparency. The government pledged to create a penalty aimed at electoral interference, including acts to manipulate someone's vote (UK Parliament 2019). In addition, the UK Elections Act 2022 included several reforms billed by the Conservative Party as 'protecting the integrity of UK democracy'. One change focused on a digital imprint requirement which requires disclosing the person or entity which produces campaign material (House of Commons Library 2022). Similarly, the law will give new powers to the Minister for the Cabinet Office in defining campaigning and includes penalties for groups attempting to participate covertly in such activities while obscuring who is financing and organising their efforts. France and Germany have acted at the EU level. The EU 'Code of Practice on Disinformation' of 2018 focuses on the channels of hybrid interference, i.e., Facebook, Google, Twitter, Mozilla, Microsoft and TikTok (Harrison 2021). The 2018 code focuses on five core commitments which include: a commitment to disrupt the incentives of (dis)information sources, ensuring transparency in advertising, clear policies on the use of automated software (bots), investment in technology that prioritise the presentation of verified and relevant information, and the commitment to support good faith independent efforts to tackle (dis)information. The EU Digital Services Act of April 2022 further deepens this commitment to creating a safer digital space by holding digital platforms to greater accountability in, among other aspects, moderating content, preventing the spread of (dis)information, and imposing sanctions, up to the threat of a total ban within the EU, for repeated breaches of these responsibilities (European Commission 2022).

Hebdo attacks. Similarly, attempts were made to polarize the population based on political orientation during the 2017 elections by providing a platform to fringe movements and parties by echoing their rhetoric in social and traditional media. As in other campaigns, a media platform was provided to a Eurosceptic party that was seen as a challenger to more mainstream and moderate political parties, the party of Marine Le Pen. This strategy not only created horizontal distrust between voters but also sowed discord and uncertainty within France's and Europe's political establishment. In 2019, during the *gilet jaune* protest, further attempts were made to deepen polarisation between different citizen groups, including supporters and opponents of the Macron administration and his policies.

At the European level, statements from various institutions representing the targeted states of France and Germany echo fears of hybrid interference's impact on trust. One of the earliest resolutions produced on this topic during the period of study was the European Parliament (2016) resolution on EU Strategic Communication to Counteract Propaganda against it by Third Parties, which noted 'the huge resources dedicated to propaganda activities by Russia and the possible impact of hostile propaganda on decision-making processes in the EU and the undermining of public trust.' This problem was further recognised and began to be tackled by the Action Plan Against Disinformation produced by the European Commission (2018), which concluded that 'Disinformation is a major challenge for European democracies and societies…Disinformation undermines the trust of citizens in democracy and democratic institutions…This can have considerable adverse effects on society across the Union…' Further, a communication produced jointly by the European Commission and High Representative of the European Union for Foreign and Security Policy (2020), also noted that hybrid interference attacks democratic institutions and sows mistrust.

In Britain, the British House of Lords, in 2019, commissioned a select body, the Democracy and Digital Technologies Committee, to study and find ways to tackle (dis)information, among other phenomena. In a report entitled, 'Digital Technology and the Resurrection of Trust,' the committee reported that the UK was living through a 'pandemic' of disinformation, and further stated: 'If allowed to flourish, these counterfeit truths will result in the collapse of public trust, and without trust democracy as we know it will simply decline into irrelevance. The situation is that serious. In the digital world, our belief in what we see, hear and read is being distorted to the point at which we no longer know who or what to trust.' (House of Lords 2020)

These quotes demonstrate our contention that trust wedges are designed to create or augment turbulence in Western societies, often with the primary objective of making governability within targeted countries as complex as possible. Governments fear losing their ability to provide cohesion among and/or legitimate authority over various parts of their population. Moreover, the effect of the degradation of horizontal trust over time weakens the socio-political contract of the polity, and individual citizens may begin to feel alienation from their fellow citizens. In the void left by their government's potential inability to channel the common purpose of the polity, fringe or radical groups may enter the social debate. The splintering of the common focus in public discourse generates further alienation, disengagement, and frustration, continuously feeding the cycle of trust degradation at the horizontal and vertical levels. Over time, weakened social cohesion can begin to unravel the basis for a liberal and pluralist democracy.

Conclusion

The paper elucidates and connects the various ways Russia targets trust by finding and exploiting weaknesses in the cyber and information domains. By analysing the documented acts committed against the United Kingdom, France and Germany, we laboured to contribute to understanding the rationale and processes Russia utilises to erode trust and heighten societal polarisation. Such examples included targeting the bonds between the different groups, their governments, and the governments of various states. We found that Russia is targeting Western liberal democracies through an approach that uses cyber operations working in tandem with (dis)information produced by an ecosystem of state and semi-state actors – a system that includes outlets of traditional and social media, different societal groups, political parties, and their accompanying interests to create uncertainty and turbulence in the short-term but which may carry the longer-term risk of eroding trust in various ways.

The cases elucidate how intensifying interference activity in the cyber and information domains, combined with new channels of dissemination and enhanced sophistication in reaching audiences, presents new challenges for targeted entities. The evidence we presented sought to demonstrate how hybrid interference may be realised through events that seem unrelated but are, in fact, complementary occurrences for a larger strategy of eroding trust. To this end, we have elaborated upon how various types of interferences, whether through hacking and leaking forgeries, attacking technical infrastructure, spreading (dis)information during democratic processes, or other instances may be understood through the framework of horizontal and vertical trust. Thus, the study's main contribution is to demonstrate how Russian actions, whether technical or informational, are used as part of a strategy to undermine horizontal and vertical trust.

While foreign interference is not new, today's combination of democratic demands, rising levels of distrust in government, relatively unregulated social media environment, and vulnerable technical infrastructure provide an attractive entry point for foreign actors to meet their objectives. The authorities and institutions in the country-cases rightfully emphasise their fears about the consequences of undermining these horizontal and vertical ties in their societies and on the foundations of democracy. The risks associated with such interference are of fundamental importance because they target trust, the tie that binds societies under a common idea with their governments. Once this tie is loosened, it opens the door for a wide variety of social and political pressures on Western societies.

Declaration of Interest Statement:

The authors have no conflicts of interest to declare.

References

Aaltola, M. 2017. Democracy's Eleventh Hour. FIIA – Finnish Institute of International Affairs. Accessed June 5, 2021. https://www.fiia.fi/en/publication/democracys-eleventh-hour?read

Aaltola, M. 2020. *Democratic Vulnerability and Autocratic Meddling: The Thucydidean Brink in Regressive Geopolitical Competition.* New York: Springer Publishing.

Abrams, S. 2016. Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal* 15 (1): 5-31. https://doi.org/10.11610/Connections.15.1.01

Abramson, J. 2017. Trust and Democracy. Aspen Institute. Accessed May 23, 2021. https://www.aspeninstitute.org/wp-content/uploads/2017/07/Abramson.Trust-and-Democracy.pdf

Agnew, J. 2017. *Globalization and sovereignty: Beyond the territorial trap.* Rowman & Littlefield.

Asmolov, G. 2018. The Disconnective Power of Democracy. *Journal of International Affairs* 71, Special Issue 2018: 69-76. https://www.jstor.org/stable/26508120.

Atlantic Council. 2019. Operation "Secondary Infektion": A Suspected Russian Intelligence Operation Targeting Europe and the United States. Accessed December 5, 2021. https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf

Avaaz. 2019. Yellow vests Flooded by Fake News. Accessed April 29, 2022. https://avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf

Ball, D. 2017. Protecting Falsehoods with a Bodyguard of Lies: Putin's Use of Information Warfare. NATO Defense College. Accessed March 19, 2021. http://www.jstor.org/stable/resrep10264

BARB. 2016. Weekly TV Set Viewing Summary 20-26 June 2016. Broadcasters' Audience Research Board. Accessed May 24, 2022. https://www.barb.co.uk/viewing-data/weekly-viewing-summary/

Barker, T. and T. Stuchtey. 2016. How Germany Can Counter Russian Hacking: A Cyber Program for Berlin. Foreign Affairs, December 15. Accessed June 15, 2022. https://www.foreignaffairs.com/articles/germany/2016-12-15/how-germany-can-counter-russian-hacking

Bartosh, A. 2018. Трансформация современных конфликтов. [Transformation of modern conflicts]. Вопросы *Безопасности [Security Matters]* 1 (1):1-18. https://doi.org/10.25136/2409-7543.2018.1.22294

BBC News. 2015. Charlie Hebdo attack: Three days of terror. *BBC News*, January 14. Accessed October 5, 2021. https://www.bbc.com/news/world-europe-30708237

Bechis, F. 2021. Playing the Russian Disinformation Game: Information Operations from Soviet Tactics to Putin's Sharp Power. In *Democracy and Fake News: Information Manipulation and Post-Truth Politics*, ed. S. Giusti and E. Piras, 119-131. New York: Routledge.

Berg, M. and T. Johansson. 2016. Trust and Safety in the Segregated City: Contextualizing the Relationship between Institutional Trust, Crime-related Insecurity, and Generalized Trust. *Scandinavian Political Studies* 39 (4): 458-481.

Beuth, P., K. Biermann, M. Klingst, and H. Stark. 2017. Merkel and the Fancy Bear. *ZeitOnline*, May 12. Accessed November 3, 2021. https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2 Fdigital%2F2017-05%2Fcyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia

Bild. 2016. Wikileaks veröffentlicht deutsche Geheimdokumente [Wikileaks Publishes Secret German Documents]. *Bild*, December 1. Accessed November 15, 2021. https://www.bild.de/politik/2016/politik/wikileaks-politik-eilmeldung-49027054.bild.html

Blank, S. 2016. Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition. Strategic Studies Institute, U.S. Army War College. Accessed March 19, 2021. https://www.jstor.org/stable/resrep11980.11?seq=1#metadata_info_tab_contents

Bodine-Baron, E., Helmus, T. C., Radin, A., & Treyger, E. 2018. *Countering Russian Social Media Influence*. RAND Corporation. https://doi.org/10.7249/RR2740

Boghardt, T. 2009. Operation INFEKTION: Soviet Bloc Intelligence and its AIDS Disinformation Campaign. *Studies in Intelligence* 53 (4):1-24.

Brangetto, P., and M. Veenendaal. 2016. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. NATO CCD COE. Accessed June 15, 2022. https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf

Casier, T. 2020. Not on speaking terms, but business as usual: the ambiguous coexistence of conflict and cooperation in EU–Russia relations. *East European Politics* 36 (4):529–543. https://doi.org/10.1080/21599165.2020.1756784

Channel 1 Russia. 2016. Австрия временно приостанавливает действие Шенгенского соглашения из-за случаев насилия в Германии [Austria temporarily suspends the Schengen agreement due to incidents of violence in Germany]. *1tv.ru*, January 16. Accessed March 8, 2021. https://www.1tv.ru/news/2016-01-16/3330-avstriya_vremenno_priostanavlivaet_deystvie_shengenskogo_soglasheniya_iz_za_sluchaev_nasiliya_v_germanii

Christensen, H. 2017. Knowing and distrusting: how political trust and knowledge shape direct-democratic participation. *European Societies* 20 (4):72-594. https://doi.org/10.1080/14616696.2017.1402124

Congressional Research Service. 2021. Russian Cyber Units. Congressional Research Service. Accessed November 10, 2021. https://crsreports.congress.gov/product/pdf/IF/IF11718

Council of the EU. 2020. Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack. Council of the EU, October 22. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/#

Council of the EU. 2021. Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes. Council of the EU, September 24. https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/

Dalton, R. 2004. *Democratic Challenges, Democratic Choices: The Erosion of Political Support in Advanced Industrial Democracies*. Oxford: Oxford University Press.

Delcker, J. 2017. Germany fears Russia stole information to disrupt election. *POLITICO*, March 20. Accessed November 15, 2021. https://www.politico.eu/article/hacked-information-bomb-under-germanys-election/

Delhey, J., K. Newton, and C. Welzel. 2011. How general is trust in "most people"? Solving the radius of trust problem. *American Sociological Review* 76 (5):786– 807.

Demos. 2018. Russian Influence Operations on Twitter. Demos. Accessed June 5, 2022. https://demos.co.uk/project/russian-influence-operations-on-twitter/

DFRLab. 2017. #ElectionWatch: Scottish Vote, pro-Kremlin Trolls – DFRLab. Medium. December 13. Accessed November 4, 2020. https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb

Dowling, M. 2021. Democracy under Siege: Foreign Interference in a Digital Era. Australian *Journal of International Affairs* 75 (4): 383-387. https://doi.org/10.1080/10357718.2021.1909534

Dowling, M. 2022. Foreign interference and Australian electoral security in the digital era. *Australian Journal of International Affairs* 76 (1):40-56. https://doi.org/10.1080/10357718.2021.1985964

DW. 2016. String of New Year's Eve sexual assaults outrages Cologne. *DW News*, January 4. Accessed December 10, 2020. https://www.dw.com/en/string-of-new-years-eve-sexual-assaults-outrages-cologne/a-18958334

Estonian Foreign Intelligence Service. 2018. International Security and Estonia. Estonian Foreign Intelligence Service. Accessed January 5, 2021. https://valisluureamet.ee/doc/raport/2018-en.pdf

European Commission. 2020. Speech of Vice President Věra Jourová on countering disinformation amid COVID-19 "From pandemic to infodemic". European Commission, June 4. https://ec.europa.eu/commission/presscorner/api/files/document/print/it/speech_20_1000/SPEECH_20_1000_EN.pdf

European Commission. 2022. Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2545

European Commission and High Representative of the European Union for Foreign and Security Policy. 2020. The EU's Cybersecurity Strategy for the Digital Age. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Parliament. 2016. European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda against it by Third Parties. Brussels: European Parliament. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html

European Parliament Policy Department. 2021. Best Practices in the whole-of-society approach in countering hybrid threats. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf

EUvsDisinfo. 2019. Operation Secondary Infektion: The DFRLab Exposes a New Russian Influence Campaign. Accessed May 10, 2021. https://euvsdisinfo.eu/operation-secondary-infektion-the-dfrlab-exposes-new-russian-influence-campaign/

EuvsDisinfo. 2021. Vilifying Germany, Wooing Germany. Accessed June 15, 2022. https://archive.ph/3PQpc

Federal Academy for Security Policy. 2016. The Lisa Case: Stratcom Lessons for European States. Accessed November 5, 2020. https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

Field, M. and M. Wright. 2018. Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals. *The Telegraph*, October 17. Accessed June 7, 2022. https://archive.ph/isUk7

France24. 2015. Russian hackers likely behind 'IS group cyber attack' on French TV network. *France24,* June 10. Accessed November 15, 2021. https://www.france24.com/en/20150610-france-cyberattack-tv5-television-network-russia-hackers

Gallagher, C. 2020. Russian intelligence could exploit Irish Border poll, security experts say. *The Irish Times*, July 23. Accessed October 1, 2021. https://www.irishtimes.com/news/crime-and-law/russian-intelligence-could-exploit-irish-border-poll-security-experts-say-1.4311030

Global Engagement Center. 2022. Kremlin Funded-Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. US State Department. Accessed June 15, 2022.https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

Gorodnichenko, Y., T. Pham, and O. Talavera. 2021. Social media, sentiment, and public opinions: Evidence from #Brexit and #USElection. *European Economic Review* 136: 103772. https://doi.org/10.1016/j.euroecorev.2021.103772

Gramer, R. 2017. Wary of Russian Cyber Threat, France Plans to Bolster its Army of 'Digital Soldiers.' *Foreign Policy*, January 10. Accessed November 19, 2021. https://foreignpolicy.com/2017/01/10/wary-of-the-russian-cyber-threat-france-plans-to-bolster-its-army-of-digital-soldiers-cyber-attack-europe-elections-hack/

Griffin, S. 2015. *Broken Trust: Dysfunctional Government and Constitutional Reform.* University Press of Kansas. Tulane Public Law Research Paper No. 15-2. Accessed June 10, 2021. SSRN: https://ssrn.com/abstract=2570627

Hague Center for Strategic Studies. 2019. Hybrid Conflict: Neither war, nor peace. Strategic Monitor 2019-2020. https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/hybrid-conflict/

Hammond-Errey, M. (2019). Understanding and Assessing Information Influence and Foreign Interference. *Journal of Information Warfare* 18 (1):1-22. https://www.jstor.org/stable/26894654

Harrison, R. 2021. Tackling Disinformation in Times of Crisis: The European Commission's Response to the COVID-19 Infodemic and the Feasibility of a Consumer-Centric Solution. *Utrecht Law Review* 17 (3):18-33. https://doi.org/10.36633/ulr.675

Henschke, A., M. Sussex, and C. O'Connor. 2020. Countering foreign interference: election integrity lessons for liberal democracies. *Journal of Cyber Policy* 5 (2):180–198. https://doi.org/10.1080/23738871.2020.1797136

Hottges, T. 2018. A Joint Approach for a Safer Cyberspace, May 28. Accessed June 15, 2022. https://www.telekom.com/en/company/management-unplugged/timotheus-hoettges/details/a-joint-approach-for-a-safer-cyberspace-525908

House of Commons Library. 2022. Elections Bill 2021-22: Progress of the Bill. The UK House of Commons. https://researchbriefings.files.parliament.uk/documents/CBP-9421/CBP-9421.pdf

House of Lords. 2020. Digital Technology and the Resurrection of Trust. Select Committee on Democracy and Digital Technologies. https://committees.parliament.uk/publications/1634/documents/17731/default/

Hurst, L. 2019. Reddit: Classified UK-US document leak linked to Russian operation. *Euronews,* December 7. Accessed November 15, 2021. https://www.euronews.com/2019/12/07/reddit-leak-of-classified-uk-us-trade-document-originated-from-russia

Kallberg, J. 2020. What is the rationale behind election interference? U.S. Army Cyber Institute, August 30. Accessed September 9, 2021. https://digitalcommons.usmalibrary.org/aci_ja/181

Kalugin, O. 1998. Inside the KGB: An Interview with Maj. Gen. Oleg Kalugin [Interview]. *CNN*, January. Accessed October 5, 2020. https://web.archive.org/web/20070627183623/http:/www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/ wansea/

Karlsen, G. 2019. Divide and rule: ten lessons about Russian political influence activities in Europe. *Palgrave Communications* 5 (19). https://doi.org/10.1057/s41599-019-0227-8

Keslassy, E. 2015. French Government Reacts to CyberCaliphate's Attack on TV5 Monde. *Variety,* April 9. https://variety.com/2015/tv/global/ wanse-government-reacts-to-cybercaliphates-attack-on-tv5-monde-1201469306/#!

Kleinz, T. 2016. Allergische Reaktion mit Folgen [Allergic Reaction with Consequences]. *Zeit Online,* December 1. Accessed October 10, 2021. https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2Fdigital%2Finternet%2F2016-11%2Ftelekom-router-botnetz-hoettges-cyber-nato

Kotsur, V. 2017. Ассанж подольет масла в огонь предвыборной кампании Франции [Assange will add fuel to the French election campaign]. *Izvestia,* February 3. Accessed September 9, 2021. https://iz.ru/news/661960

Laruelle, M. 2021. *Is Russia Fascist?: Unravelling Propaganda East and West.* London: Cornell University Press.

Laruelle, M., and K. Limonier. 2021. Beyond "hybrid warfare": a digital exploration of Russia's entrepreneurs of influence. *Post-Soviet Affairs* 37 (4):318-335. https://doi.org/10.1080/1060586X.2021.1936409

Lavrov, S. 2017. Foreign Minister Sergey Lavrov's address and answers to questions at the 53rd Munich Security Conference, Munich. The Ministry of Foreign Affairs of the Russian Federation, February 18. Accessed October 10, 2021. https://www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/2648249

Le Journal du Dimanche. 2017. Le Drian sur le cyberespionnage : "La France n'est pas à l'abri, il ne faut pas être naïf" [Le Drian on cyber espionage: "France is not immune, we must not be "I"]. *Le Journal du Dimanche,* January 7. Accessed November 7, 2021. https://www.lejdd.fr/International/Le-Drian-sur-le-cyberespionnage-La-France-n-est-pas-a-l-abri-il-ne-faut-pas-etre-naif-837985#xtor=CS1-4

Limnell, J. A. 2018. Russian Cyber Activities in the EU. In *Hacks, Leaks and Disruptions: Russian Cyber Strategies*. European Union Institute for Security Studies. Accessed December 3, 2020. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

MacAskill, E., and R. Syal, 2017. Cyber-attack on UK parliament: Russia is suspected culprit. *The Guardian,* November 27. Accessed November 5, 2021. https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit

Mahairas, A. and M. Dvilyanski, 2018. Disinformation – Дезинформация (Dezinformatsiya). *The Cyber Defense Review* 3 (3):21-28.

Mankoff, J. 2020a. Russian Influence Operations in Germany and Their Effect. Center for Strategic and International Studies. https://www.csis.org/analysis/ wansea-influence-operations-germany-and-their-effect

– 2020b. With Friends Like These: Assessing Russian Influence in Germany. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200724_Mankoff_FullReport_v3.pdf

Mason, R. 2019. Theresa May accuses Russia of interfering in elections and fake news. *The Guardian,* July 10. Accessed December 1, 2021. https://www.theguardian.com/politics/2017/no wanseaeresa-may-accuses-russia-of-interfering-in-elections-and-fake-news

Matlack, C., and R. Williams. 2018. France to Probe Possible Russian Influence on Yellow Vest Riots. *Bloomberg News,* December 8. Accessed September 10, 2021. https://www.bloomberg.com/news/articles/2018-12-08/pro-russia-social-media-takes-aim-at-macron-as-yellow-vests-rage

McDonald, S. 2021. Disinformation in Scottish Public Life: An Overview of the Threat and Proposed Solutions. Accessed June 15, 2022. https://www.stewartmcdonald.scot/files/disinformation-in-scottish-public-life-june-2021.pdf

McKay, S., and C. Tenove. 2020. Disinformation as a Threat to Deliberative Democracy. *Political Research Quarterly* 74 (3):703-717. https://doi.org/10.1177/1065912920938143

Meister, S. 2016. Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign. German Marshall Fund of the United States, Accessed November 4, 2020. http://www.jstor.org/stable/resrep19011.7

Monaghan, S. (2019). Countering hybrid warfare. *Prism* 8 (2):82-99.

Morgan, S. 2018. Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy* 3 (1):39-43. https://doi.org/10.1080/23738871.2018.1462395

Mostrous, A. 2017. Russia used Twitter bots and trolls 'to disrupt' Brexit vote. *The Times,* November 15. Accessed November 17, 2021. https://www.thetimes.co.uk/arti wanswanse-used-web-posts-to-disrupt-brexit-vote-h9nv5zg6c

Moulson, G. 2021. Germany protests to Russia over pre-election cyberattacks. *AP NEWS,* September 6. Accessed October 5, 2021. https://apnews.com/article/technology-europe-russia-elections-germany-26ea77a3b96b94d5760aab48c9dfc008

Nannestad, P. 2008. What Have We Learned About Generalized Trust, If Anything?. *Annual Review of Political Science* 11 (1):413–436. https://doi.org/10.1146/annurev.polisci.11.060606.135412

Newton, K., D. Stolle, and S. Zmerli. 2018. Social and Political Trust. In *The Oxford Handbook of Social and Political Trust,* ed. E. Uslaner. Oxford University Press: New York.

Nimmo, B. 2016. Putin’s Media Are Pushing Britain for The Brexit. *The Interpreter*, February 12. Accessed November 17, 2021. https://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/

– 2019. UK Trade Leaks and Secondary Infektion: New Findings and Insights from a Known Russian Operation. Graphika. Accessed December 5, 2020. https://public-assets.graphika.com/reports/graphika_report_uk_trade_leaks_&_secondary_infektion.pdf

Norri–Sederholm, T., E. Norvanto, K. Talvitie–Lamberg, and A. Huhtinen. 2020. Misinformation and Disinformation in Social Media as the Pulse of Finnish National Security. In *Social Media and the Armed Forces*, ed. E. Moehlecke de Baseggio, O. Schneider, T. Szvircsev Tresch. Springer, Cham. https://doi.org/10.1007/978-3-030-47511-6_12

OECD. 2021. Government at a Glance 2021. OECD. Accessed December 6, 2021. https://www.oecd-ilibrary.org/docserver/1c258f55-en.pdf

ODNI. 2017. Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution. Office of the Director of National Intelligence. Accessed June 5, 2022. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Ostanin, I. and E. Rose. 2016. Brexit: How Russian Influence Undermines Public Trust in Referendums. OCCRP. Accessed February 4, 2021. https://www.occrp.org/en/28-ccwatch/cc-watch-indepth/5368-brexit-how-russian-influence-undermines-public-trust-in-referendums

Paquette, E. 2015. Piratage de TV5 Monde: l’enquête s’oriente vers la piste russe. [Hacking of TV5 Monde: The investigation points to the Russian track]. *LExpress*, June 9. Accessed December 1, 2021. https://www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe_1687673.html

Pamment, J., H. Nothhaft, H. Agardh-Twetman, and A. Fjallhed. 2018. Countering information influence activities: the state of the art (version 1.4). Department of Strategic Communication, Lund University. Accessed September 9, 2021. https://www.msb.se/RibData/Filer/pdf/28697.pdf

Percival, R. 2021. SNP on alert as Russia could “meddle” in Scottish independence referendum – new warning. *Express*, September 28. Accessed November 9, 2021. https://www.express.co.uk/news/politics/1497764/snp-news-russia-scottish-independence-referendum-vladimir-putin-latest

President of the Russian Federation. 2009. Russian National Security Strategy to 2020. ETH Zurich Center for Security Studies. Accessed November 9, 2021. https://css.ethz.ch/en/services/digital-library/publications/publication.html/154915

– 2015. Russian National Security Strategy. Accessed November 9, 2021. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

– 2021. Russian National Security Strategy. Accessed June 6, 2022. http://publication.pravo.gov.ru/Document/View/0001202107030001

Putnam, R. 1993. What makes democracy work? *National Civic Review* 82 (2):101–107. https://doi.org/10.1002/ncr.4100820204

Putnam, R. 2000. *Bowling alone: the collapse and revival of American community*. New York: Simon & Schuster.

Putnam, R. 2007. E Pluribus Unum: Diversity and Community in the Twenty-first Century The 2006 Johan Skytte Prize Lecture. *Scandinavian Political Studies* 30 (2):137-174. https://doi.org/https://doi.org/10.1111/j.1467-9477.2007.00176.x

RAND Corporation. 2018. Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life. Accessed September 10, 2021. https://www.rand.org/pubs/research_reports/RR2314.html

Reddit. 2019. Suspected Campaign from Russia on Reddit. Accessed September 10, 2021. https://www.reddit.com/r/redditsecurity/comments/e74nml/suspected_campaign_from_russia_on_reddit/

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare.* New York: Farrar, Straus, and Giroux.

Rosenberger, L., and L. Gorman, 2020. How Democracies Can Win the Information Contest. *The Washington Quarterly* 43 (2):75–96. https://doi.org/10.1080/0163660x.2020.1771045

Rothstein, B., and D. Stolle. 2008. The State and Social Capital: An Institutional Theory of Generalized Trust. *Comparative Politics* 40 (4):441–459. https://doi.org/10.5129/001041508x12911362383354

Rzheshevsky, A. 2005. *Far East Military Threats: Old and New.* Moscow: Parlamentskaya Gazeta.

Sabbagh, D. 2020. UK says Russia sought to interfere in 2019 election by spreading documents online. *The Guardian*, July 17. Accessed September 10, 2021. https://www.theguardian.com/uk-news/2020/jul/16/uk-says-russia-sought-to-interfere-in-2019-election-by-leaking-documents-online

Soestanto, S. 2021. The limits of like-mindedness in cyberspace. Real Instituto Elcano, November 19. Accessed June 3, 2022. https://media.realinstitutoelcano.org/wp-content/uploads/2021/12/ari98-2021-soesanto-the-limits-of-like-mindedness-in-cyberspace.pdf.

Setala, M. and T. Schiller. eds. 2012. *Citizens' Initiatives in Europe: Procedures and Consequences of Agenda-Setting by Citizens.* London: Palgrave Macmillan.

Sputnik. 2017. Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests. *Sputnik,* February 4. Accessed March 10, 2021. https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq/

Steinke, R., and H. Prantl. 2016, November 29. BND-Präsident warnt vor Hackern bei Bundestagswahl 2017 [BND President warns of hackers in the 2017 federal election]. *Süddeutsche.de,* November 29. Accessed October 13, 2021. https://www.sueddeutsche.de/politik/bundestagswahl-bnd-praesident-warnt-vor-cyberangriffen-aus-russland-1.3270995

Taylor, B. 2018. *The Code of Putinism*. Oxford: Oxford University Press.

Thomas, T. 2019. *Russian Military Thought: Concepts and Elements. The Mitre Corporation*. Mclean: VA.

Tsygankov, A. P. 2019. *Russia and America: The Asymmetric Rivalry*. Cambridge: Polity Press.

UK Government. 2018. "UK Exposes Russian cyber attacks." Accessed June 4, 2022. https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks

UK Government. 2020. "Intelligence and Security Committee of Parliament Report on Russia." Accessed November 10, 2021. https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf

UK Parliament. 2019. "Defending Democracy Programme". Accessed June 3, 2022. https://hansard.parliament.uk/commons/2019-07-22/debates/19072238000019/DefendingDemocracyProgramme

US Department of Justice. 2018. U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations. Accessed November 19, 2021. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

Uslaner, E. 2002. *The Moral Foundations of Trust.* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.824504

– 2018. *The Oxford Handbook of Social and Political Trust (1st ed.)*. Oxford: Oxford University Press.

Vinocur, N. 2017. Emmanuel Macron aide blames Russia for hacking attempts. *POLITICO,* February 13. Accessed September 10, 2021. https://www.politico.eu/article/emmanuel-macron-aide-blames-russia-for-hacking-attempts/

Vilmer, J. 2018. Lessons from the Macron Leaks. In Hacks, Leaks and Disruptions: Russian Cyber Strategies. European Union Institute for Security Studies. Accessed December 3, 2020. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Vilmer, J., A. Escorcia, M. Guillaume, and J. Herrera. 2018. Information Manipulation: A Challenge for our Democracies. Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Wigell, M. 2019. Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs* 95 (2):255-275. https://doi.org/10.1093/ia/iiz018

Wike, R., and J. Fetterolf. 2018. Liberal Democracy’s Crisis of Confidence. *Journal of Democracy* 29 (4):136–150. https://doi.org/10.1353/jod.2018.0069

Zafesova, A. 2021. Lie to Live: The production of a faked reality as an existential function of Putin’s regime. In *Democracy and Fake News: Information Manipulation and Post-Truth Politics*, ed. S. Giusti and E. Piras. New York: Routledge.

Zmerli, S., and K. Newton. 2017. Objects of political and social trust: Scales and hierarchies. In *Handbook on Political Trust*, eds. S. Zmerli and T. W. G. van der Meer, 104– 124. London: Edward Elgar.