Cyber-enabled foreign interference in elections and referendums

Sarah O'Connor

With Fergus Hanson, Emilia Currey and Tracy Beattie

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 41/2020

About the authors

Sarah O'Connor is a Researcher working with the International Cyber Policy Centre at ASPI.

Fergus Hanson is the Director of the International Cyber Policy Centre at ASPI.

Emilia Currey is a Researcher working with the International Cyber Policy Centre at ASPI.

Tracy Beattie is a Research Intern working with the International Cyber Policy Centre at ASPI.

Acknowledgements

The authors would like to thank Danielle Cave, Dr Samantha Hoffman, Tom Uren and Dr Jacob Wallis for all of their work on this project. We would also like to thank Michael Shoebridge, anonymous peer reviewers, and external peer reviewers Katherine Mansted, Alicia Wanless and Dr Jacob Shapiro for their invaluable feedback on drafts of this report.

In 2019, ASPI's International Cyber Policy Centre was awarded a US$100,000 research grant from Twitter, which was used towards this project. The work of ASPI ICPC would not be possible without the support of our partners and sponsors across governments, industry and civil society.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published October 2020.

ISSN 2209-9689 (online),
ISSN 2209-9670 (print)

Cover image: Produced by Rebecca Hendin, online.

Funding for this report was provided by Twitter.

Cyber-enabled foreign interference in elections and referendums

Sarah O'Connor

With Fergus Hanson, Emilia Currey and Tracy Beattie

Policy Brief
Report No. 41/2020

Contents

What's the problem?

Over the past decade, state actors have taken advantage of the digitisation of election systems, election administration and election campaigns to interfere in foreign elections and referendums.[1] Their activity can be divided into two attack vectors. First, they've used various cyber operations, such as denial of service (DoS) attacks and phishing attacks, to disrupt voting infrastructure and target electronic and online voting, including vote tabulation. Second, they've used online information operations to exploit the digital presence of election campaigns, politicians, journalists and voters. Together, these two attack vectors (referred to collectively as 'cyber-enabled foreign interference' in this report because both are mediated through cyberspace) have been used to seek to influence voters and their turnout at elections, manipulate the information environment and diminish public trust in democratic processes.

This research identified 41 elections and seven referendums between January 2010 and October 2020 where cyber-enabled foreign interference was reported, and it finds that there's been a significant uptick in such activity since 2017. This data collection shows that Russia is the most prolific state actor engaging in online interference, followed by China, whose cyber-enabled foreign interference activity has increased significantly over the past two years. As well as these two dominant actors, Iran and North Korea have also tried to influence foreign elections in 2019 and 2020. All four states have sought to interfere in the 2020 US presidential elections using differing cyber-enabled foreign interference tactics. In many cases, these four actors use a combination of cyber operations and online information operations to reinforce their activities. There's also often a clear geopolitical link between the interfering state and its target: these actors are targeting states they see as adversaries or useful to their geopolitical interests.

Democratic societies are yet to develop clear thresholds for responding to cyber-enabled interference, particularly when it's combined with other levers of state power or layered with a veil of plausible deniability.[2] Even when they're able to detect it, often with the help of social media platforms, research institutes and the media, most states are failing to effectively deter such activity. The principles inherent in democratic societies—openness, freedom of speech and the free flow of ideas—have made them particularly vulnerable to online interference.

What's the solution?

This research finds that not all states are being targeted by serious external threats to their electoral processes, so governments should consider scaled responses to specific challenges. However, the level of threat to all states will change over time, so there's little room for complacency. For all stakeholders—in government, industry and civil society—learning from the experience of others will help nations minimise the chance of their own election vulnerabilities being exploited in the future.[3] The integrity of elections and referendums is key to societal resilience. Therefore, these events must be better protected through greater international collaboration and stronger engagement between government, the private sector and civil society.

Policymakers must respond to these challenges without adopting undue regulatory measures that would undermine their political systems and create 'the kind of rigidly controlled environment autocrats seek'.[4] Those countries facing meaningful cyber-enabled interference need to adopt a multi-stakeholder approach that carefully balances democratic principles and involves governments, parliaments, internet platforms, cybersecurity companies, media, NGOs and research institutes. This report recommends that governments identify vulnerabilities and threats as a basis for developing an effective risk-mitigation framework for resisting cyber-enabled foreign interference.

The rapid adoption of social media and its integration into the fabric of political discourse has created an attack surface for malign actors to exploit. Global online platforms must take responsibility for taking appropriate action against actors attempting to manipulate their users, yet these companies are commercial entities whose interests aren't always aligned with those of governments. They aren't intelligence agencies so are sometimes limited in their capacity to attribute malign activities directly. To mitigate risk during election cycles, social media companies' security teams should work closely with governments and civil society groups to ensure that there's a shared understanding of the threat actors and of their tactics in order to ensure an effectively calibrated and collaborative security posture.

Policymakers must implement appropriate whole-of-government mechanisms which continuously engage key stakeholders in the private sector and civil society. Greater investments in capacity building must be made by both governments and businesses in the detection and deterrence of these. It's vital that civil society groups are supported to build up capability that stimulates and informs international public discourse and policymaking. Threats to election integrity are persistent, and the number of actors willing to deploy these tactics is growing.

Background

Foreign states' efforts to interfere in the elections and referendums of other states, and more broadly to undermine other political systems, are an enduring practice of statecraft.[5] Yet the scale and methods through which such interference occurs has changed, with old and new techniques adapting to suit the cyber domain and the opportunities presented by a 24/7, always connected information environment.[6]

When much of the world moved online, political targets became more vulnerable to foreign interference, and millions of voters were suddenly exposed, 'in a new, "neutral" medium, to the very old arts of persuasion or agitation'.[7] The adoption of electronic and online voting, voter tabulation and voter registration,[8] as well as the growth of online information sharing and communication, has made interference in elections easier, cheaper and more covert.[9] This has lowered the entry costs for states seeking to engage in election interference.[10]

Elections and referendums are targeted by foreign adversaries because they are opportunities when significant political and policy change occurs and they are also the means through which elected governments derive their legitimacy.[11] By targeting electoral events, foreign actors can attempt to influence political decisions and policymaking, shift political agendas, encourage social polarisation and undermine democracies. This enables them to achieve long-term strategic goals, such as strengthening their relative national and regional influence, subverting undesired candidates, and compromising international alliances that 'pose a threat' to their interests.[12]

Elections and referendums also involve diverse actors, such as politicians, campaign staffers, voters and social media platforms, all of which can be targeted to knowingly or unknowingly participate in, or assist with, interference orchestrated by a foreign state.[13] There are also a number of cases where journalists and media outlets have unwittingly shared, amplified, and contributed to the online information operations of foreign state actors.[14] The use of unknowing participants has proved to be a key feature of cyber-enabled foreign election interference.

This is a dangerous place for liberal democracies to be in. This report highlights that the same foreign state actors continue to pursue this type of interference, so much so that it is now becoming a global norm that's an expected part of some countries' election processes. On its own, this perceived threat has the potential to undermine the integrity of elections and referendums and trust in public and democratic institutions.

Methodology and definitions

This research is an extension and expansion of the International Cyber Policy Centre's *Hacking democracies: cataloguing cyber-enabled attacks on elections*, which was published in May 2019. That project developed a database of reported cases of cyber-enabled foreign interference in national elections held between November 2016 and April 2019.[15] This new research extends the scope of *Hacking democracies* by examining cases of cyber-enabled foreign interference between January 2010 and October 2020. This time frame was selected because information on the use of cyber-enabled techniques as a means of foreign interference started to emerge only in the early 2010s.[16]

This reports appendix includes a dataset that provides an inventory of case studies where foreign state actors have reportedly used cyber-enabled techniques to interfere in elections and referendums. The cases have been categorised by:

- target
- type of political process
- year
- attack vector (method of interference)
- alleged foreign state actor.

Also accompanying this report is an interactive online map which geo-codes and illustrates our dataset, allowing users to apply filters to search through the above categories.

This research relied on open-source information, predominantly in English, including media reports from local, national, and international outlets, policy papers, academic research, and public databases. It was desktop based and consisted of case selection, case categorisation and mixed-methods analysis.[17] The research also benefited from a series of roundtable discussions and consultations with experts in the field,[18] as well as a lengthy internal and external peer review process.

The accompanying dataset only includes cases where attribution was publicly reported by credible researchers, cybersecurity firms or journalists. The role of non-state actors and the use of cyber-enabled techniques by domestic governments and political parties to shape political discourse and public attitudes within their own societies weren't considered as part of this research.[19]

This methodology has limitations. For example, the research is limited by the covert and ongoing nature of cyber-enabled foreign interference, which is not limited to the period of an election cycle or campaign. Case selection for the new dataset, in particular, was impeded by the lack of publicly available information and uncertainty about intent and attribution, which are common problems in work concerning cyber-enabled or other online activity. It likely results in the underreporting of cases and a skewing towards English-language and mainstream media sources. The inability to accurately assess the impact of interference campaigns also results in a dataset that doesn't distinguish between major and minor campaigns and their outcomes. The methodology omitted cyber-enabled foreign interference that occurred outside the context of elections or referendums.[20]

In the context of this policy brief, the term 'attack vector' refers to the means by which foreign state actors carry out cyber-enabled interference. Accordingly, the dataset contains cases of interference that can broadly be divided into two categories:

- **Cyber operations:** covert activities carried out via digital infrastructure to gain access to a server or system in order to compromise its service, identify or introduce vulnerabilities, manipulate information or perform espionage[21]
- **Online information operations:** information operations carried out in the online information environment to covertly distort, confuse, mislead and manipulate targets through deceptive or inaccurate information.[22]

Cyber operations and online information operations are carried out via an 'attack surface', which is to be understood as the 'environment where an attacker can try to enter, cause an effect on, or extract data from'.[23]

Key findings

ASPI's International Cyber Policy Centre has identified 41 elections and seven referendums between January 2010 and October 2020 (Figure 1) that have been subject to cyber-enabled foreign interference in the form of cyber operations, online information operations or a combination of the two.[24]

Figure 1: Cases of cyber-enabled foreign interference, by year and type of political process

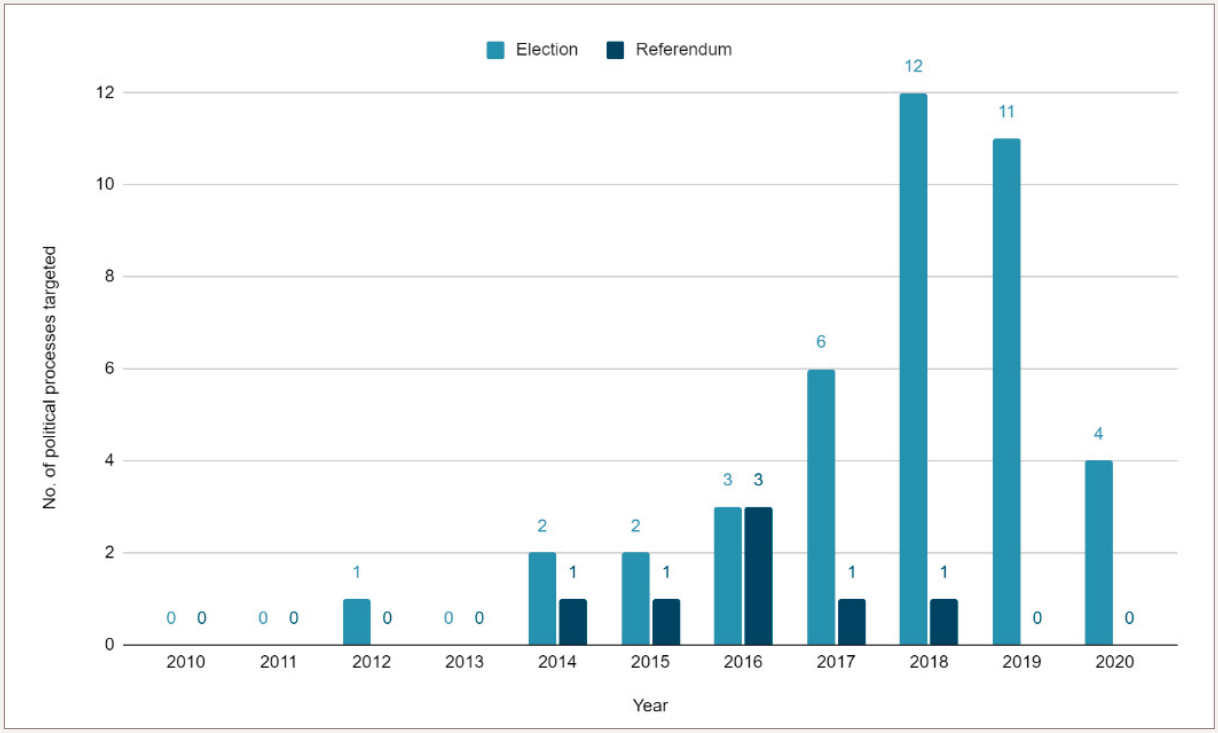


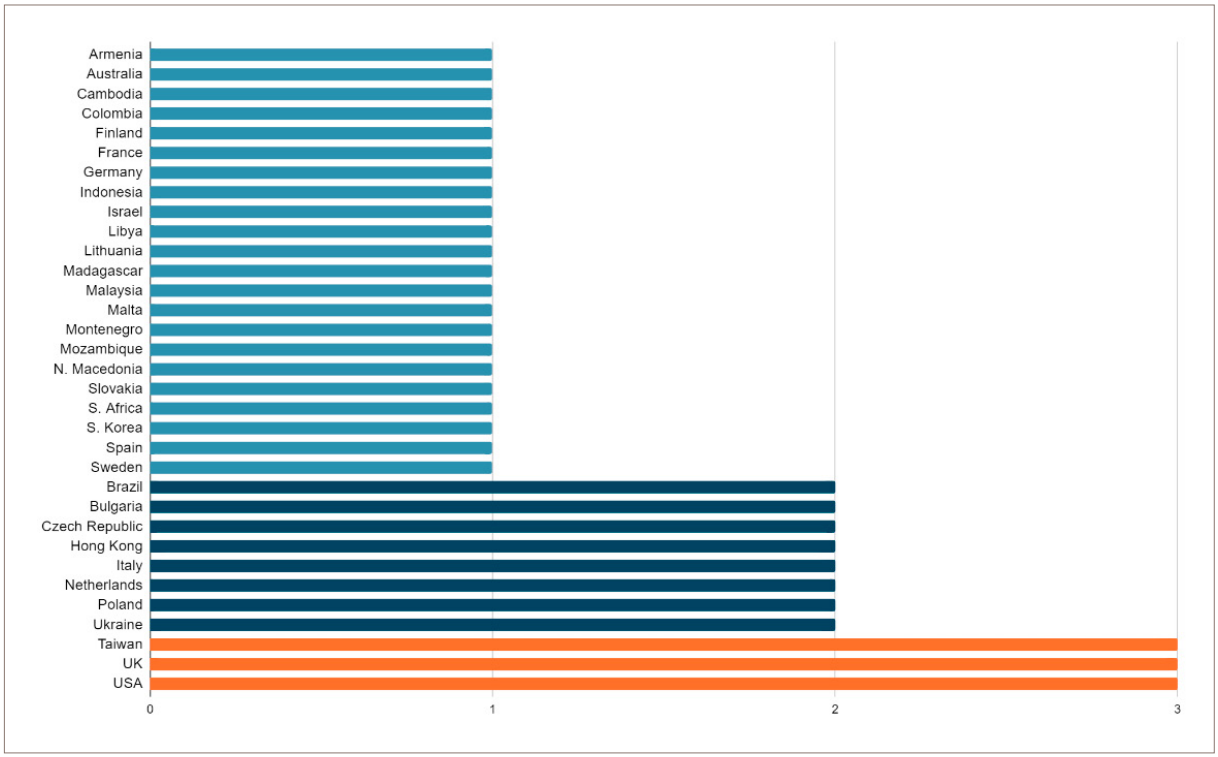
Figure 1 shows that reports of the use of cyber-enabled techniques to interfere in foreign elections and referendums has increased significantly over the past five years. Thirty-eight of the 41 elections in which foreign interference was identified, and six of the referendums, occurred between 2015 and 2020 (Figure 1). These figures are significant when we consider that elections take place only every couple of years and that referendums are typically held on an *ad hoc* basis, meaning that foreign state actors have limited opportunities to carry out this type of interference.

As a key feature of cyber-enabled interference is deniability, there are likely many more cases that remain publicly undetected or unattributed. Moreover, what might be perceived as a drop in recorded cases in 2020 can be attributed to a number of factors, including election delays caused by Covid-19 and that election interference is often identified and reported on only after an election period is over.

Figure 2: Targets of cyber-enabled foreign interference in an election or referendum

Note: The numbers in the map represent the number of reported cases of cyber-enabled foreign interference in an election or referendum. Access this interactive map here. Source: Maptive, map data © 2020 Google.

Figure 3: Number of political processes targeted (1–4), by state or region



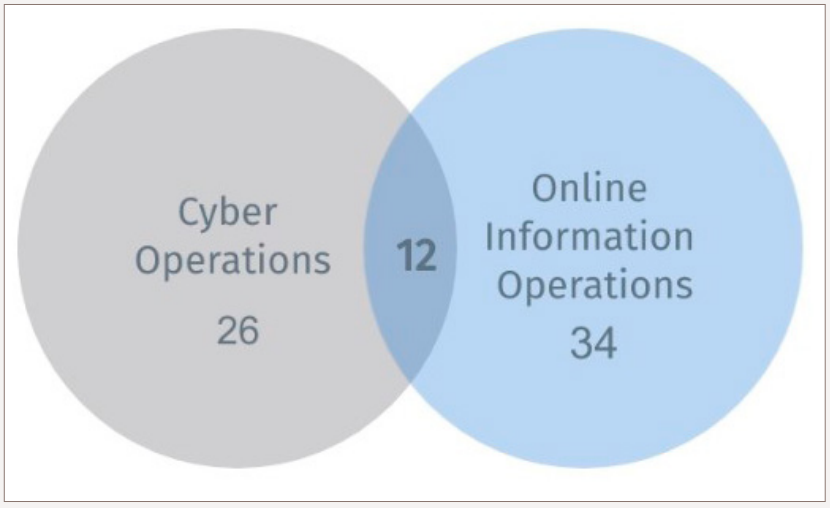
Cyber-enabled interference occurred on six continents (Africa, Asia, Europe, North America, Australia and South America).The research identified 33 states that have experienced cyber-enabled foreign interference in at least one election cycle or referendum, the overwhelming majority of which are democracies.[25] The EU has also been a target: several member states were targeted in the lead-up to the 2019 European Parliament election.[26]

Significantly, this research identified 11 states that were targeted in more than one election cycle or referendum (Figure 3). The repeated targeting of certain states is indicative of their (perceived) strategic value, the existence of candidates that are aligned with the foreign state actors' interests,[27] insufficient deterrence efforts, or past efforts that have delivered results.[28] This research also identified five cases in which multiple foreign state actors targeted the same election or referendum (the 2014 Scottish independence referendum, the 2016 UK referendum on EU membership, the 2018 Macedonian referendum, the 2019 Indonesian general election and the 2020 US presidential election). Rather than suggesting coordinated action, the targeting of a single election or referendum by multiple foreign state actors more likely reflects the strategic importance of the outcome to multiple states.

The attack vectors

The attack vectors are cyber operations and online information operations.[29] Of the 48 political processes targeted, 26 were subjected to cyber operations and 34 were subjected to online information operations. Twelve were subjected to a combination of both (Figure 4).

Figure 4: Attacks on political processes, by attack vector



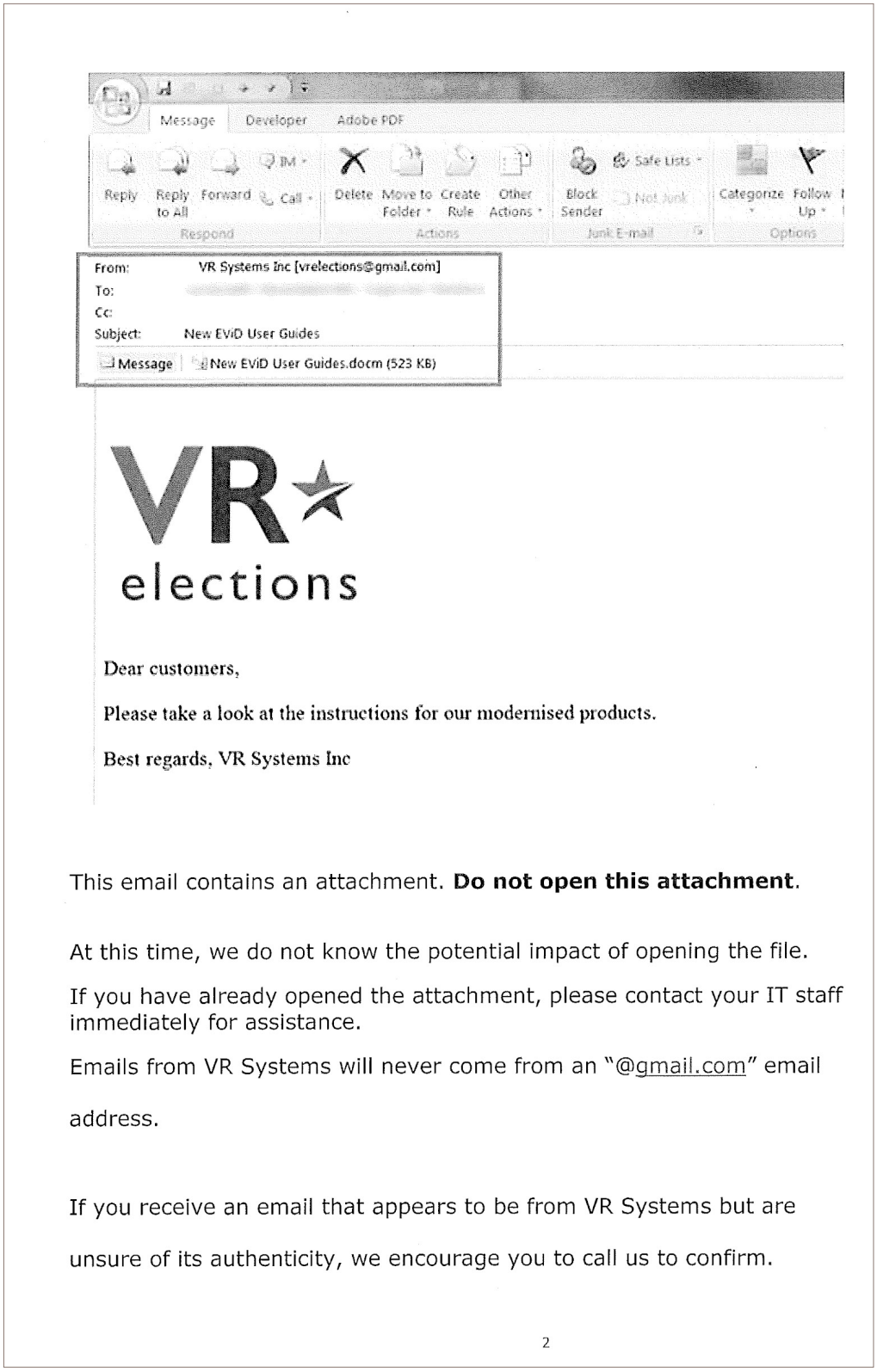
Cyber operations

This research identified 25 elections and one referendum over the past decade in which cyber operations were used for interference purposes. In the context of election interference, cyber operations fell into two broad classes: operations to directly disrupt (such as DoS attacks) or operations to gain unauthorised access (such as phishing). Unauthorised access could be used to enable subsequent disruption or to gather intelligence that could then enable online information operations, such as a hack-and-leak campaign.

Phishing attacks were the main technique used to gain unauthorised access to the personal online accounts and computer systems of individuals and organisations involved in managing and running election campaigns or infrastructure. They were used in 17 of the 25 elections, as well as the referendum, with political campaigns on the receiving end in most of the reported instances. Phishing involves misleading a target into downloading malware or disclosing personal information, such as login credentials, by sending a malicious link or file in an otherwise seemingly innocuous email or

message (Figure 5).[30] For example, Google revealed in 2020 that Chinese state-sponsored threat actors pretended to be from antivirus software firm McAfee in order to target US election campaigns and staffers with a phishing attack.[31]

Figure 5: The email Russian hackers used to compromise state voting systems ahead of the 2016 US presidential election



Source: Sam Biddle, 'Here's the email Russian hackers used to try to break into state voting systems', *The Intercept*, 2 June 2018, online.

When threat actors gain unauthorised access to election infrastructure, they could potentially disrupt or even alter vote counts, as well as use information gathered from their access to distract public discourse and sow doubt about the validity and integrity of the process.

Then there are DoS attacks, in which a computer or online server is overwhelmed by connection requests, leaving it unable to provide service.[32] In elections, they're often used to compromise government and election-related websites, including those used for voter registration and vote tallying. DoS attacks were used in six of the 25 elections, and one referendum, targeting vote-tallying websites, national electoral commissions and the websites of political campaigns and candidates. For example, in 2019, the website of Ukrainian presidential candidate Volodymyr Zelenskiy was subjected to a distributed DoS attack the day after he announced his intention to run for office. The website received 5 million requests within minutes of its launch and was quickly taken offline, preventing people from registering as supporters.[33]

Online information operations

This research identified 28 elections and six referendums over the past decade in which online information operations were used for interference purposes. In the context of election interference, online information operations should be understood as the actions taken online by foreign state actors to distort political sentiment in an election to achieve a strategic or geopolitical outcome.[34] They can be difficult to distinguish from everyday online interactions and often seek to exploit existing divisions and tensions within the targeted society.[35]

Online information operations combine social media manipulation ('inauthentic coordinated behaviour'), for example partisan media coverage and disinformation to distort political sentiment during an election and, more broadly, to alter the information environment. The operations are designed to target voters directly and often make use of social media and networking platforms to interact in real time and assimilate more readily with their targets.[36]

Online information operations tend to attract and include domestic actors.[37] There have been several examples in which Russian operatives have successfully infiltrated and influenced legitimate activist groups in the US.[38] This becomes even more prominent as foreign state actors align their online information operations with domestic disinformation and extremist campaigns, amplifying rather than creating disinformation.[39] The strategic use of domestic disinformation means that governments and regulators may find it difficult to target them without also taking a stand against domestic misinformers and groups.

It is important to acknowledge the synergy of the two attack vectors, and also how they can converge and reinforce one another.[40] This research identified three elections where cyber operations were used to compromise a system and obtain sensitive material, such as emails or documents, which were then strategically disclosed online and amplified.[41] For example, according to *Reuters*, classified documents titled 'UK-US Trade & Investment Working Group Full Readout' were distributed online before the 2019 British general election as part of a Russian-backed strategic disclosure campaign.[42] The main concern with the strategic use of both attack vectors is that it further complicates the target's ability to detect, attribute and respond. This means that any meaningful response will need to consider both potential attack vectors when securing vulnerabilities.

State actors and targets

Cyber-enabled foreign interference in elections and referendums between 2010 and 2020 has been publicly attributed to only a small number of states: Russia, China, Iran and North Korea. In most cases, a clear geopolitical link between the source of interference and the target can be identified; Russia, China, Iran and North Korea mainly target states in their respective regions, or states they regard as adversaries— such as the US.[43]

The increasing cohesion among foreign state actors, notably China and Iran learning and adopting various techniques from Russia, has made it increasingly difficult to distinguish between the different foreign state actors.[44] This has been further complicated by the adoption of Russian tactics and techniques by domestic groups, in particular groups aligned with the far-right for example.[45]

Russia

Russia is the most prolific foreign actor in this space. This research identified 31 elections and seven referendums involving 26 states over the past decade in which Russia allegedly used cyber-enabled foreign interference tactics. Unlike the actions of many of the other state actors profiled here, Russia's approach has been global and wide-ranging. Many of Russia's efforts remain focused on Europe, where Moscow allegedly used cyber-enabled means to interfere in 20 elections, including the 2019 European Parliament election and seven referendums. Of the 16 European states affected, 12 are members of the EU and 13 are members of NATO.[46] Another focus for Russia has been the US and while the actual impact on voters remains debatable, Russian interference has become an expected part of US elections.[47] Moscow has also sought to interfere in the elections of several countries in South America and Africa, possibly in an attempt to undermine democratisation efforts and influence their foreign policy orientations.[48]

Russia appears to be motivated by the intent to signal its capacity to respond to perceived foreign interference in its internal affairs and anti-Russian sentiment.[49] It also seeks to strengthen its regional power by weakening alliances that pose a threat. For instance, Russia used cyber operations and online information operations to interfere in both the 2016 Montenegrin parliamentary election and the 2018 Macedonian referendum. This campaign was part of its broader political strategy to block the two states from joining NATO and prevent the expansion of Western influence into the Balkan peninsula.[50]

Figure 6: States targeted by Russia between 2010 and 2020

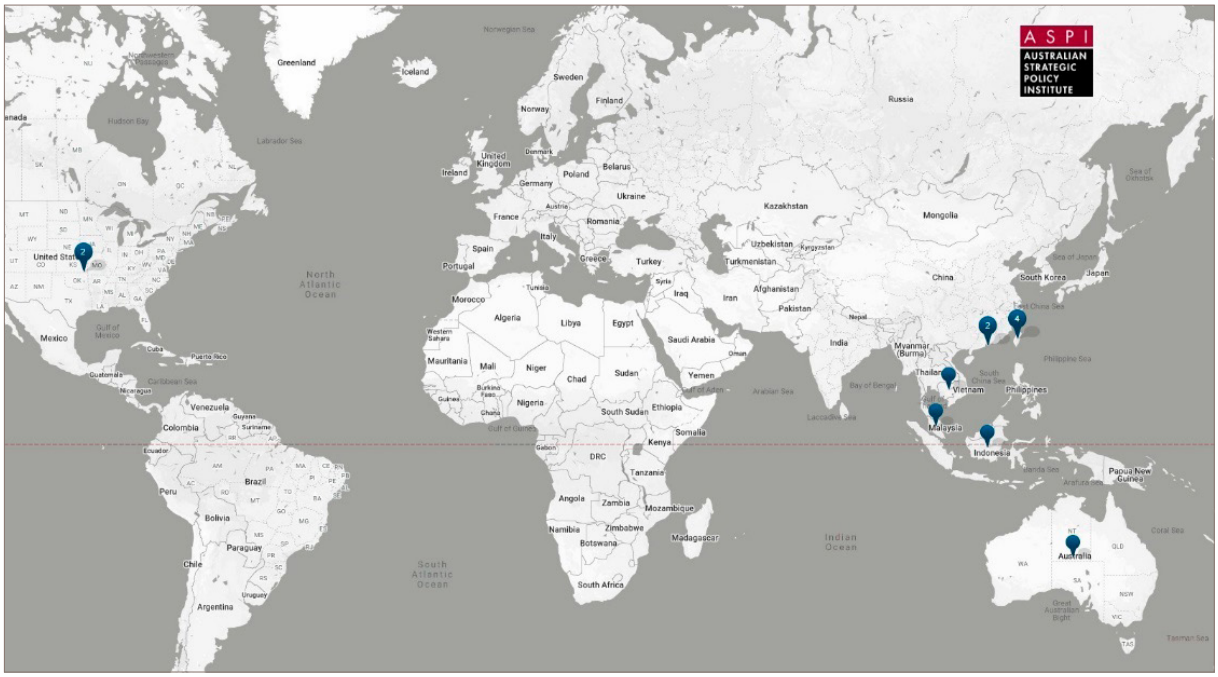
Source: Maptive, map data © 2020 Google.

China

Over the past decade, it's been reported that China has targeted 10 elections in seven states and regions. Taiwan, specifically Taiwanese President Tsai Ing-wen and her Democratic Progressive Party, has been the main target of China's cyber-enabled election interference.[51] Over the past three years, however, the Chinese state has expanded its efforts across the Indo-Pacific region.[52] Beijing has also been linked to activity during the 2020 US presidential election. As reported by the *New York Times* and confirmed by both Google and Microsoft, state-backed hackers from China allegedly conducted unsuccessful spear-phishing attacks to gain access to the personal email accounts of campaign staff members working for the Democratic Party candidate Joseph Biden.[53]

China's interference in foreign elections is part of its broader strategy to defend its 'core' national interests, both domestically and regionally, and apply pressure to political figures who challenge those interests. Those core interests, as defined by the Chinese Communist Party, include the preservation of domestic stability, economic development, territorial integrity and the advancement of China's great-power status.[54] Previously, China's approach could be contrasted with Russia's in that China attempted to deflect negativity and shape foreign perceptions to bolster its legitimacy, whereas Russia sought to destabilise the information environment, disrupt societies and weaken the target.[55] More recently, however, China has adopted methods associated with Russian interference, such as blatantly destabilising the general information environment in targeted countries with obvious mistruths and conspiracy theories.[56]

Figure 7: States and regions targeted by China between 2010 and 2020

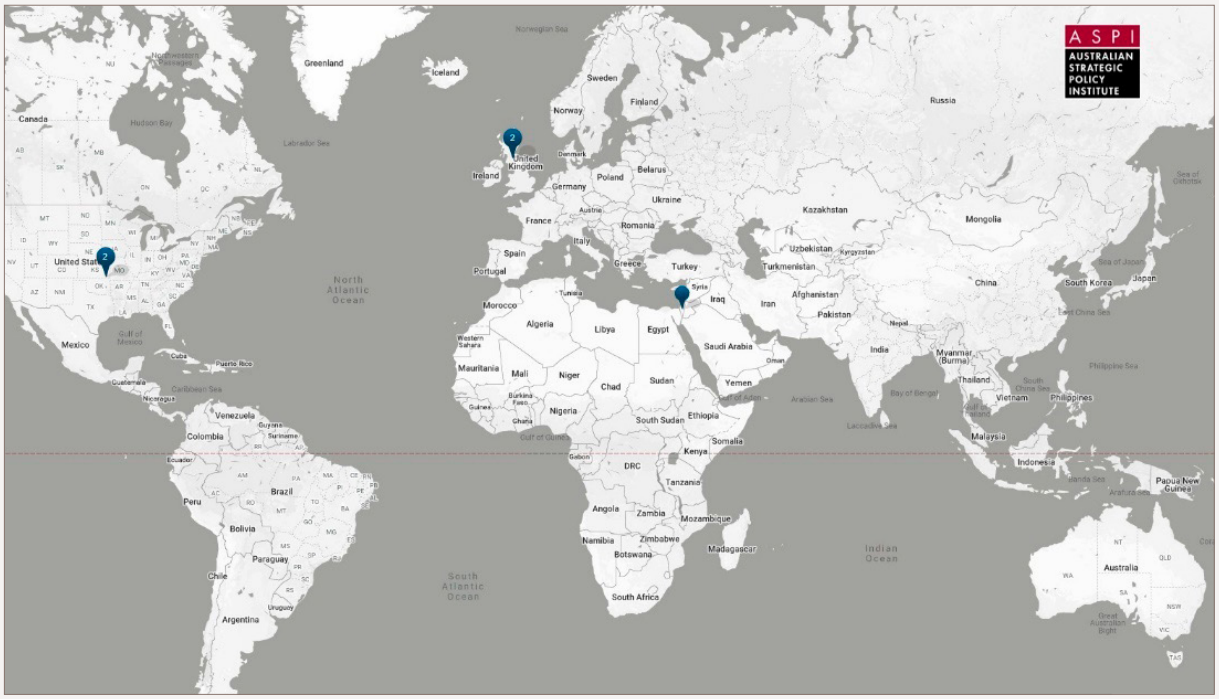


Source: Maptive, map data © 2020 Google.

Iran

This dataset shows that Iran engaged in alleged interference in two elections and two referendums in three states.[57] Iranian interference in foreign elections appears to be similar to Russian interference in that it's a defensive action against the target for meddling in Iran's internal affairs and a reaction to perceived anti-Iran sentiment. A pertinent and current example of this is Iran's recent efforts to interfere in the 2020 US presidential election by targeting President Trump's campaign.[58] As reported by the *Washington Post*, Microsoft discovered that the Iranian-backed hacker group Phosphorus had used phishing emails to target 241 email accounts belonging to government officials, journalists, prominent Iranian citizens and staff associated with Trump's election campaign and successfully compromised four of those accounts.[59]

Figure 8: States targeted by Iran between 2010 and 2020



Source: Maptive, map data © 2020 Google.

North Korea

North Korea has been identified as a foreign threat actor behind activity targeting both the 2020 South Korean legislative election and the 2020 US presidential election.[60] Somewhat similarly to China's approach, North Korea's interference appears to focus on silencing critics and discrediting narratives that undermine its national interests. For example, North Korea targeted North Korean citizens running in South Korea's 2020 legislative election, including Thae Yong-ho, the former North Korean Deputy Ambassador to the UK and one of the highest-ranking North Korean officials to ever defect.[61]

Figure 9: States targeted by North Korea between 2010 and 2020

Source: Maptive, map data © 2020 Google.

Detection and attribution

Detection and attribution requires considerable time and resources, as those tasks require the technical ability to analyse and reverse engineer a cyber operation or online information operation. Beyond attribution, understanding the strategic and geopolitical aims of each event is challenging and time-consuming.[62] The covert and online nature of cyber-enabled interference, whether carried out as a cyber operation or an online information operation, inevitably complicates the detection and identification of interference. For example, a DoS attack can be difficult to distinguish from a legitimate rise in online traffic. Moreover, the nature of the digital infrastructure and the online information environment used to carry out interference enables foreign state actors to conceal or falsify their identities, locations, time zones and languages.

As detection and attribution capabilities improve, the tactics and techniques used by foreign states will adapt accordingly, further complicating efforts to detect and attribute interference promptly.[63] There are already examples of foreign state actors adapting their techniques, such as using closed groups and encrypted communication platforms (such as WhatsApp, Telegram and LINE) to spread disinformation[64] or using artificial intelligence to generate false content.[65] It can also be difficult to determine whether an individual or group is acting on its own or on behalf of a state.[66] This is further complicated by the use of non-state actors, such as hackers-for-hire, consultancy firms and unwitting individuals, as proxies. Ahead of the 2017 Catalan independence referendum, for example, the Russian-backed media outlets *RT* and *Sputnik* used Venezuelan and Chavista-linked social media accounts as part of an amplification campaign. The hashtag #VenezuelaSalutesCatalonia was amplified by the accounts to give the impression that Venezuela supported Catalonian independence.[67] More recently, Russia outsourced part of its 2020 US presidential disinformation campaign to Ghanaian and Nigerian nationals who were employed to generate content and disseminate it on social media.[68]

The ‘bigger picture’

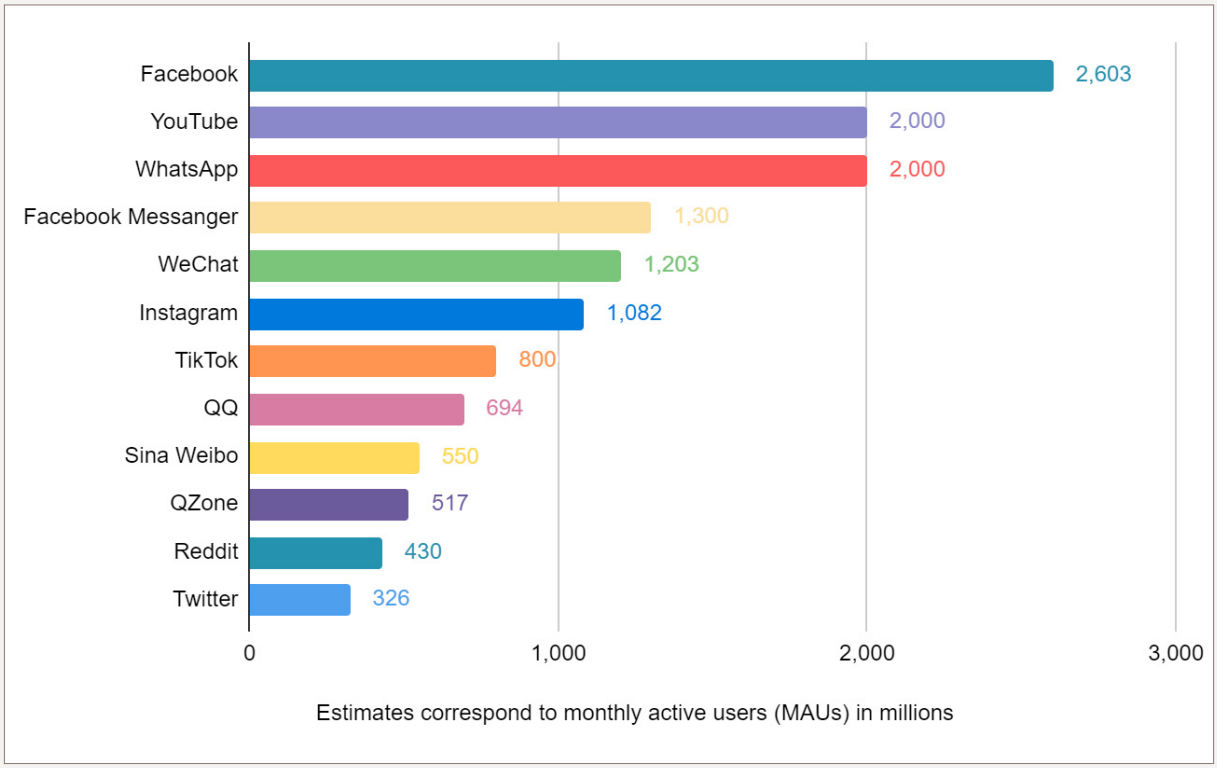
States vary in their vulnerability to cyber-enabled foreign interference in elections and referendums. In particular, ‘highly polarised or divided’ democracies tend to be more vulnerable to such interference.[69] The effectiveness of cyber-enabled interference in the lead-up to an election is overwhelmingly determined by the robustness and integrity of the information environment and the extent to which the electoral process has been digitised.[70] Academics from the School of Politics and International Relations at the Australian National University found that local factors, such as the length of the election cycle and the target’s preparedness and response, also play a significant role. For example, Emmanuel Macron’s *En Marche!* campaign prepared for Russian interference by implementing strategies to respond to both cyber operations (specifically, phishing attacks) and online information operations. In the event that a phishing attack was detected, Macron’s IT team was instructed to ‘flood’ phishing emails with multiple login credentials to disrupt and distract the would-be attacker. To deal with online information operations, Macron’s team planted fake emails and documents that could be identified in the event of a strategic disclosure and undermine the adversary’s effort.[71]

Electronic and online voting, vote tabulation and voter registration systems are often presented as the main targets of cyber-enabled interference. It is important to recognise that the level of trust the public has in the integrity of electoral systems, democratic processes and the information environment is at stake. In Europe, a 2018 Eurobarometer survey on democracy and elections found that 68% of respondents were concerned about the potential for fraud or cyberattack in electronic voting, and 61% were concerned about ‘elections being manipulated through cyberattacks’.[72] That figure matched the result of a similar survey conducted by the Pew Research Center in the US, which found that 61% of respondents believed it was likely that cyberattacks would be used in the future to interfere in their country’s elections.[73]

However, not all states are equally vulnerable to this type of interference. Some, for example, opt to limit or restrict the use of information and communication technologies in the electoral process.[74] The Netherlands even reverted to using paper ballots to minimise its vulnerability to a cyber operation, ensuring that there wouldn’t be doubts about the electoral outcome.[75] Authoritarian states that control, suppress and censor their information environments are also less vulnerable to cyber-enabled foreign interference.[76]

The proliferation of actors involved in elections and the digitisation of election functions has dramatically widened the attack surface available to foreign state actors. This has in large part been facilitated by the pervasive and persistent growth of social media and networking platforms, which has made targeted populations more accessible than ever to foreign state actors. For example, Russian operatives at the Internet Research Agency were able to pose convincingly as Americans online to form groups and mobilise political rallies and protests.[77] The scale of this operation wouldn’t have been possible without social media and networking platforms.

Figure 10: Number of people using social media platforms, July 2020 (million)



Source: 'Most popular social networks worldwide as of July 2020, ranked by number of active users', *Statista*, 2020, online.

While these platforms play an increasingly significant role in how people communicate about current affairs, politics and other social issues, they continue to be misused and exploited by foreign state actors.[78] Moreover, they have fundamentally changed the way information is created, accessed and consumed, resulting in an online information environment 'characterised by high volumes of information and limited levels of user attention'.[79]

In responding to accusations of election interference, foreign actors tend to deny their involvement and then deflect by indicating that the accusations are politically motivated. In 2017, following the release of the United States' declassified assessment of Russian election interference,[80] Russian Presidential Spokesperson Dmitry Peskov compared the allegations of interference to a 'witch-hunt' and stated that they were unfounded and unsubstantiated, and that Russia was 'growing rather tired' of the accusations.[81] Russian President Vladimir Putin even suggested that it could be Russian hackers with 'patriotic leanings' that have carried out cyber-enabled election interference rather than state-sponsored hackers.[82]

Plausible deniability is often cited in response to accusations of interference, with China's Foreign Ministry noting that the 'internet was full of theories that were hard to trace'.[83] China has attempted to deter future allegations by threatening diplomatic relations, responding to the allegations that it was behind the sophisticated cyber attack on Australia's parliament by issuing a warning that the 'irresponsible' and 'baseless' allegations could negatively impact China's relationship with Australia.[84]

Recommendations

The threats posed by cyber-enabled foreign interference in elections and referendums will persist, and the range of state actors willing to deploy these tactics will continue to grow. Responding to the accelerating challenges in this space requires a multi-stakeholder approach that doesn't impose an undue regulatory burden that could undermine democratic rights and freedoms. Responses should be calibrated according to the identified risks and vulnerabilities of each state. This report proposes recommendations categorised under four broad themes: identify, protect, detect and respond.

1. Identify

Identify vulnerabilities and threats as a basis for developing an effective risk-mitigation framework

- Governments should develop and implement risk-mitigation frameworks for cyber-enabled foreign interference that incorporate comprehensive threat and vulnerability assessments. Each framework should include a component that is available to the public, provide an assessment of cybersecurity vulnerabilities in election infrastructure, explain efforts to detect foreign interference, raise public awareness, outline engagement with key stakeholders, and provide a clearer threshold for response.[85]
- The security of election infrastructure needs to be continuously assessed and audited, during and in between elections.
- Key political players, including political campaigns, political parties and governments, should engage experts to develop and facilitate tabletop exercises to identify and develop mitigation strategies that consider the different potential attack vectors, threats and vulnerabilities.[86]

2. Protect

Improve societal resilience by raising public awareness

- Governments need to develop communication and response plans for talking to the public about cyber-enabled foreign interference, particularly when it involves attempts to interfere in elections and referendums.
- Government leaders should help to improve societal resilience and situational awareness by making clear and timely public statements about cyber-enabled foreign interference in political processes. This would help to eliminate ambiguity and restore community trust. Such statements should be backed by robust public reporting mechanisms from relevant public service agencies.
- Governments should require that all major social media and internet companies regularly report on how they detect and respond to cyber-enabled foreign interference. Such reports, which should include positions on political advertising and further transparency on how algorithms amplify and suppress content, would be extremely useful in informing public discourse and also in shaping policy recommendations.

Facilitate cybersecurity training to limit the effect of cyber-enabled foreign interference

- Cybersecurity, cyber hygiene and disinformation training sessions and briefings should be provided regularly for all politicians, political parties, campaign staff and electoral commission staff to reduce the possibility of a successful cyber operation, such as a phishing attack, that can be exploited by foreign state actors.[87] This could include both technical guides and induction guides for new staff, focused on detecting phishing emails and responding to DoS attacks.

Establish clear and context-specific reporting guidelines to minimise the effect of online information operations

- As possible targets of online information operations, researchers and reporters covering elections and referendums should adopt 'responsible' reporting guidelines to minimise the effect of online information operations and ensure that they don't act as conduits.[88] The guidelines should highlight the importance of context when covering possible strategic disclosures, social media manipulation and disinformation campaigns.[89] Stanford University's Cyber Policy Center has developed a set of guidelines that provide a useful reference point for reporters and researchers covering elections and referendums.[90]

3. Detect

Improve cyber-enabled foreign interference detection capabilities

- The computer systems of parliaments, governments and electoral agencies should be upgraded and regularly tested for vulnerabilities, particularly in the lead-up to elections and referendums.
- Greater investments by both governments and the private sector must be made in the detection of interference activities through funding data-driven investigative journalism and research institutes so that key local and regional civil society groups can build capability that stimulates and informs public discourse and policymaking.
- Governments and the private sector must invest in long-term research into how emerging technologies, such as 'deep fake' technologies,[91] could be exploited by those engaging in foreign interference. Such research would also assist those involved in detecting and deterring that activity.

4. Respond

Assign a counter-foreign-interference taskforce to lead a whole-of-government approach

- Global online platforms must take responsibility for enforcement actions against actors attempting to manipulate their online audiences. Their security teams should work closely with governments and civil society groups to ensure that there's a shared understanding of the threat actors and their tactics in order to create an effectively calibrated and collaborative security posture.
- Governments should look to build counter-foreign-interference taskforces that would help to coordinate national efforts to deal with many of the challenges discussed in this report. Australia's National Counter Foreign Interference Coordinator and the US's Foreign Influence Task Force provide different templates that could prove useful. Such taskforces, involving policy, electoral, intelligence and law enforcement agencies, should engage globally and will need to regularly engage with industry and civil society. They should also carry out formal investigations into major electoral interference activities and publish the findings of such investigations in a timely and transparent manner.

Signal a willingness to impose costs on adversaries

- As this research demonstrates that a small number of foreign state actors persistently carry out cyber-enabled election interference, governments should establish clear prevention and deterrence postures based on their most likely adversaries. For example, pre-emptive legislation that automatically imposes sanctions or other punishments if interference is detected has been proposed in the US Senate.[92]
- Democratic governments should work more closely together to form coalitions that develop a collective and publicly defined deterrence posture. Clearly communicated costs could change the aggressor's cost–benefit calculus.

Appendix

Africa

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Madagascar	2018	Election	Russia	Online information operation	According to the *New York Times*, Russia reportedly interfered in Madagascar's 2018 presidential elections through social media disinformation campaigns coordinated by a troll factory based in St Petersburg.[a] After the political candidate whom Russia initially backed lost an early vote, Russia quickly shifted support to Andry Rajoelina, who ultimately won the election.[b] That support came in the form of a 'disinformation campaign on social media' in addition to other, more traditional, forms of influence, such as paying people to attend rallies and bribing challengers to drop out of the race.[c] Authorities have traced those actions back to multiple Russian actors, including Yevgeny Prigozhin, a Russian businessman with ties to Vladimir Putin.[d] Prigozhin was indicted for playing a pivotal role in manipulating the 2016 US presidential election.[e]
Libya	2019	Election	Russia	Online information operation	According to *Bloomberg*, Libyan security forces discovered foreign interference attempts in the 2019 Libyan general election after two Russian citizens were arrested for allegedly working in a Russian troll farm linked to businessman Yevgeny Prigozhin.[f] Prigozhin was indicted for playing a pivotal role in manipulating the 2016 US presidential election.[g] The suspects worked for a troll farm that specialised in influencing African elections and reportedly met with Saif al-Islam Gaddafi (son of the late Libyan dictator) to assist in planning his election campaign.[h] In response to the arrests, the Russian-based Foundation for the Defense of National Values released a statement saying that there was no intervention in Libya's electoral process and that the suspects were merely carrying out sociological studies.[i] A Senior Fellow at the Carnegie Moscow Centre, Alexander Baunov, said that the objective of Russia's interference in Libya was to increase its influence across Africa.[j]
Mozambique	2019	Election	Russia	Online information operation	According to Stanford University's Internet Observatory, Russia launched a Facebook disinformation campaign in the weeks leading up to Mozambique's presidential and parliamentary elections in 2019.[k] The campaign consisted of a network of four Facebook pages that posted content supporting President Filipe Nyusi and the ruling party, Frelimo.[l] The pages also shared negative stories about the opposition party, Renamo, at least one of which was untrue. The networks of Facebook pages also drove users to encrypted messaging platforms such as WhatsApp and Telegram to increase engagement.[m] Facebook attributed the systems to Yevgeny Prigozhin, a Russian businessman with ties to Vladimir Putin, as part of a broader Russian interference campaign that targeted several other African countries, including Cameroon, Libya, and Sudan. Facebook has since removed the networks.[n]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
South Africa	2019	Election	Russia	Online information operation	According to *The Guardian*, documents prepared by an organisation linked to Yevgeny Progozhin, a Russian businessman with ties to Vladimir Putin, revealed a Russian-backed campaign to influence South Africa's general election.[o] The documents, which were under the guise of a research institution called the Association for Free Research and International Cooperation (AFRIC), demonstrated Russia's intentions to strengthen the ruling African National Congress party and discredit the opposing parties—the Democratic Alliance and the Economic Freedom Fighters.[p] According to US Special Counsel Robert Mueller, AFRIC is a branch of Russia's Internet Research Agency responsible for the social media operations that bolstered Trump's position during the 2016 US presidential elections.[q] Interference methods referred to in the documents included disseminating video content, coordinating with journalists and possibly social media manipulation to influence South African public rhetoric.[r]

a Michael Schwirtz, Gaelle Borgia, 'How Russia meddles abroad for profit: cash, trolls and a cult leader', *New York Times*, 11 November 2019, online; Nathaniel Gleicher, 'Removing More Coordinated Inauthentic Behavior From Russia', Facebook Newsroom, 30 October 2019, online.
b Luke Harding, Jason Burke, 'Leaked documents reveal Russian effort to exert influence in Africa', *The Guardian*, 11 June 2019, online.
c Schwirtz & Borgia, 'How Russia meddles abroad for profit: cash, trolls and a cult leader'.
d Freeman Spogli Institute for International Studies (FSI), *Evidence of Russia-linked influence operations in Africa*, Stanford University, 30 October 2019, online.
e Davey Alba, Sheera Frenkel, 'Russia tests new disinformation tactics in Africa to expand influence', *New York Times*, 30 October 2019, online.
f Samer Khalil al-Atruysh, Ilya Arkhipov, Henry Meyer, 'Libyan security forces arrest two Russians allegedly attempting to interfere in elections', *Time*, 5 July 2019, online; Luke Harding, Jason Burke, 'Leaked documents reveal Russian effort to exert influence in Africa'; Nathaniel Gleicher, 'Removing More Coordinated Inauthentic Behavior From Russia', Facebook Newsroom, 30 October 2019, online.
g Alba & Frenkel, 'Russia tests new disinformation tactics in Africa to expand influence'.
h FSI, *Evidence of Russia-linked influence operations in Africa*.
i al-Atruysh et al., 'Libyan security forces arrest two Russians allegedly attempting to interfere in elections'.
j al-Atruysh et al., 'Libyan security forces arrest two Russians allegedly attempting to interfere in elections'.
k FSI, *Evidence of Russia-linked influence operations in Africa*; Nathaniel Gleicher, 'Removing More Coordinated Inauthentic Behavior From Russia'.
l FSI, *Evidence of Russia-linked influence operations in Africa*.
m FSI, *Evidence of Russia-linked influence operations in Africa*.
n Alba & Frenkel, 'Russia tests new disinformation tactics in Africa to expand influence'.
o Jason Burke, Luke Harding, 'Documents suggest Russian plan to sway South Africa election', *The Guardian*, 9 May 2019, online.
p Burke & Harding, 'Documents suggest Russian plan to sway South Africa election'.
q Burke & Harding, 'Documents suggest Russian plan to sway South Africa election'.
r Burke & Harding, 'Documents suggest Russian plan to sway South Africa election'.

Australia

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Australia	2019	Election	China	Cyber operation	According to the *Sydney Morning Herald*, Australian Prime Minister Scott Morrison confirmed on 18 February 2019 that a hacker group had targeted the Liberal, Labor and National parties and accessed the fileservers at Parliament House ahead of the federal election.[a] The Prime Minister noted that the breach, which occurred on 8 February 2019, was the work of a 'sophisticated' but did not make any formal attributions.[b] A number of sources within the Australian Signals Directorate (ASD)—Australia's cyber intelligence agency—confirmed that their investigation had concluded China was responsible.[c]

a David Wroe, 'China key suspect in pre-election hack against major parties', *The Sydney Morning Herald*, 18 February 2019, online.
b Brett Worthington, 'Scott Morrison reveals foreign government hackers targeted Liberal, Labor and National parties in attack on Parliament's servers', *ABC News*, 18 February 2019, online.
c Colin Packham, 'Exclusive: Australia concluded China was behind hack on parliament, political parties – sources', *Reuters*, 16 September 2019, online.

Indo-Pacific

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Taiwan	2011	Election	China	Cyber operation	According to the *Taipei Times*, the email accounts of senior politicians from the Taiwanese Democratic Progressive Party (DPP) were compromised by hackers based in China and Taiwan.[a] The Deputy Director of the DPP's Research Committee linked the attacks to the presidential and legislative elections scheduled for January 2012.[b] A number of attacks could be attributed to IP addresses from the Beijing bureau of the Chinese state-backed media outlet *Xinhua* and the Taiwanese Executive Yuan's Research, Development and Evaluation Commission.[c] The DPP confirmed that 'confidential campaign information', such as minutes of international meetings and the presidential campaign itinerary, were targeted. Research, Development and Evaluation Commission Minister Sung Yu-Hsieh denied any involvement in the attacks but indicated that the Government Service Network might have been involved.[d]
Hong Kong	2016	Election	China	Cyber operation	According to *Bloomberg*, a Chinese-backed phishing attack targeted two Hong Kong Government agencies just weeks before Hong Kong's legislative elections in 2016.[e] American cybersecurity firm FireEye reported that the perpetrators, who were believed to be connected with the Chinese APT3 cyber-espionage group, launched a spear-phishing attack through emails containing malware-infected hyperlinks and attachments. John Watters, president of iSIGHT (a unit within FireEye), stated that the attacks were 'certainly' politically motivated.[f] The Hong Kong Office of the Government Chief Information Officer confirmed that 'the systematic operations of the concerned departments' were not affected and no leaks were reported.[g]
Cambodia	2018	Election	China	Cyber operation	According to *Nikkei Asian Review*, China attempted to interfere in the 2018 Cambodian election to secure Hun Sen's leadership.[h] American cybersecurity firm FireEye reported that Chinese-backed hackers targeted several of Hun Sen's political opponents as well as a number of government bodies, including the National Election Commission, through repeated online attacks.[i] The attacks resulted in unauthorised access to government information and opposition activities, which FireEye linked to a server in Hainan, China.[j]
Hong Kong	2018	Election	China	Cyber operation	According to American cybersecurity firm FireEye, Chinese cyber-espionage actors used malware to target 'Hong Kong entities' in October 2018, one month before a November by-election.[k] FireEye identified the activity as election-related.
Malaysia	2018	Election	China	Cyber operation	According to American cybersecurity firm FireEye, suspected Chinese threat actors targeted multiple government agencies with phishing emails leading up to the 2018 Malaysian general election.[l] FireEye identified the activity as election-related.

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Taiwan	2018	Election	China	Cyber operation	According to American cybersecurity firm FireEye, suspected Chinese threat actors targeted Taiwanese government entities with election-themed phishing emails leading up to the 2018 Taiwanese local elections.[m] FireEye identified the activity as election-related.
Taiwan	2018	Election	China	Online information operation	According to the *New York Times*, Taiwanese officials alleged that the People's Republic of China launched an online disinformation campaign in the lead-up to Taiwanese 2018 midterm elections to undermine the Democratic Progressive Party (DPP), which is led by President Tsai Ing-Wen, and support 'candidates more sympathetic to Beijing', specifically those of the Kuomintang (KMT).[n] According to Taiwanese Foreign Minister Joseph Wu, disinformation and propaganda was being spread 'not from newspapers or [China's] propaganda machine but through [Taiwan's] social media, online chat groups, Facebook, the zombie accounts set up, somewhere, by the Chinese government'.[o] According to *Foreign Policy*, a professional Chinese cyber group launched a social media manipulation campaign that targeted the 2018 local elections.[p] The group created an unofficial Facebook page called 'Han Kuo-yu Fans for Victory! Holding up a Blue Sky!' one day after Han Kuo-yu, who is from the KMT, declared candidacy for Kaohsiung's mayoral race. The group amassed more than 61,000 members and was used as a platform to disseminate and amplify 'talking points, memes, and very often fake news' against Kuomintang dissenters and the opposing DPP.[q] After the election, it was found that the administrators of the Facebook group had fake LinkedIn profiles indicating that they were employees of the Chinese technology company Tencent. Professor Ying-Yu Lin of the National Chung Cheng University suggested that the cyber group was connected to the Chinese military's Strategic Support Force, initiated by President Xi Jinping.[r]
Indonesia	2019	Election	Russia	Cyber operation	According to *Bloomberg*, the head of Indonesia's General Election Commission (KPU), Arief Buidman, alleged that Russian hackers had attempted to discredit the polling process ahead of Indonesia's 2019 election by targeting the country's voter database.[s] It was reported that attempts were made by the hackers to 'manipulate and modify' content in the database and create fake voter identities, otherwise known as 'ghost voters'.[t]
Indonesia	2019	Election	China	Cyber operation	According to Bloomberg, the head of Indonesia's General Election Commission (KPU), Arief Buidman, alleged that Chinese hackers had attempted to discredit the polling process ahead of Indonesia's 2019 election by targeting the country's voter database.[u] It was reported that attempts were made by the hackers to 'manipulate and modify' content on Indonesia's voter database and create fake voter identities, otherwise known as 'ghost voters'.[v]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Israel	2019	Election	Iran	Cyber operation	According to *Haaretz*, Israel's security service, Shin Bet, alleged that hackers linked to Iran accessed the phone of Benny Gantz, the leader of the centrist political alliance Kahol Lavan, to retrieve personal information and professional correspondence.[w] The data breach's timing raised concerns that the stolen information could be used to discredit Gantz and undermine his candidacy against Prime Minister Benjamin Netanyahu ahead of the Israeli legislative election on 9 April 2019.[x]
South Korea	2020	Election	North Korea	Cyber operation	According to *Radio Free Asia*, private security companies EST Security and AhnLab found evidence of a phishing attack by North Korea against former North Korean citizens who were running in South Korea's legislative elections on 15 April 2020.[y] Both security companies found that the North Korean hacking organisation Kimsusky attempted to access personal computers through spear phishing by using documents containing private information on the candidates' names, dates of birth, academic backgrounds and family histories. The documents were titled under the mysterious name of 'Director Jai-Chun Lee'. According to EST Security, the attackers targeted computers by installing malware to collect information and carry out further attacks.[z]
Taiwan	2020	Election	China	Online information operation	According to *The Guardian*, Taiwan faced a disinformation campaign alleged to have originated from mainland China just weeks before the 2020 national election.[aa] According to Tzeng Yi-Suo, the director of the Cyber-warfare Division at Taiwan's Institute for National Defence and Security Research, elements of this campaign involved the instant distribution of artificial-intelligence-generated fake news to social media platforms.[ab] It was also reported that a large number of online trolls and fake social media accounts shared pro-China content and left thousands of comments under a presidential candidate's post or news articles in order to alter search algorithms.[ac] The motive behind this disinformation campaign was to create mass confusion through divide-and-rule tactics.[ad]

a Chris Wang, 'Hackers attack DPP's presidential campaign office', *Taipei Times*, 10 August 2011, online.
b 'Taiwan party: Chinese hacked us', *News24*, 9 August 2011, online.
c Wang, 'Hackers attack DPP's presidential campaign office'.
d Wang, 'Hackers attack DPP's presidential campaign office'.
e David Tweed, 'Hong Kong Government hacked by Chinese cyberspies, FireEye says', *Bloomberg*, 2 September 2016, online; Center for Strategic & International Studies (CSIS), *Significant cyber incidents since 2006*, CSIS, Washington DC, no date, online.
f Raymond Yeung, 'Two government agencies in Hong Kong attacked by hackers, US firm says', *South China Morning Post*, 2 September 2016, online.
g Yeung, 'Two government agencies in Hong Kong attacked by hackers, US firm says'.
h Yuichiro Kanematsu, 'Fears of Chinese cybermeddling grow after Cambodia election', *Nikkei Asia*, 18 August 2018, online.
i David Tweed, 'Chinese cyber sleuths target Cambodia as election looms', *Sydney Morning Herald*, 11 July 2018, online.
j Kanematsu, 'Fears of Chinese cybermeddling grow after Cambodia election'.
k FireEye, *Cyber threat activity targeting elections*, 2019, online.
l FireEye, *Cyber threat activity targeting elections*.
m FireEye, *Cyber threat activity targeting elections*; Reuters, 'Taiwan says China behind cyberattacks on government agencies, emails', *CISO.in*, 19 August 2020, online.
n Raymond Zhong, 'Awash in disinformation before vote, Taiwan points finger at China', *New York Times*, 6 January 2020, online; Keoni Everington, 'China's 'troll factory' targeting Taiwan with disinformation prior to election', *Taiwan News*, 5 November 2018, online.
o James Reinl, '"Fake news" rattles Taiwan ahead of elections', *al-Jazeera*, 23 November 2019, online.
p Paul Huang, 'Chinese cyber-operatives boosted Taiwan's insurgent candidate', *Foreign Policy*, 26 June 2019, online.
q Internet Observatory, *Taiwan: presidential election 2020 scene setter*, Stanford University, 26 August 2019, online.
r Internet Observatory, *Taiwan: presidential election 2020 scene setter*; Keoni Everington, 'China's "troll factory" targeting Taiwan with disinformation prior to election', *Taiwan News*, 5 November 2018, online.

s Viriya Singgih, Arys Aditya, Karlis Saln, 'Indonesia says election under attack from Chinese, Russian hackers', *Bloomberg*, 13 March 2019, online.
t Kate Lamb, 'Indonesia election mired in claims of foreign hacking and "ghost" voters', *The Guardian*, 19 March 2019, online.
u Singgih et al., 'Indonesia says election under attack from Chinese, Russian hackers'.
v Lamb, 'Indonesia election mired in claims of foreign hacking and "ghost" voters'.
w 'Israel suspects Iran of hacking election frontrunner Gantz's phone: TV', *Reuters*, 15 March 2019, online.
x 'Israel says Iran hacked ex-general Gantz's phone ahead of election', *Haaretz*, 15 March 2019, online.
y 'Security companies in South Korea discover North Korean cyberattack', *Radio Free Asia*, 10 April 2020, online.
z 'Security companies in South Korea discover North Korean cyberattack'.
aa Lily Kuo, 'Taiwan's citizens battle pro-China fake news campaigns as election nears', *The Guardian*, 30 December 2019, online.
ab Philip Sherwell, 'China uses Taiwan for AI target practice to influence elections', *The Australian*, 5 January 2020, online.
ac Kuo, 'Taiwan's citizens battle pro-China fake news campaigns as election nears'.
ad Sherwell, 'China uses Taiwan for AI target practice to influence elections'.

Europe

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Ukraine	2014	Election	Russia	Cyber operation	According to *Bloomberg*, a hacktivist group connected to the Russian Government and known as CyberBerkut infiltrated the Ukrainian Central Election Commission and took down the vote-tallying system four days before the presidential election on 25 May 2014.[a] The election results were changed to falsely display the winner as Dmytro Yarosh, an ultra-right political candidate and commander of the Ukrainian Volunteer Army.[b] Despite the data breach, CyberBerkut didn't change the election outcome, and commission officials successfully prevented the altered results from being shown publicly.
Ukraine	2014	Election	Russia	Online information operation	According to *Bloomberg*, a hacktivist group connected to the Russian government and known as CyberBerkut shared material relating to the election commission's network maps, system logs and member emails on its website before declaring that it had 'destroyed the computer network infrastructure'.[c] The group also managed to coordinate with Russian state media to falsely broadcast Dmytro Yarosh as the winner.[d]
UK	2014	Referendum	Iran	Online information operation	According to *The Herald*, multiple Facebook pages were taken down ahead of the 2014 Scottish independence referendum after they were discovered to be fake Iranian-backed accounts.[e] A pro-independence page called 'Free Scotland 2014', for example, was involved in spreading fake news to more than 20,000 of its followers about Jeremy Corbyn, Boris Johnson, Donald Trump, and the British monarch. The page was also connected to a series of Iranian state-backed media outlets.[f] Twitter confirmed that it shut down a further 284 fake accounts, most of which originated from Iran, for engaging in inauthentic coordinated manipulation.[g] The motive behind the fake accounts was to promote left-wing and anti-Western opinions by targeting British voters.[h]
UK	2014	Referendum	Russia	Online information operation	According to *The Guardian*, Russian activists reportedly organised a disinformation campaign to undermine the Scottish independence referendum result.[i] The activists created fake accounts on Facebook, Twitter and YouTube to share false allegations of vote-rigging and sparked petitions demanding a national recount of the vote. One online petition garnered more than 100,000 supporters.[j] The allegations were rejected by Scottish electoral officials.[k] An expert in Russian cyber operations at the Atlantic Council, Ben Nimmo, said there was 'significant circumstantial evidence to show the Russians had preferred videos purporting to show interference in the vote counts … to skew the result in favour of the no campaign'.[l]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Bulgaria	2015	Election and Referendum	Russia	Cyber operation	According to *BBC News*, Bulgaria was subjected to a distributed DoS attack on the day a referendum and local elections were held.[m] The Bulgarian President said that there was a 'high probability' that the attack came from Russia.[n] The attack was aimed at causing confusion about the results. The head of the state-owned Information Services, which was responsible for counting the vote, stated that the attack wouldn't affect either the results of the elections or the referendum.[o]
Poland	2015	Election	Russia	Online information operation	According to social network mapping and analysis company Graphika, the Russian-backed Secondary Infektion operation deployed a disinformation attack against the leader of Poland's right-wing Law and Justice Party, Jarosław Kaczyński, ahead of the 2015 presidential and parliamentary elections.[p] The operation built a narrative over several months to discredit Kaczynski, who's an outspoken critic of President Vladimir Putin, by alleging that he suffers from a genetic disorder with symptoms of 'high excitability, uncontrolled manifestation of panic and aggression'.[q] The creation of the narrative was achieved by spreading fake articles across different language platforms, fabricating a leak on the CyberGuerrilla Anonymous Nexus forum, and running a global petition on the American activism website Avaaz.[r]
Italy	2016	Referendum	Russia	Online information operation	According to the *New York Times*, a wave of fake news, much of which originated from Russian sources, circulated throughout social media in the lead-up to the 2016 Italian constitutional referendum.[s] *BuzzFeed News* reported that 'leaders of Italy's most popular political party, the anti-establishment Five Star Movement', favoured sharing stories that were based on Russian propaganda across their platforms.[t] Russian state-backed media *RT* released a video that it claimed showed thousands protesting against the referendum when in fact the rally was in favour of the referendum.[u] The video was viewed 1.5 million times.[v]
Montenegro	2016	Election	Russia	Online information operation	According to *NBC News*, in the lead-up to the 2016 Montenegrin parliamentary election, the Russian Government 'launched a coordinated disinformation campaign using traditional and social media to allege widespread voting irregularities'.[w] Social media networks were inundated with public complaints, which forced the Montenegrin Government to temporarily shut down WhatsApp, Viber and similar messaging apps.

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Montenegro	2016	Election	Russia	Cyber operation	According to *Balkan Insight*, Montenegro's Ministry for Information Society and Telecommunications reported a series of distributed DoS attacks against media and state institutions (including the website the ruling Democratic Party of Socialists of Montenegro) during the 2016 parliamentary elections.[x] Several anti-censorship blogs reported that Montenegro's Centre for Democratic Transitions (an NGO that promotes democracy and good governance in the country) was rendered inaccessible on election day. Media outlets *CDM* and *Antena M* and the telecommunications carrier Crnogorski Telekom also experienced a similar wave of cyberattacks during that period. Although the Montenegrin state authorities did not publicly attributed the attacks to Russia, an investigation into the denial of service attacks hinted at 'a Russian role'.[y] The Montenegrin Government was also subjected to a credential phishing attack four days after the elections on 20 October 2016, according to cybersecurity firm Trend Micro.[z] Security analysts indicated that the Russian hacktivist group Fancy Bear was probably behind the attack. Pierluigi Paganini, a security analyst at the EU Agency for Network and Information Security, identified the motive behind this attack as Russia's attempt to undermine Montenegro's role in NATO amid its accession process.[aa]
The Netherlands	2016	Referendum	Russia	Online information operation	According to the *New York Times*, Dutch left-wing politician Harry van Bommel's efforts to convince Dutch voters to reject the EU–Ukraine trade referendum in 2016 were supported by a group of Russians.[ab] In addition to attending public meetings and appearances,[ac] the Russians used social media to spread disinformation, including a video that reportedly showed members of the Ukrainian National Guard burning the Dutch flag and threatening to carry out attacks against the Dutch if they voted against the trade agreement.[ad]
UK	2016	Referendum	Iran	Online information operation	According to *The Telegraph*, a network of Iranian internet trolls on Twitter attempted to divide public opinion by spreading divisive information on the day of Britain's EU membership referendum.[ae] More than 770 Iranian Twitter accounts were found to have been engaged in coordinated manipulation by spreading disinformation on British politicians Nigel Farage and Boris Johnson while praising the leader of Britain's opposition Labour Party, Jeremy Corbyn.[af]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
UK	2016	Referendum	Russia	Online information operation	According to *NPR*, British national security and law enforcement authorities found overlapping characteristics between Russian-backed disinformation campaigns in the 2016 US presidential election and the Brexit referendum.[ag] Researchers at the University of London found that there was a sudden deactivation of 13,493 fake Twitter accounts and a further 26,500 username changes in the weeks following the Brexit referendum.[ah] The users showed a 'clear slant towards the leave campaign' and posted around 65,000 messages over four weeks, and only 56% of the users authored original tweets. Interestingly, some of the bot accounts also tweeted pro-Remain content. Researcher Dr Dan Mercea suggests that the aim was to 'swell artificial levels of public support for different sides of the vote' and create a 'false impression of public popularity.'[ai] The UK government's official response was that they had found no evidence of successful interference in the EU referendum. However, a report from the UK Parliament's intelligence and security committee found that the government had 'actively avoided looking for evidence that Russia interfered'.[aj]
Armenia	2017	Election	Russia	Online information operation	According to the Atlantic Council's Digital Forensic Research Lab (DFRLab), a disinformation campaign was mobilised by Russian Twitter bots during the 2017 Armenian parliamentary elections.[ak] A key element of the campaign was the dissemination of a fake email purporting to be from the US Agency for International Development that claimed that the US intended to influence the Armenian elections by providing support to the opposing Way Out Party and the Free Democrats Party. Although the email was quickly debunked by the US Embassy in Yerevan due to several spelling errors and having been sent from a Gmail account, a corrected version of the email was reshared on Pastebin. The campaign also involved targeted suspensions of four key Armenian journalist accounts on Twitter the night before the election (all of which were unblocked after civil society activists reached out to Twitter), as well as two hacking attempts against prominent Armenian scholar Babken DerGrigorian.[al]
Czech Republic	2017	Election	Russia	Online information operation	According to *The Guardian*, Russian state-backed media outlets Sputnik and RT published disinformation, mainly concerning migrants, to disrupt the public discourse in the lead up to the Czech Republic's 2017 legislative elections.[am] The Czech State Secretary for European Affairs Tomáš Prouza commented that Russia was aiming to "sow doubts into the minds of the people that democracy is the best system to organise a country...and discourage people from participation in the democratic processes."[an]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Czech Republic	2017	Election	Russia	Cyber operation	According to *The Guardian*, the Czech Republic's Ministry of Foreign Affairs suffered a sophisticated data breach after hackers compromised dozens of email accounts belonging to senior diplomats ahead of the 2017 legislative elections.[ao] It was reported that thousands of files were downloaded from the ministry's external mailing system. It was widely acknowledged within the Czech ministry that Russia was behind the attack, although no public attribution was made.[ap] Vlado Bizik, a cybersecurity expert with the Prague-based European Values think tank, drew similarities between this attack and one Poland had recently suffered, which was attributed to Russia.[aq]
France	2017	Election	Russia	Cyber operation	According to the *New York Times*, En Marche! revealed in a statement that it had been the target of a 'massive, coordinated act of hacking' and that the hackers had obtained internal information, such as emails and documents.[ar] According to the Carnegie Endowment for International Peace, the hackers used spear-phishing emails to get campaign staff's login credentials.[as] The emails redirected the targets to a fake Microsoft storage website where they were asked to enter their login details. Facebook confirmed that Russian operatives had set up 12 fake accounts and posed as acquaintances of people close to Macron to gain personal information.[at] In the days leading up to the election, '9 gigabytes of stolen files and 21,000 emails' obtained from the hack were leaked online.[au]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
France	2017	Election	Russia	Online information operation	According to *Wired*, just before the final vote between Emmanuel Macron and Marine Le Pen on 5 May 2017, nine gigabytes of files and 21,000 emails that had previously been stolen in the October 2016 data breach were released on the anonymous document-sharing website Pastebin under the username 'EMLEAKS'.[av] Two months later, the documents and emails leaked to Pastebin were republished on WikiLeaks using the hashtag #MacronLeaks.Macron's party, La République En Marche!, claimed that its computer systems were subject to thousands of attacks originating from Russia.[aw] Japanese cybersecurity firm Trend Micro confirmed that the initial phishing emails had been traced back to the Russian-backed hacker group Fancy Bear, which is an instrument of Russia's Main Intelligence Directorate (GRU).[ax] According to *The Guardian*, Russian state-backed media outlets were involved in the dissemination of disinformation in the lead-up to France's 2017 presidential election.[ay] France's polling commission raised concerns over an article that contradicted 'the findings of mainstream opinion polls' by placing François Fillon, the conservative presidential candidate, as the leading candidate. The article was posted and shared by several Russian state-backed media outlets including *Russia Today* (*RT*) and *Sputnik*. Richard Ferrand, who was then the general secretary of En Marche!, and French presidential candidate Emmanuel Macron were also targeted in this disinformation campaign.[az] Macron, who was the only candidate 'unequivocally critical of Vladimir Putin's Russia', was the primary target of the conspiracies and false narratives, which were spread by a 'network of hyperactive automated accounts (bots)' expressing pro-Russian, anti-EU views.[ba] In contrast, Russian state-backed media revealed a strong bias towards pro-Russian candidates such as Marine Le Pen, François Fillon and Jean-Luc Mélenchon. French social media monitoring firm *Reputatio Lab* estimated that the Russian-backed news outlets reached an audience of around 145,000 people.[bb]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Germany	2017	Election	Russia	Online information operation	According to *Politico*, German Chancellor Angela Merkel was targeted by a large-scale disinformation campaign organised by the Russian cyber operation Secondary Infektion shortly before the 2017 federal election.[bc] The European East StratCom Task Force reported more than 2,500 examples in 18 different languages of fake news in Germany, France, and the Netherlands at that time. According to the Atlantic Council's Digital Forensic Research Lab (DFRLab), Russian-language bots amplified a narrative from the far-right Alternative für Deutschland party 'warning about possible fraud and calling on supporters to volunteer as election observers'.[bd] Russian social media platform Vkontakte (VK), which reportedly 'boasts a significant German audience' and is 'the 8th most popular website in Germany based on traffic', was a key platform through which this and other fake news stories were amplified.[be] After the election, Secondary Infektion launched a further disinformation campaign claiming that Angela Merkel's Christian Democratic Union only won because millions of new immigrants voted for the party.[bf] The campaign involved an article containing a fabricated screenshot of a tweet attributed to the former director for the Office for Democratic Institutions and Human Rights, Michael Georg Link, which reported that 98% of recent German citizens voted for the party.[bg]
Germany	2017	Election	Russia	Cyber operation	According to *Reuters*, the German Federal Office for Information Security confirmed that two political think tanks tied to the Christian Democratic Union and the Social Democratic Party were subjected to Russian-backed phishing attacks.[bh] 'German officials and lawmakers say the attacks are the latest in a series aimed at disrupting German elections and damaging Chancellor Angela Merkel, who has pushed to maintain sanctions on Russia over its actions in eastern Ukraine'.[bi] The hacker group used phishing emails to install malicious software at the Konrad Adenauer Foundation and the Friedrich Ebert Foundation, but the attacks were successfully resisted.[bj] While Russia denied involvement in the phishing attacks, experts indicated that they were carried out either by Pawn Storm, a Russian hacking group responsible for attacks on the French and American political processes, or Fancy Bear, which is linked to the Russian Main Intelligence Directorate (GRU).[bk]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Malta	2017	Election	Russia	Cyber operation	According to *The Guardian*, Russian-backed hackers attempted to access and disrupt the Maltese Government's server in the month before Malta's 2017 general election.[bl] A source working within the Maltese Government's IT agency said that the hackers had attempted to gain access to the IT system by sending phishing emails, distributed DoS attacks and the use of malware. Around 5 million phishing emails were sent in the month leading up to the election. The Russian hacker group Fancy Bear had been identified by a 'confidential external risk assessment' as the source of the attack.[bm] *The Guardian* reported that 'the attacks come after recent claims from the prime minister, Joseph Muscat, that a foreign intelligence agency had suggested Malta would become a target for a Russian disinformation campaign.'[bn]
The Netherlands	2017	Election	Russia	Online information operation	According to the annual report of the General Intelligence and Security Service of the Netherlands (Algemene Inlichtingen-en Veiligheidsdienst, AIVD), Russia had attempted to influence the 2017 Dutch general election through the dissemination of disinformation.[bo] Rob Bertholee, the then head of the AIVD, noted that Russia had 'tried to push voters in the wrong direction by spreading news items that are not true, or partially true.' Journalists from *NRC Handelsblad* reported that voters had been encouraged to vote for far-right politician Geert Wilders and the far-right PVV party by social media accounts linked to the Russian Internet Research Agency (IRA).[bp]
The Netherlands	2017	Election	Russia	Cyber operation	According to *de Volkskrant*, two Russian-backed hacker groups (Fancy Bear and Cozy Bear) attempted to gain online access to a number of ministries in the Netherlands, including the Ministry of General Affairs, which includes the Prime Minister's office.[bq] The hacking attempts took place over six months in the lead-up to the Dutch general election, although they were ultimately unsuccessful in obtaining any confidential information or credentials. Rob Bertholee, head of the General Intelligence and Security Service of the Netherlands, confirmed that it was Russia that was 'trying to penetrate secret government documents'.[br]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Spain	2017	Referendum	Russia	Online information operation	According to *El País*, the Russian state-backed media outlets *Sputnik* and *RT* were openly spreading disinformation and propaganda in favour of Catalan independence in the lead-up to the referendum in 2017.[bs] *RT Actualidad*, *RT*'s Spanish-language outlet, 'spread stories on the Catalan crisis with a bias against constitutional legality', notably misrepresenting the EU's position regarding the referendum. Between 27 August and 28 September 2017, *RT Actualidad* published 42 articles about the Catalan referendum, all of which promoted some form of disinformation. Visiting scholar at George Washington University Professor Javier Lesaca analysed more than 5 million social media posts between 29 September and 5 October 2017 and found an 'entire army of zombie accounts' dedicated to sharing that content from *Sputnik* and *RT*. Lesaca noted that 'the digital disruption' observed in the public discourse surrounding the 2016 US presidential election and the 2016 Brexit referendum was observed in the lead-up to the Catalonia referendum, and that the 'authors of the disruption are the very same'. Tweets by WikiLeaks founder Julian Assange criticising the Spanish Government were also artificially amplified by bot accounts linked with Russia.[bt]
Czech Republic	2018	Election	Russia	Online information operation	According to *Balkan Insight*, the 2018 Czech Republic presidential elections faced a Russian-backed disinformation campaign, in support of pro-Russia candidate Milos Zeman, who ultimately won 'his second term by a slender majority of around 150,000 votes'.[bu] The campaign portrayed Zeman's political opponent Jiří Drahoš as a former collaborator with the communist secret police, a supporter of unrestricted immigration, a paedophile, and a puppet of foreign interests.[bv] The Center for European Policy Analysis' Elf Army identified that this disinformation activity increased when Zeman was publicly criticised in Czech media and when Czech Prime Minister Andrej Babis encountered any political scandals. Complementary to this, Jakub Kalensky, senior fellow at the Atlantic Council, stated that Zeman was 'one of the five EU politicians quoted in the Russian state media most frequently' which he argued had the effect of exaggerating Zeman's significance within the EU. In a report to the US Congress, Kalensky attributed this disinformation campaign during the 2018 election to Russia.[bw]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Italy	2018	Election	Russia	Online information operation	According to *The Local Italy*, five Twitter accounts with 'similar characteristics to those of Russian trolls' were engaged in the dissemination of disinformation and propaganda in the lead-up to the 2018 Italian elections, providing a one-sided representation of the political discourse in favour of the populist parties.[bx] Russian-backed hackers reportedly stole Italian citizens' identities and posed as political activists to manipulate public discourse. Moreover, the Russian state-backed media outlets Sputnik and RT played a significant role in creating and sharing anti-immigration narratives in the lead up to the elections.[by] Alto Data Analytics examined the polarising role of Russian state-backed media outlets within Italy's societal debates and found that they published content that exploited local narratives.[bz]
Lithuania	2018	Election	Russia	Online information operation	According to Graphika, former Lithuanian President Dalia Grybauskaite was subjected to disinformation attacks by the Russian-backed Secondary Infektion group during the 2018 Lithuanian presidential election campaigns.[ca] The group spread accusations on social media that Grybauskaite was supported by the CIA and the KGB and was a former prostitute and an agent of the Chinese Government seeking to undermine the EU.[cb] The group also fabricated a fake KGB letter claiming that Grybauskaite worked as a KGB informer during her studies in Moscow and was previously detained for 'immoral behaviour in public places' in 1982. The letter was subsequently shared by Russian-backed media outlets, including in a video feature by *Sputnik*. Although Grybauskaitė was unable to run for the presidency due to the Lithuanian constitutional limit of two terms in office, the attack was likely to undermine her presidency's validity and hinder public confidence in the government.[cc] The message that the next Lithuanian President should renew strong ties with Moscow was also amplified by Russian actors.[cd]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
North Macedonia	2018	Referendum	Russia	Online information operation	According to the *New York Times*, Russian operatives used Facebook to disseminate disinformation and depress voter turnout in the lead-up to the 2018 Macedonian referendum.[ce] They reportedly used Facebook to spread and promote false articles and posts that would 'heighten social divisions, drive down participation and amplify public anger'. A key focus of the disinformation campaign was to encourage Macedonians to boycott the vote, and hundreds of new websites appeared online urging Macedonians to 'burn their ballots'. As the referendum required 50% of registered voters to participate for it to be valid, that particular tactic was significant. Moreover, the Atlantic Council's Digital Forensic Research Lab found that the coverage provided by Russian state-backed media outlets *Sputnik* and *RT* in the lead-up to the referendum was unbalanced, providing one-sided content to create confusion and polarise Macedonia's information environment.[cf] An article that was widely shared falsely warned that Google would remove Macedonian from its list of recognised languages, depending on the outcome of the vote. Similarly, before the Macedonians were due to vote, *Sputnik* published an article falsely claiming that 'between 80% and 90% of Macedonians will boycott the referendum'. While the Macedonian Government declined to speculate on the source of the interference, in comments to reporters, then US Defense Secretary James Mattis accused Russia of financing 'influence campaigns' to spread disinformation ahead of the referendum.[cg]
North Macedonia	2018	Referendum	UK	Online information operation	According to the Bureau of Investigative Journalism, British PR agency Stratagem International, which specialises in 'under the radar' operations to influence voters, was employed by the Macedonian Government to assist with the 'Yes' campaign in the 2018 referendum and received funding from the UK's Foreign and Commonwealth Office.[ch] Stratagem International confirmed that it was being funded by the Foreign Office as 'a resource for the referendum Taskforce (Yes Campaign)'.[ci]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Sweden	2018	Election	Russia	Online information operation	According to the London School of Economics' Institute of Global Affairs, Russian state-backed media outlets launched a disinformation campaign alleging election fraud ahead of the 2018 Swedish general election.[cj] The narrative of election fraud was also pushed on social media closer to election day; the Swedish Civil Contingencies Agency reported 13,558 Twitter posts using different 'election fraud' hashtags. A report by Graphika showed that the Russian Secondary Infektion operation forged a fake blog post attributed to Swedish politician Carl Bildt that called for a 'Mueller Commission' investigation into alleged interference in the Swedish election.[ck] This campaign aimed to undermine trust in the Swedish democratic system by targeting people's core belief in free and fair elections.[cl] Russian state-backed media outlets *RT* and *Sputnik* also published more than 520 stories on Sweden between 16 July and 8 September 2018, with a noticeable increase in the two weeks leading up to the election.[cm] The publications demonstrated partisan bias by giving positive coverage of the Alternative for Sweden, the Sweden Democrat and the Pirate Party campaigns.[cn] At the same time, the Swedish Government and the EU endured substantially negative coverage.[co] Russian-language social media groups were also promoting far-right smear campaigns and generating abusive comments after the election to undermine the results' credibility.[cp]
EU	2019	Election	Russia	Cyber operation	According to *Deutsche Welle*, Russian state-backed hacker group Fancy Bear targeted European institutions with phishing emails in the lead-up to the 2019 European Parliament elections.[cq] The discovery was made by Microsoft, which detected multiple Russian-based hacking attempts on pro-democracy think tanks and NGOs specialising in election security, nuclear policy and foreign relations several months before the elections.[cr] Between September and December 2018, phishing attacks were launched against 104 different online accounts owned by think tank employees from the Aspen Institute, the German Council for Foreign Relations and the German Marshall Fund.[cs]
EU	2019	Election	Russia	Online information operation	According to *Deutsche Welle*, European authorities have reported that Russia interfered in the EU's parliamentary elections in May 2019.[ct] It was revealed that Russian state-backed groups attempted to undermine the credibility of the EU, suppress voter turnout and sway voter preferences by conducting disinformation campaigns on Facebook, Twitter and YouTube.[cu] The disinformation campaigns focused on downplaying the significance of the European Parliament and supporting parties that are Euro-skeptic or pro-Russia.[cv]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Finland	2019	Election	Russia	Cyber operation	According to *Bloomberg*, the Finnish National Bureau of Investigation (Keskusrikospoliisi, KRP) confirmed that a web service used to publish vote tallies was targeted by a DoS attack a week before the national election was held.[cw] The attack had the potential to impede the reporting of the election results and undermine the public's trust. Finnish authorities declined to publicly speculate on the source of the DoS attack. However, *Cybersecurity Insiders* noted that it was 'suspected to be the work of hackers backed by Russian Intelligence'.[cx]
Slovakia	2019	Election	Russia	Online information operation	According to the National Endowment for Democracy, a disinformation campaign allegedly linked to Russian state-backed media and diplomatic representatives targeted political candidates during the 2019 Slovakian presidential election.[cy] Attempts were reportedly made by 14 different media outlets and disinformation pages on Facebook to publish content supporting pro-Kremlin judge and politician Stephan Harabin while smearing the now President Zuzana Caputova, drawing on issues involving immigration, gender equality and anti-Semitic conspiracy theories.[cz] The narratives were further disseminated by members of the Slovakian Government's ruling coalition.
Ukraine	2019	Election	Russia	Online information operation	According to the *New York Times*, the Security Service of Ukraine (Sluzhba Bezpeky Ukrayiny, SBU) reported that it had countered a Russian attempt to use Facebook to undermine the vote in the 2019 Ukrainian elections.[da] In an effort to circumvent Facebook's new safeguards and interfere in the elections, instead of setting up fake accounts, Russian operatives sourced 'people in Ukraine on Facebook who wanted to sell their accounts or temporarily rent them out' and then used the accounts to manipulate voter attitudes through the dissemination of disinformation. Shortly before the elections, Facebook removed 41 Instagram accounts operated by the Internet Research Agency troll organisation in Russia that published posts targeting central and western Ukrainians.[db] Following the first round of voting, Russian state-backed media outlets criticised the results, which placed Volodymyr Zelenskiy ahead in the polls.[dc] Articles published by those outlets claimed that the election was 'a rigged contest' and falsely linked Zelenskiy to the 2019 Notre Dame fire in an effort to undermine his electability.[dd]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Ukraine	2019	Election	Russia	Cyber operation	According to *Kyiv Post*, the website of the presidential candidate, Volodymyr Zelenskiy, was subjected to a distributed DoS attack on 1 January 2019.[de] The attack occurred after Zelenskiy announced his intention to run for the presidency and called on his supporters to join his team by registering online using the website. The website received 5 million requests within minutes of its launch and was quickly taken offline. While Zelenskiy and his team declined to speculate on the source of the attack, *Vice* reported that cyber experts suspected Russia as the source of the attack.[df] As the election neared, state-backed hackers from Russia targeted the Central Elections Commission (CEC) and its employees with phishing emails infected with malware.[dg] The head of Ukraine's Cyber Protection Centre, Roman Boyarchuk, confirmed that from December 2018 around 8,000 targeted phishing emails were sent per week, as hackers attempted to probe the CEC website and obtain information on the communication network used to report the election results. In addition to the phishing attacks, the CEC was subjected to distributed DoS attacks on 24 and 25 February.[dh] Ukraine's then President, Petro Poroshenko, accused Russia of being the source of the attack.[di]
UK	2019	Election	Russia	Online information operation	According to *Reuters*, classified documents titled 'UK-US Trade & Investment Working Group Full Readout' were distributed online before the 2019 British general election as part of a Russian-backed strategic disclosure campaign.[dj] The Labour Party said the classified documents showed the Conservative Party privatising the state-run National Health Service in trade talks with the US. A network of 61 Russian social media accounts used open-access websites, including BuzzFeed, Medium, Reddit and Quora, to publish the leaked documents alongside fake news and conspiracy theories. Experts have observed that this campaign's pattern resembled that of the Russian Secondary Infektion operation.[dk] With the National Health Service being a key point of debate in the British elections, Graphika reported that the campaign was designed to create divisions between Western countries through credible online intermediaries.[dl] This campaign prompted calls for the government to release a report into Russian interference in British politics publicly.

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Poland	2020	Election	Russia	Online information operation	According to the Stanford Internet Observatory, the Polish military faced a Russian-based disinformation operation in the lead-up to the 2020 Polish presidential election.[dm] The Polish Special Services reported that the online attacks 'correspond to Russian actions' connected to the Niezależny Dziennik Polityczny website, which allegedly has ties with Russian state intelligence.[dn] The disinformation operation involved hackers publishing a forged open letter on Poland's War Studies Academy website stating that the Defender–Europe 20 military exercise, which involves the deployment of US and NATO forces near the Russian border, poses a significant threat to Poland.[do] The forged letter was republished in fabricated news articles and disseminated via fake Facebook accounts.[dp] The articles received more than 8,500 comments, likes and shares before authorities took them down.[dq] It appears that the objective of this disinformation operation was to enhance pro-Russian political movements in Poland, such as the far-right Confederation Party, polarise Polish society and undermine NATO.[dr]

a Leonid Bershidsky, 'How hackers exposed Ukraine's vulnerability', *Bloomberg*, 26 May 2014, online.
b Andy Greenberg, 'Everything we know about Russia's election-hacking playbook', *Wired*, 6 September 2017, online.
c Bershidsky, 'How hackers exposed Ukraine's vulnerability'.
d Greenberg, 'Everything we know about Russia's election-hacking playbook'.
e Sandra Dick, 'Fake pro-independence Facebook page that originated in Iran is taken down', *The Herald*, 23 August 2018, online.
f Dick, 'Fake pro-independence Facebook page that originated in Iran is taken down'.
g Dick, 'Fake pro-independence Facebook page that originated in Iran is taken down'.
h Dick, 'Fake pro-independence Facebook page that originated in Iran is taken down'
i Severin Carrell, 'Russian cyber-activists "tried to discredit Scottish independence vote"', *The Guardian*, 13 December 2017, online.
j @DFRLab, '#ElectionWatch: Scottish vote, pro-Kremlin trolls', *Medium*, 13 December 2017, online.
k Carrell, 'Russian cyber-activists "tried to discredit Scottish independence vote"'.
l Carrell, 'Russian cyber-activists "tried to discredit Scottish independence vote"'.
m Gordon Corera, 'Bulgaria warns of Russian attempts to divide Europe', *BBC News*, 4 November 2016, online.
n Corera, 'Bulgaria warns of Russian attempts to divide Europe'.
o 'Huge hack attack on Bulgaria election authorities "not to affect vote count"', *NoInvite.com*, 27 October 2015, online.
p 'Secondary Infektion at a glance', Graphika, no date, online.
q Ben Nimmo, Camille Francois, C Shawn Elb, Lea Ronzaud, Rodrigo Ferreira, Chris Hernon, Tim Kostelancik, *Secondary Infection*, Graphika, 2020, 24, online.
r Nimmo et al., *Secondary Infection*, 24.
s Jason Horowitz, 'Spread of fake news provokes anxiety in Italy', *New York Times*, 2 December 2016, online.
t Alberto Nardelli, Craig Silverman, 'Italy's most popular political party is leading Europe in fake news and Kremlin propaganda', *BuzzFeed News*, 30 November 2016, online.
u Nardelli & Silverman, 'Italy's most popular political party is leading Europe in fake news and Kremlin propaganda'.
v Nardelli & Silverman, 'Italy's most popular political party is leading Europe in fake news and Kremlin propaganda'.
w Ken Dilanian, Josh Meyer, Cynthia McFadden, William M Arkin, Robert Windrem, 'Exclusive: White House readies to fight election day cyber mayhem', *NBC News*, 4 November 2016, online.
x Dusica Tomovic, Maja Zivanovic, 'Russia's Fancy Bear hacks its way into Montenegro', *Balkan Insight*, 5 March 2018, online; PR Service, 'Web portal of Government of Montenegro and several other web sites were under enhanced cyberattacks', news release, Government of Montenegro, 17 February 2017, online.
y Jonathan Keane, 'Hackers tried to disrupt the parliamentary elections in Montenegro', *Business Insider*, 18 October 2016, online.
z Feike Hacquebord, *Two years of Pawn Storm: examining an increasingly relevant threat*, TrendMicro, 2017, online.
aa Tomovic & Zivanovic, 'Russia's Fancy Bear hacks its way into Montenegro'.
ab Andrew Higgins, 'Fake news, fake Ukrainians: how a group of Russians tilted a Dutch vote', *New York Times*, 16 February 2017, online.
ac Erik Brattberg, Tim Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*, Carnegie Endowment for International Peace, 23 May 2018, online.
ad Diego A Martin, Jacob N Shapiro, *Trends in online foreign influence efforts*, Princeton University, 8 July 2019, online.
ae Matthew Field, Mike Wright, 'Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals', *The Telegraph*, 17 October 2018, online.
af Matthew Field, Mike Wright, 'Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals'.
ag Scott Simon, 'Senate finds Russian bots, bucks helped push Brexit vote through', *NPR*, 19 January 2019, online.
ah '13,500-strong Twitter bot army disappeared shortly after EU referendum, research reveals', news release, *City*, University of London, 20 October 2017, online.

ai '13,500-strong Twitter bot army disappeared shortly after EU referendum, research reveals', news release, *City*, University of London.
aj Dan Sabbagh, Luke Harding, Andrew Roth, 'Russia report reveals UK government failed to investigate Kremlin interference', *The Guardian*, 21 July 2020, online.
ak @DFRLab, 'Fakes, bots, and blockings in Armenia', *Medium*, 2 April 2017, online; Freedom House, Armenia, Freedom on the Net 2017, online.
al @DFRLab, 'Fakes, bots, and blockings in Armenia'; Amy Mackinnon, 'Manipulating Elections Via Twitter in Armenia', *.coda*, 6 April 2017, online.
am Robert Tait, 'Czech Republic to fight "fake news" with specialist unit', *The Guardian*, 28 December 2016, online.
an Tait, 'Czech Republic to fight "fake news" with specialist unit'.
ao Robert Tait, 'Czech cyber-attack: Russia suspected of hacking diplomats' emails', *The Guardian*, 1 February 2017, online.
ap Tait, 'Czech cyber-attack: Russia suspected of hacking diplomats' emails'.
aq Tait, 'Czech cyber-attack: Russia suspected of hacking diplomats' emails'.
ar Aurelien Breeden, Sewell Chan, Nicole Perlroth, 'Macron campaign says it was target of "massive" hacking attack', *New York Times*, 5 May 2017, online.
as Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.
at Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.
au Eric Auchard, Bate Felix, 'French candidate Macron claims massive hack as emails leaked', *Reuters*, 6 May 2017, online.
av Andy Greenberg, 'Hackers hit Macron with huge email leak ahead of French election', *Wired*, 5 May 2017, online.
aw Reuters, 'French election contender Macron is Russian 'fake news' target: party chief', *Reuters*, 13 February 2017, online.
ax Feike Hacquebord, *Two years of Pawn Storm: examining an increasingly relevant threat*, Trend Micro, 2017, online.
ay Reuters, 'French polling watchdog warns over Russian news agency's election report', *The Guardian*, 3 April 2017, online.
az 'French presidential candidate Macron target of Russian "fake news," his party chief claims', *Deutsche Welle*, 13 February 2017, online.
ba Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.
bb Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.
bc Cynthia Kroet, 'Russian fake news campaign targets Merkel in German election', *Politico*, 24 January 2017, online.
bd @DFRLab, 'Russian internet: fake news haven?', *Medium*, 28 January 2017, online.
be @DFRLab, 'Russian internet: fake news haven?'.
bf Nimmo et al., *Secondary Infection*, 53
bg Nimmo et al., *Secondary Infection*, 53
bh Andrea Shalal, 'Germany confirms cyber attacks on political party think tanks', *Reuters*, 28 April 2017, online.
bi Shalal, 'Germany confirms cyber attacks on political party think tanks'.
bj Shalal, 'Germany confirms cyber attacks on political party think tanks'.
bk Shalal, 'Germany confirms cyber attacks on political party think tanks'.
bl Jamie Doward, 'Malta accuses Russia of cyber-attacks in run-up to election', *The Guardian*, 28 May 2017, online.
bm Doward, 'Malta accuses Russia of cyber-attacks in run-up to election'.
bn Doward, 'Malta accuses Russia of cyber-attacks in run-up to election'.
bo General Intelligence and Security Service, 'Spionage en ongewenste inmenging' [Espionage and unwanted interference], Netherlands Government, 2018, online.
bp 'Russian trolls active in Belgium and The Netherlands', *vrtNWS*, 16 July 2018, online.
bq Huib Modderkolk, 'Russen faalden bij hackpogingen ambtenaren op Nederlandse ministeries', *de Volkskrant*, 4 February 2017, online.
br Huib Modderkolk, 'Russen faalden bij hackpogingen ambtenaren op Nederlandse ministeries'.
bs David Alandete, 'Russian meddling machine sets sights on Catalonia', *El Pais*, 28 September 2017, online.
bt Alandete, 'Russian meddling machine sets sights on Catalonia.
bu Albin Sybera, 'Truth missing in action in Czech information wars', *Balkan Insight*, 9 September 2019, online.
bv Sybera, 'Truth missing in action in Czech information wars'.
bw Jakub Kalensky, 'Testimony: "Russian Disinformation Attacks on Elections: Lessons from Europe"', Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment, 16 July 2019, online.
bx 'Russian "troll factory" tweets tried to influence Italian voters', *The Local*, 2 August 2018, online.
by Alto Analytics, *The construction of anti-immigration electoral messages in Italy*, 27 February 2018, online.
bz Alto Analytics, *The construction of anti-immigration electoral messages in Italy.*
ca Secondary Infektion at a glance'.
cb Secondary Infektion at a glance'.
cc Secondary Infektion at a glance'.
cd Nimmo et al., *Secondary Infection*, 35.
ce Marc Santora, Julian E Barnes, 'In the Balkans, Russia and the West fight a disinformation-age battle', *New York Times*, 16 September 2018, online.
cf @DFRLab, '#ElectionWatch: *Sputnik* misleading in Macedonia', *Medium*, 23 September 2018, online.
cg 'US says Russia meddling in Macedonia ahead of name referendum', *Deutsche Welle*, 17 September 2018, online.
ch Jessica Purkiss, 'Russian Warriors and British PR Firms: Macedonia's Information War', *The Bureau of Investigative Journalism*, 29 September 2018, online.
ci Jessica Purkiss, 'Russian Warriors and British PR Firms: Macedonia's Information War'.
cj Chloe Colliver, Peter Pomerantsev, Anne Applebaum, Jonathan Birdwell, *Smearing Sweden: international influence campaigns in the 2018 Swedish election*, ISD, October 2018, 6, online.
ck Nimmo et al., *Secondary Infection.*
cl Patrik Oksanen, 'Lessons from the 2018 Swedish elections', *Disinfo Portal*, 11 June 2019, online.
cm Colliver et al., *Smearing Sweden: international influence campaigns in the 2018 Swedish election.*
cn Colliver et al., *Smearing Sweden: international influence campaigns in the 2018 Swedish election.*
co Colliver et al., *Smearing Sweden: international influence campaigns in the 2018 Swedish election.*
cp Colliver et al., *Smearing Sweden: international influence campaigns in the 2018 Swedish election.*
cq 'Hackers target democratic institutions in Europe, says Microsoft', *Deutsche Welle*, 20 February 2019, online.

cr 'Hackers target democratic institutions in Europe, says Microsoft'.
cs Saheli Roy Choudhuyry, 'Microsoft says hackers tried to breach European think tanks and non-profit organizations', *CNBC*, 20 February 2019, online.
ct 'Russia trying to meddle in EU elections—report', *Deutsche Welle*, 14 April 2019, online.
cu 'Russia trying to meddle in EU elections—report'.
cv 'Russia trying to meddle in EU elections—report'.
cw Kati Pohjanpalo, 'Finland detects cyber attack on online election-results service', *Bloomberg*, 10 April 2019, online.
cx Naveen Goud, 'Finland election results service hit by cyber attack', *Cybersecurity Insiders*, no date, online.
cy Katarina Klingova, 'A ray of hope in the haze: disinformation and the Slovak presidential election', *Power3.0*, 14 May 2019, online.
cz Klingova, 'A ray of hope in the haze: disinformation and the Slovak presidential election'.
da Michael Schwirtz, Sheera Frenkel, 'In Ukraine, Russia tests a new Facebook tactic in election tampering', *New York Times*, 29 March 2019, online; Nathaniel Glicher, 'Removing Coordinated Inauthentic Behavior in Thailand, Russia, Ukraine and Honduras', 25 July 2019, online.
db @DFRLab, '#ElectionWatch: Insta-deception targets Ukraine', *Medium*, 19 February 2019, online.
dc 'Ukraine elections marred by disinformation wars', *.coda*, 21 April 2019, online.
dd 'Ukraine elections marred by disinformation wars', *.coda*, 21 April 2019, online.
de Artur Korniienko, 'Hackers take down website of presidential candidate Zelenskiy's team', *Kyiv Post*, 2 January 2019, online.
df David Gilbert, 'Inside the massive cyber war between Russia and Ukraine', *Vice*, 30 March 2019, online.
dg Pavel Polityuk, 'Exclusive: Ukraine says it sees surge in cyber attacks targeting election', *Reuters*, 26 January 2019, online.
dh Interfax-Ukraine, 'Poroshenko reports on DDOS-attacks on Ukrainian CEC from Russia on Feb. 24-25', *Kyiv Post*, 26 February 2019, online.
di Sean Lyngaas, 'Ukraine's president accuses Russia of launching cyberattack against election commission', *Cyberscoop*, 26 February 2019, online.
dj Jack Stubbs, 'Leak of papers before UK election raises "spectre of foreign influence"—experts', *Reuters*, 3 December 2019, online.
dk Stubbs, 'Leak of papers before UK election raises "spectre of foreign influence"—experts'; Ben Nimmo, 'UK trade leaks (updated 12.8.19', Graphika, 2019, online.
dl Stubbs, 'Leak of papers before UK election raises "spectre of foreign influence"—experts'; Nimmo, 'UK trade leaks (updated 12.8.19'.
dm Internet Observatory, *Poland presidential election 2020: disinformation strikes the military*, Stanford University, 8 May 2020, online.

North America

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
US	2016	Election	Russia	Cyber operation	According to the *New York Times*, on 19 March 2016, Russian-backed hackers sent a phishing email to John Podesta, Hillary Clinton's campaign chairman, that contained a link redirecting him to a login site and prompting him to enter his credentials.[a] When Podesta did so, the hackers gained complete access to his email account, from which they stole 50,000 emails.[b] The Mueller report confirmed that the actors involved were part of the Russian-backed hacker group known as Fancy Bear.[c] Similar attacks were launched against members of the Democratic National Committee (DNC). After gaining access to the DNC network, the group stole a significant amount of data, including nearly 20,000 emails and 8,000 attachments relating to internal political deliberations sent by and to the DNC.[d] In addition to targeting the Clinton campaign and the DNC, Russian-backed hackers targeted 21 US states' electoral systems to find vulnerabilities that would provide access to the voter registration databases.[e] The hackers mostly engaged in preliminary activities such as 'scanning and probing'. However, some attempts were made to gain access to the electoral systems, and 'an exceptionally small number of them were actually successfully penetrated.'[f] The *New York Times* reported that Russian-backed hackers had sent phishing emails containing 'a malicious Trojan virus' to 120 election email accounts in the county.[g] In 2019, Florida Senator Marco Rubio confirmed that at least one election office in his county had been compromised and that the hackers were 'in a position' to alter the voter roll data.[h] The Russian Main Intelligence Directorate (GRU) also conducted cyber-espionage operations over several months against an American supplier of election-related software and sent spear-phishing emails to 122 election officials before the 2016 presidential election.[i] The hackers first sent the software vendor a spear-phishing email containing a link to a fake Google website that required login credentials. Once the hackers gained access to the software vendor's internal systems, they then sent additional spear-phishing emails purporting to be from the vendor to local government organisations. The second round of emails contained Microsoft Word documents infected with malware that gave the hackers unlimited access to computer devices. Spear-phishing emails were also sent to the American Samoa Election Office, purporting to be from a 'legitimate absentee ballot-related service provider'.[j] The software vendor publicly identified as VR Systems, which provided electronic voting services and equipment in eight states across the US.[k] Phishing attacks were also launched against American think tanks and NGOs in the hours after President Donald Trump's electoral win.[l] The emails, which contained malware, claimed that American elections are flawed and that Trump's win was rigged. The Russian state-sponsored group The Dukes, also known as Cozy Bear or APT29, was allegedly behind the attack.[m]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
US	2016	Election	Russia	Online information operation	According to cybersecurity firm Trend Micro, the Russian hacking group Pawn Storm released several months' worth of data stolen from the US Democratic National Committee (DNC).[n] The data was collected by a Gmail credential phishing campaign, which targeted several political staff from both the Clinton and Obama campaigns, and was released as two different sets of documents. The first set was released by Guccifer 2.0, a hacker persona created by Russian military intelligence officers, and DCLeaks.com. The second set was released three days before the Democrats' national convention, when WikiLeaks published 19,252 documents that it had received from Russian-backed hackers through an intermediary. There were also attempts by Pawn Storm to offer mainstream media outlets 'exclusive access' to the stolen data in an attempt to publicise the attacks and influence public opinion on American politics. The US Director of National Intelligence and the Department of Homeland Security jointly identified Russia as being responsible for the cyber operation and subsequent online information operation.[o] In addition to the strategic disclosure of the stolen DNC data, Twitter accounts linked to Russia's Internet Research Agency (IRA) were involved in a widespread disinformation campaign to influence public opinion in the lead-up to the 2016 US presidential election.[p] Two reports released by the Senate Intelligence Committee, commissioned by researchers from Oxford University's Computational Propaganda Project and cybersecurity firm New Knowledge, examined the IRA's Russian disinformation campaign.[q] New Knowledge's report found that, as part of the disinformation campaign, the IRA had created fake and deceptive social media accounts to engage with and manipulate the public discourse on almost every social media platform.[r] The social media accounts were designed to look like they belonged to everyday Americans.[s] Russian operatives used the accounts to amass followers based on an innocuous theme before shifting to another more divisive theme. According to the two reports, Russian operatives linked to the IRA specifically targeted African-Americans in the lead-up to the election to suppress voter turnout.[t]
US	2018	Election	Russia	Online information operation	According to the *New York Times*, the Russia-based Internet Research Agency (IRA) attempted to influence American voters in the lead-up to the 2018 midterm congressional elections by using Facebook and Instagram to disseminate disinformation.[u] Facebook's head of cybersecurity policy, Nathaniel Gleicher, confirmed that 115 accounts were removed from Facebook and Instagram for 'inauthentic coordinated behaviour' directly linked to the IRA.[v] According to the Atlantic Council's Digital Forensic Research Lab (DFRLab), Russian state-backed media outlet *RT*'s coverage of the 2018 midterms was partisan, favouring content related to the Republican Party and its candidates.[w] *RT* also featured links to Republican campaign advertisements.

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
US	2018	Election	Russia	Cyber operation	According to the *Daily Beast*, US Senator Claire McCaskill's office was targeted by a phishing campaign.[x] Staffers received 'forged notification emails' claiming that their Microsoft Exchange passwords had expired and prompting them to change the passwords using a link provided in the email. The link redirected the target to a 'convincing replica of the US Senate's Active Directory Federation Services (ADFS) login page', which displayed a 'single sign-on point for email and other services', The *Daily Beast* noted that the tactic used 'was a variant of the password-stealing technique used by Russia's so-called "Fancy Bear" hackers against [Hillary] Clinton's campaign chairman, John Podesta in 2016'. Following the report, Senator McCaskill confirmed that Russian-backed hackers had attempted to gain access to her office's server, but noted that they were 'not successful'.[y] This was the first reported case of Russian interference in the 2018 midterm congressional elections and involved 'a critical vote that could shape the remainder of President Donald Trump's presidency'.[z] The week before the *Daily Beast* published its report, Tom Burt, the corporate vice president for customer security and trust at Microsoft, noted that Russian-backed hackers had registered a phishing page as a Microsoft account to target several midterm candidates.[aa] The Democratic Congressional Campaign Committee was also targeted by a hacker group in an attack that resembled the Russian-backed hacking of the Democratic National Committee.[ab] *Techcrunch* reported that the hackers were able to obtain the credentials of a systems administrator with 'unrestricted access' to the congressional campaign committee's server. The Mueller report confirmed that the actors involved were part of the hacker group Fancy Bear, which is linked the Russian military intelligence agency.[ac]
US	2020	Election	Russia	Online information operation	According to *CNN News*, Russian-sponsored trolls operating from Ghana and Nigeria were targeting the US ahead of the 2020 presidential election with a disinformation campaign linked to online black empowerment movements.[ad] The trolls often directed anger towards white Americans by sharing graphic images and language on police brutality and racial profiling.[ae] Darren Linvill, a professor at Clemson University, explained that the trolls 'talked almost exclusively about what was happening on the streets of the US and not on the streets of Africa'. Around 263,200 Instagram users, 13,200 Facebook users and 68,000 Twitter users were reportedly following the troll accounts. Facebook and Twitter suspended some of the accounts linked to Ghana and Nigeria.[af] The accounts have since been attributed to the Russian-funded Eliminating Barriers for the Liberation of Africa group and the Russian Internet Research Agency, which previously interfered in the 2016 and 2018 election campaigns.

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
US	2020	Election	Iran	Online information operation	According to *Reuters*, Facebook removed a network of fake accounts and personas linked to the Islamic Republic of Iran Broadcasting Corporation for coordinated inauthentic behaviour involving discussions of the US presidential election in 2020.[ag] Some key tactics of the network included sharing videos aligned with Iranian interests, amplifying authentic content from liberal users, using unrelated political hashtags to reach a broader audience and directly contacting prominent politicians and public figures for interviews to solicit desired political narratives.[ah] The pro-Iranian videos shared by the accounts subsequently appeared on the Iranian-backed media outlet *Tehran Times*, which is owned by the Islamic Propagation Organisation under the Supreme Leader Ali Khamenei. Ben Nimmo, an analyst with the Digital Forensic Research Lab, pointed out that this network was a small but significant operation, as the accounts 'picked their targets individually and engaged them personally'.[ai]
US	2020	Election	North Korea	Cyber operation	According to the *New York Times*, state-backed hackers from North Korea began targeting organisations linked to the presidential candidates with phishing emails in the lead-up to the 2020 US presidential election.[aj]
US	2020	Election	Russia	Cyber operation	According to the *New York Times*, state-backed hackers from Russia began targeting organisations linked to the presidential candidates with phishing emails in the lead-up to the 2020 US presidential election.[ak] Microsoft confirmed that it had detected cyberattacks from a hacker group based in Russia that had targeted 'more than 200 organizations including political campaigns, advocacy groups, parties and political consultants'.[al]
US	2020	Election	China	Cyber operation	According to the *New York Times*, Google confirmed that state-backed hackers from China conducted spear-phishing attacks to gain access to personal email accounts of campaign staff members working for former Vice President and Democrat candidate Joe Biden ahead of the 2020 American presidential election.[am] While unsuccessful, the attacks were very similar to the Russian breach of John Podesta's personal emails.[an] Microsoft also confirmed that it had detected cyberattacks against 'high-profile individuals associated with the election' and 'prominent leaders in the international affairs community' from a hacker group operating from China.[ao]

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
US	2020	Election	Iran	Cyber operation	According to the *Washington Post*, an Iranian-backed hacker group called Phosphorus or APT35 targeted President Donald Trump's election campaign in the lead-up to the 2020 presidential election.[ap] Between August and September 2019, the Microsoft Threat Intelligence Center discovered that the group made more than 2,700 attempts to identify email accounts before targeting 241 specific accounts belonging to government officials, journalists, prominent Iranian citizens and other staff associated with the election campaign.[aq] Four accounts were compromised as a result. The group achieved that by gathering information from its targets through account recovery features and phone number authentication.[ar] Similarly, Google confirmed that Iranian hackers had targeted personal email accounts belonging to the Trump campaign staff.[as]

a Scott Shane, Mark Mazzetti, 'The plot to subvert an election: unraveling the Russia story so far', *New York Times*, 20 September 2018, online.
b Raphael Satter, 'Inside story: How Russians hacked the Democrats' emails', *Associated Press*, 5 November 2017, online.
c 'The Mueller report, annotated', *Washington Post*, 2 December 2019, online.
d Tom Hamburger, Karen Tumulty, 'WikiLeaks releases thousands of documents about Clinton and internal deliberations', *Washington Post*, 23 July 20126, online; Center for Strategic & International Studies (CSIS), *Significant cyber incidents since 2006*, CSIS, Washington DC, no date, online.
e The Associated Press, 'U.S. Tells 21 States That Hackers Targeted Their Voting Systems', *New York Times*, 22 September 2017, online.
f Cynthia McFadden, William M. Arkin & Kevin Monahan, 'Russians penetrated U.S. voter systems, top U.S. official says', *NBC News*, 8 February 2018, online.
g Frances Robles, 'Russian Hackers Were 'In a Position' to Alter Florida Voter Rolls, Rubio Confirms', *New York Times*, 26 April 2019, online.
h Frances Robles, 'Russian Hackers Were 'In a Position' to Alter Florida Voter Rolls, Rubio Confirms'.
i Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim, 'Top-secret NSA report details Russian hacking effort days before 2016 election', *The Intercept*, 6 June 2017, online.
j Cole et al., 'Top-secret NSA report details Russian hacking effort days before 2016 election'.
k Sam Biddle, 'Here's the email Russian hackers used to try to break into state voting systems', *The Intercept*, 2 June 2018, online.
l Steven Adair, 'PowerDuke: Widespread post-election spear phishing campaigns targeting think tanks and NGOs', *Volexity*, 9 November 2016, online.
m Steven Adair, 'PowerDuke: Widespread post-election spear phishing campaigns targeting think tanks and NGOs''.
n Feike Hacquebord, *Two years of Pawn Storm: examining an increasingly relevant threat*, Trend Micro, 2017, online.
o Department of Homeland Security, 'Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on election security', US Government, 7 October 2016, online; CSIS, *Significant cyber incidents since 2006*.
p @DFRLabs, '#TrollTracker: Twitter troll farm archives', *Medium*, 17 October 2018, online.
q Philip N Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, Camille Francois, *The IRA, social media and political polarization in the United States, 2012–2018*, Computational Propaganda Research Project, University of Oxford, 2018, online.
r Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, *The tactics & tropes of the Internet Research Agency*, New Knowledge, no date, online.
s DiResta et al., *The tactics & tropes of the Internet Research Agency.*
t DiResta et al., *The tactics & tropes of the Internet Research Agency*; Howard et al., *The IRA, social media and political polarization in the United States, 2012–2018.*
u Sheera Frenkel, Mike Isaac, 'Russian trolls were at it again before midterms, Facebook says', *New York Times*, 7 November 2018, online; Facebook, 'Removing Bad Actors on Facebook', *Facebook Newsroom*, 31 July 2018, online.
v Nathaniel Gleicher, 'Election update', *Facebook Newsroom*, 5 November 2018, online.
w @DFRLab, '#ElectionWatch: *RT*'s one-sided coverage of midterms', *Medium*, 25 August 2018, online.
x Kevin Poulsen, Andrew Desiderio, 'Russian hackers' new target: a vulnerable Democratic senator', *Daily Beast*, 26 October 2018, online.
y Quint Forgey, Tim Starks, '"I will not be intimidated": McCaskill responds to report of Russian targeting', *Politico*, 26 July 2018, online.
z Quint Forgey, Tim Starks, '"I will not be intimidated": McCaskill responds to report of Russian targeting'.
aa The Aspen Institute, 'Defending Democratic Institutions: Election 2018 and Beyond', *YouTube*, 19 July 2018, online.
ab Zack Whittaker, 'Mueller report sheds new light on how the Russians hacked the DNC and the Clinton campaign', *TechCrunch*, 19 April 2019, online.
ac 'The Mueller report, annotated'.
ad Clarissa Ward, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, Tim Lister, 'Russian election meddling is back—via Ghana and Nigeria—and in your feeds', *CNN*, 11 April 2020, online; Facebook, Detailed Report: March 2020 Coordinated Inauthentic Behavior Report, March 2020, online.
ae Graphika, *IRA in Ghana: double deceit*, online.

af Nathaniel Gleicher, 'Removing coordinated inauthentic behavior From Russia', *Facebook*, 12 March 2020, online; @TwitterSafety, *Twitter*, 13 March 2020 online.
ag Jack Stbbs, Katie Paul, 'Facebook says it dismantles disinformation network tied to Iran's state media', *Reuters*, 6 May 2020, online; Facebook, *April 2020 coordinated inauthentic behavior report*, Facebook, April 2020, online.
ah Olga Robinson, Shayan Sardarizadeh, 'Facebook removes "foreign interference" operations from Iran and Russia', *BBC News*, 14 February 2020, online.
ai Robinson & Sardarizadeh, 'Facebook removes "foreign interference" operations from Iran and Russia'; Nathaniel Gleicher, 'Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar', Facebook Newsroom, 12 February 2020, online.
aj Nicole Perlroth, David E Sanger, 'Iranian hackers Target trump campaign as threats to 2020 mount', *New York Times*, 4 October 2019, online.
ak Perlroth & Sanger, 'Iranian hackers Target trump campaign as threats to 2020 mount'.
al Tom Burt, 'New cyberattacks targeting US elections', *Microsoft on the Issues*, 10 September 2020, online.
am David E Sanger, Nicole Perlroth, 'Chinese hackers target email accounts of Biden campaign staff, Google says', *New York Times*, 18 September 2020, online.
an Sanger & Perlroth, 'Chinese hackers target email accounts of Biden campaign staff, Google says'.
ao Burt, 'New cyberattacks targeting US elections'.
ap Jay Greene, Tony Romm, Ellen Nakashima, 'Iranians tried to hack US presidential campaign in effort that targeted hundreds, Microsoft says', *Washington Post*, 5 October 2019, online.
aq Tom Burt, 'Recent cyberattacks require us all to be vigilant', *Microsoft on the Issues*, 4 October 2019, online.
ar Burt, 'Recent cyberattacks require us all to be vigilant'.
as Christopher Bing, 'Chinese and Iranian hackers targeted Biden and Trump campaigns, Google says', *Reuters*, 5 June 2020, online.

South America

Targeted state	Year	Political process	Alleged foreign state actor	Attack vector	Information
Brazil	2014	Election	Russia	Online information operation	According to a study conducted by the Department of Public Policy Analysis of the Getulio Vargas Foundation, Russia allegedly interfered in the 2014 Brazilian presidential election by using bots and disinformation networks on social media.[a] A botnet containing 699 automated profiles was found to have generated more than 773,700 posts relating to Brazilian presidential candidates Aecio Neves, Marina Silva, and Dilma Rousseff within one month.[b] Most of the automated profiles contained Cyrillic characters and references to Russian landmarks, which was taken to be indicative of Russian origin.[c]
Brazil	2018	Election	Russia	Online information operation	According to the Atlantic Council's Digital Forensic Research Lab, two Russian-backed networks consisting of 232 different online profiles were engaged in a disinformation campaign to influence the 2018 Brazilian general election.[d] The first network involved Twitter users interacting with Russian-backed media outlets to publish 8,185 tweets relating to Brazilian politics, most of them involving the current president, Jair Bolsonaro, and former president Luiz Inácio Lula da Silva.[e] The second network retweeted content published by automated accounts from Argentina, Cuba, Ecuador and Venezuela that were aligned with Brazil's left-wing parties.[f] American cybersecurity firm FireEye also reported that a front group for Russia had made use of Twitter bots in an attempt to interfere in the election.[g] The bots were used to artificially increase the reach of Facebook and Twitter posts that questioned Brazil's democratic model and the election's legitimacy. For example, the bots increased the reach of the hashtag #OpEleiçãoContraOFascismo (Operation Against Fascism).[h]
Colombia	2018	Election	Russia	Cyber operation	According to *VOA News*, the Colombian Government and military officials investigated 'tens of thousands' of cyber operations launched against the country's voter registration system in the lead-up to the 2018 parliamentary elections.[i] The Colombian authorities traced the cyber operations to Venezuela, which was acting as 'a proxy for Russia'.[j] It appears that the objective of the cyber operations was to disrupt the voter registration system.[k]

a FGV DAPP, 'FGV DAPP Survey reveals evidence of Russian robots in 2014 presidential election campaigns', FGV DAPP, August 2017, online.
b FGV DAPP, 'FGV DAPP Survey reveals evidence of Russian robots in 2014 presidential election campaigns'.
c Andrew Allen, 'Bots in Brazil: the activity of social media bots in Brazilian elections', *Think Brazil*, Wilson Center, 17 August 2018, online.
d @DFRLab, '#ElectionWatch: Bots around Brazil's first presidential debate', *Medium*, 18 August 2018, online.
e @DFRLab, '#ElectionWatch: FGV DAPP uncovers foreign Twitter influence in Brazil', *Medium*, 2 November 2018, online.
f @DFRLab, '#ElectionWatch: FGV DAPP uncovers foreign Twitter influence in Brazil'.
g Bruno Benevides, 'Russian hackers are trying to interfere in Brazilian elections, cybersecurity firm says', *Folha de S. Paulo*, 5 October 2018, online.
h Benevides, 'Russian hackers are trying to interfere in Brazilian elections, cybersecurity firm says'.
i Martin Arostegui, 'Colombia probes voter registration cyberattacks traced to Russia's allies', *VOA News*, 15 March 2018, online.
j Arostegui, 'Colombia probes voter registration cyberattacks traced to Russia's allies'.
k Julia Gurganus, *Russia: Playing a geopolitical game in Latin America*, Carnegie Endowment for International Peace, 3 May 2018, online.

Notes

1 Fergus Hanson, Sarah O'Connor, Mali Walker, Luke Courtois, *Hacking democracies: cataloguing cyber-enabled attacks on elections*, ASPI, Canberra, 17 May 2019, online.

2 Katherine Mansted, 'Engaging the public to counter foreign interference', *The Strategist*, 9 December 2019, online.

3 Erik Brattberg, Tim Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*, Carnegie Endowment for International Peace, May 2018, online.

4 Laura Rosenberger, 'Making cyberspace safe for democracy: the new landscape of information competition', *Foreign Affairs*, May/June 2020, online.

5 For a comprehensive overview of foreign interference in elections, see David Shimer, *Rigged: America, Russia, and one hundred years of covert electoral interference*, Knopf Publishing Group, 2020; Casey Michel, 'Russia's long and mostly unsuccessful history of election interference', *Politico*, 26 October 2019, online.

6 David M Howard, 'Can democracy withstand the cyber age: 1984 in the 21st century', *Hastings Law Journal*, 2018, 69:1365.

7 Philip Ewing, 'In "Rigged," a comprehensive account of decades of election interference', *NPR*, 9 June 2020, online.

8 Eric Geller, 'Some states have embraced online voting. It's a huge risk', *Politico*, 8 June 2020, online. For a comprehensive discussion on electronic voting, see NRC, *Asking the right questions about electronic voting*.

9 CSE, *Cyber threats to Canada's democratic process*.

10 Samantha Bradshaw, Philip N Howard, *The global disinformation order: 2019 global inventory of organised social media manipulation*, Computational Propaganda Research Project, Oxford Internet Institute, 2019, online.

11 National Research Council (NRC), 'Public confidence in elections', *Asking the right questions about electronic voting*, Computer Science and Telecommunications Board, National Academies Press, Washington DC, 2006, online.

12 Communications Security Establishment (CSE), *Cyber threats to Canada's democratic process*, Canada, 7 June 2017, online.

13 Elizabeth Dwoskin, Craig Timberg, 'Facebook takes down Russian operation that recruited U.S. journalists, amid rising concerns about election misinformation', *Washington Post*, 1 September 2020, online.

14 See Alicia Wanless and Laura Walters, *How Journalists Become an Unwitting Cog in the Influence Machine*, Carnegie Endowment for International Peace, online, 1.

15 Hanson et al., *Hacking democracies: cataloguing cyber-enabled attacks on elections*.

16 See, for example, 'US secretly created "Cuban Twitter" to stir unrest and undermine government', *The Guardian*, 3 April 2014, online; Mustafa Al-Bassam, 'British spies used a URL shortener to honeypot Arab Spring dissidents', *Motherboard*, 26 July 2016, online; Samantha Bradshaw, Philip N Howard, *Troops, trolls and troublemakers: a global inventory of organized social media manipulation*, working paper no. 2017.12, Computational Propaganda Research Project, Oxford Internet Institute, 17 July 2017, online.

17 An analysis of both quantitative and qualitative data.

18 During the research period, the International Cyber Policy Centre was fortunate to host Admiral Mike Rogers (ret'd), the former second commander of US Cyber Command and director of the US National Security Agency; Laura Rosenberger, director of the Alliance for Securing Democracy and senior fellow at the German Marshall Fund; PW Singer, strategist and senior fellow at New America; and Dr Jean-Baptiste Jeangène Vilmer, the director of the Institute for Strategic Studies (L'Institut de recherche stratégique de l'École militaire).

19 For a comprehensive overview of social media manipulation, notably governments and political parties using such techniques domestically, see Bradshaw & Howard, *The global disinformation order: 2019 global inventory of organised social media manipulation*.

20 Note that two elections identified in the initial dataset published in Hansen et al., *Hacking democracies*, have been removed for this updated and expanded dataset, as it was determined that the link between the interference and the respective elections wasn't strong enough in the light of our recoded analysis.

21 See the Convention on Cybercrime of the Council of Europe (the Budapest Convention), 23 November 2001, online.

22 See the appendix for examples of online information operations; Herb Lin, 'Developing responses to cyber-enabled information warfare and influence operations', *Lawfare*, 6 September 2018, online; Casey Corcoran, Bo Julie Crowley, Raina Davis, *Disinformation threat watch: the disinformation landscape in East Asia and implications for US policy*, Belfer Center for Science and International Affairs, Cambridge, Massachusetts, May 2019, online; Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Information manipulation: a challenge for our democracies*, Institute for Strategic Research, Paris, August 2018, online.

23 Computer Security Resource Center, 'Attack surface', *Glossary*, National Institute of Standards and Technology, online.

24 Refer to the appendix for information on all the identified cases.

25 See the appendix for a table of states that have experienced cyber-enabled foreign interference.

26 Matt Apuzzo, Adam Satariano, 'Russia is targeting Europe's elections. So are far-right copycats', *New York Times*, 12 May 2019, online.

27 Dov H Levin, 'How to manage the threat of foreign election interference', *War on the Rocks*, 15 October 2020, online.

28 See Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.

29 These attack vectors were adopted from the Joint Threat Research Intelligence Group's *The art of deception: training for online covert operations*, which was disclosed as part of the Snowden archive and published by *The Intercept*. See Glenn Greenwald, 'How covert agents infiltrate the internet to manipulate, deceive, and destroy reputations', *The Intercept*, 25 February 2014, online.

30 Australian Cyber Security Centre, *Phishing—scam emails*, Australian Government, 23 June 2020, online.

31 Shane Huntley, 'How we're tackling evolving online threats', Google Threat Analysis Group, 16 October 2020, online.

32 Australian Cyber Security Centre, *Denial of service*, Australian Government, 22 May 2020, online.

33 Artur Korniienko, 'Hackers take down website of presidential candidate Zelenskiy's team', *Kyiv Post*, 2 January 2029, online; David Gilbert, 'Inside the massive cyber war between Russia and Ukraine', *Vice*, 30 March 2019, online.

34 This is a very narrow version of the Facebook definition. Jen Weedon, William Nuland, Alex Stamos, *Information operations and Facebook*, version 1.0, 27 April 2017, online.

35 See Dustin Volz, 'US far-right activists, WikiLeaks and bots help amplify Macron leaks: researchers', *Reuters*, 7 May 2017, online.

36 Sven Herpig, Julia Schuetze, Jonathan Jones, *Securing democracy in cyberspace: an approach to protecting data-driven elections*, Stiftung Neue Verantwortung, October 2018, online.

37 See Volz, 'US far-right activists, WikiLeaks and bots help amplify Macron leaks: researchers'.

38 Nina Jankowicz, 'How an anti-Trump flash mob found itself in the middle of Russian meddling', *Politico*, 7 May 2020, online; Donnie O'Sullivan, Drew Griffin, Scott Bronstein, 'The unwitting: the Trump supporters used by Russia', *CNN*, 20 February 2018, online.

39 Peter W Singer (@peterwsinger), 'This tweet illustrates an ongoing problem in how the public finds out (or not) about foreign threats to our election. A thread', *Twitter*, 5 August 2020, online.

40 Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.

41 Raphael Satter, 'Inside story: How Russians hacked the Democrat's emails', *Associated Press*, 5 November 2017, online; Andy Greenberg, 'Hackers Hit Macron With Huge Email Leak Ahead of French Election', *WIRED*, 5 May 2017, online.

42 Jack Stubbs, 'Leak of papers before UK election raises "spectre of foreign influence"—experts', *Reuters*, 3 December 2019, online.

43 Hanson et al., *Hacking democracies: cataloguing cyber-enabled attacks on elections*.

44 Singer, 'This tweet illustrates an ongoing problem in how the public finds out (or not) about foreign threats to our election. A thread'.

45 Apuzzo & Satariano, 'Russia is targeting Europe's elections. So are far-right copycats'.

46 The UK is included in this figure as it was still part of the EU when it was targeted.

47 Scott Shane, Mark Mazzetti, 'The plot to subvert an election: unraveling the Russia story so far', *New York Times*, 20 September 2018, online.

48 'Evidence of Russia-linked influence operations in Africa', *Internet Observatory*, Stanford University, 30 October 2019, online; Davey Alba, Sheera Frenkel, 'Russia tests new disinformation tactics in Africa to expand influence', *New York Times*, 30 October 2019, online.

49 Anna Arutunyan, 'There is no Russian plot against America', *Foreign Affairs*, 5 August 2020, online.

50 See the appendix for more information.

51 'Taiwan president-elect's Facebook page flooded by Chinese users despite ban', *ABC News*, 21 January 2016, online.

52 Australia, Cambodia, Hong Kong, Indonesia, Malaysia and Taiwan.

53 David E Sanger, Nicole Perlroth, 'Chinese hackers target email accounts of Biden campaign staff, Google says', *New York Times*, 18 September 2020, online; Huntley, 'How we're tackling evolving online threats'; Tom Burt, 'New cyberattacks targeting US elections', *Microsoft On The Issues*, 10 September 2020, online.

54 Fergus Hanson, Emilia Currey, Tracy Beattie, *The Chinese Communist Party's coercive diplomacy*, ASPI, Canberra, 1 September 2020, online.

55 William Evanina, 'Statement by NCSC Director William Evanina: Election threat update for the American public', news release no. 29-20, Office of the Director of National Intelligence, 7 August 2020, online.

56 Edward Wong, Matthew Rosenberg, Julian E Barnes, 'Chinese agents helped spread messages that sowed virus panic in US, officials say', *New York Times*, 22 April 2020, online.

57 Israel, the UK and the US.

58 Nicole Perlroth, David E Sanger, 'Iranian hackers Target trump campaign as threats to 2020 mount', *New York Times*, 4 October 2019, online.

59 Jay Greene, Tony Romm, Ellen Nakashima, 'Iranians tried to hack US presidential campaign in effort that targeted hundreds, Microsoft says', *Washington Post*, 5 October 2019, online.

60 Refer to the appendix for information on all the identified cases.

61 Yong Jae Mok, 'Security companies in South Korea discover North Korean cyberattack', *Radio Free Asia*, 10 April 2020, online.

62 Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, *World War C: understanding nation-state motives behind today's advanced cyber attacks*, FireEye Labs, 2013, online.

63 Bradshaw & Howard, *The global disinformation order: 2019 global inventory of organised social media manipulation*.

64 Alba & Frenkel, 'Russia tests new disinformation tactics in Africa to expand influence'.

65 Phil Sherwell, 'Artificial intelligence: China "uses Taiwan for target practice" as it perfects cyber-warfare techniques', *The Times*, 5 January 2020, online; Ben Nimmo, Camille Francois, C Shawn Eib, Lea Ronzaud, 'IRA AGAIN: unlucky thirteen', *Graphika*, September 2020, online.

66 Benjamin Edwards, Alexander Furnas, Stephanie Forrest, Robert Axelrod, 'Strategic aspects of cyberattack, attribution, and blame', *Proceedings of the National Academy of Sciences of the United States of America*, 14 March 2017, online.

67 David Alandete, 'Russian network used Venezuelan accounts to deepen Catalan crisis', *El Plaís*, 12 November 2017, online.

68 Clarissa Ward, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, Tim Lister, 'Russian election meddling is back—via Ghana and Nigeria—and in your feeds', *CNN*, 11 April 2020, online.

69 Darren Lim, Isabella Hansen, 'Doxing democracy: lessons from election interference in the US and France', *The Strategist*, 17 July 2018, online.

70 Heather A Conley, Rachel Ellehuus, Timothy Kostelancik, Jeffrey Mankoff, Cyrus Newlin, Amy Searight, Devin Stewart, *Countering Russian & Chinese influence activities*, Center for Strategic & International Studies, 15 July 2020, online.

71 Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.

72 27,474 respondents; European Commission, *Public opinion: democracy and elections*, November 2018, online.

73 Jacob Poushter, Janell Fetterolf, *International publics brace for cyberattacks on elections, infrastructure, national security: many doubt their countries are prepared for major cyber hacks'*, Pew Research Center, 9 January 2019, online.

74 International Institute for Democracy and Electoral Assistance, *ICTs in Elections Database*, online; Kassie Bracken, Alexandra Eaton, 'How will the US combat election day cyberwarfare? With paper', *New York Times*, 18 October 2020, online.

75 Laurens Cerulus, 'Dutch go old school against Russian hacking', *Politico*, 28 January 2018, online; 'Dutch to hand-count ballots in March vote over hacking fears', *Deutsche Welle*, 1 February 2017, online.

76 Eric Rosenbach, Katherine Mansted, *Can democracy survive in the Information Age?*, Belfer Center for Science and International Affairs, October 2018, online.

77 Ewing, 'In "Rigged," a comprehensive account of decades of election interference'; Kate Conger, Charlie Savage, 'How fake influence campaigns on Facebook lured real people', *New York Times*, 2 August 2018, online.

78 Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': interim report*, fifth report of session 2017–19, House of Commons, online.

79 Bradshaw & Howard, *The global disinformation order: 2019 global inventory of organised social media manipulation*.

80 Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, Intelligence Community, 6 January 2017, online.

81 Shaun Walker, 'Russia slates 'baseless, amateurish' US election hacking report', *The Guardian*, 20 January 2017, online.

82 Matthew Cole, Richard Esposito, Sam Biddle and Ryan Grim, 'Top-secret NSA report details Russian hacking effort days before 2016 election', *The Intercept_*, 6 June 2017, online.

83 Colin Packham, 'Exclusive: Australia concluded China was behind hack on parliament, political parties - sources', *Reuters*, 16 September 2019, online.

84 Australian Associated Press, 'China rejects Australian parliament cyber attack claims as 'baseless' and 'irresponsible'', *The Guardian*, 19 February 2019, online.

85 For example, the Cybersecurity and Infrastructure Security Agency under the US Department of Homeland Security offers checklists, planning guides and mitigation strategies that can be used to protect governments from cybersecurity threats during elections; 'Cyber incident detection and notification planning guide for election security', Cybersecurity and Infrastructure Security Agency, online. The Global Cyber Alliance has a standardised cybersecurity toolkit that supports election offices in improving resilience against cyber threats, online.

86 Garret M Graff, 'The right way to cover hacks and leaks before the election', *Wired*, 7 October 2020, online; Alina Clough, Alexander de Avila, 'In guarding democracy, hindsight really will be 2020: the tabletop exercise as a model for securing American elections', *Kennedy School Review*, 15 October 2020, online.

87 Brattberg & Maurer, *Russian election interference: Europe's counter to fake news and cyber attacks*.

88 Janine Zacharia, Andrew Grotto, 'How to report responsibly on hacks and disinformation', Freeman Spogli Institute, Stanford University, online.

89 Graff, 'The right way to cover hacks and leaks before the election'.

90 Zacharia & Grotto, 'How to report responsibly on hacks and disinformation'.

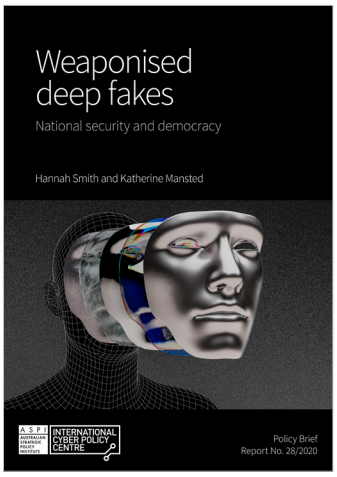
91 Hannah Smith, Katherine Mansted, *Weaponised deep fakes*, ASPI, Canberra, 29 April 2020, online.

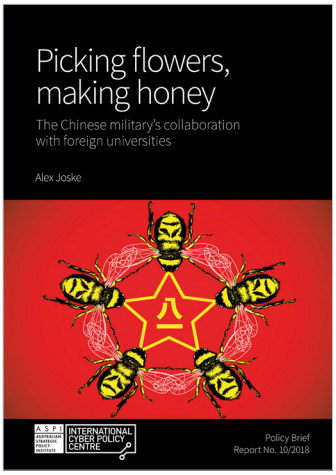
92 Ed Stein, 'The Deter Act: Congress's latest effort to discourage election interference', *Lawfare*, 1 August 2018, online.

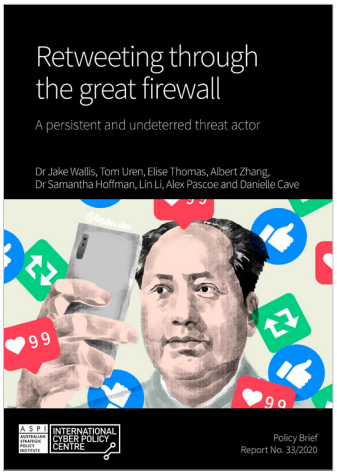
Acronyms and abbreviations

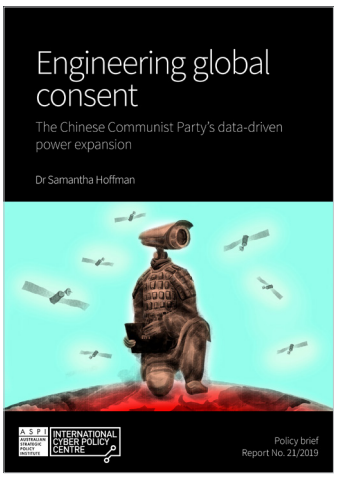
DoS	denial of service
EU	European Union
NATO	North Atlantic Treaty Organization
NGO	non-government organisation
UK	United Kingdom

Some previous ICPC publications









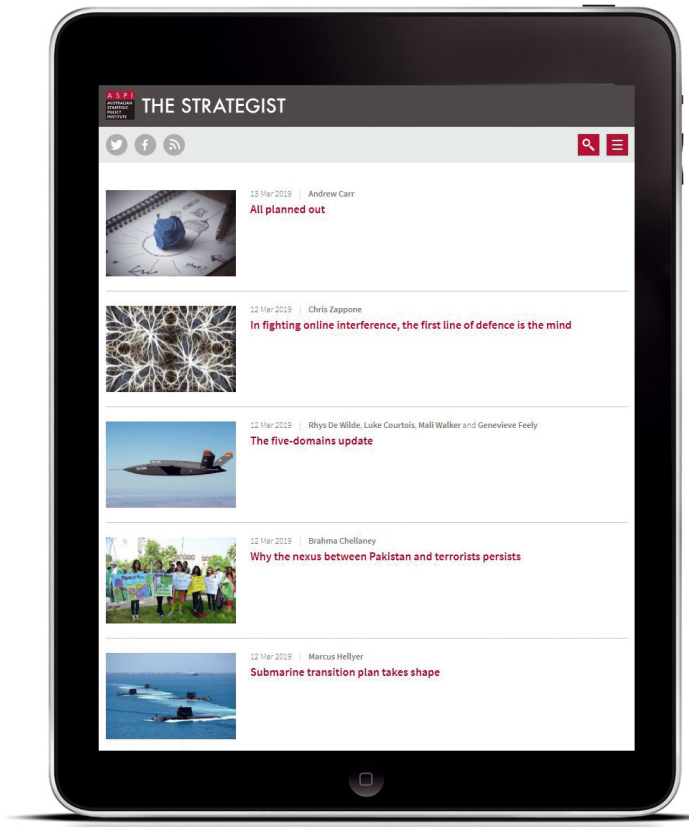
WHAT'S YOUR STRATEGY?

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

The Strategist, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au.

facebook.com/ASPI.org

@ASPI_org



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Supported by

LOCKHEED MARTIN THALES NAVAL GROUP

To find out more about ASPI go to www.aspi.org.au or contact us on 02 6270 5100 and enquiries@aspi.org.au.

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE