The RUSI Journal

ISSN: 0307-1847 (Print) 1744-0378 (Online) Journal homepage: https://www.tandfonline.com/loi/rusi20

Influence and Interference in Foreign Elections

Paul Baines & Nigel Jones

To cite this article: Paul Baines & Nigel Jones (2018) Influence and Interference in Foreign Elections, The RUSI Journal, 163:1, 12-19, DOI: 10.1080/03071847.2018.1446723

To link to this article: https://doi.org/10.1080/03071847.2018.1446723

Published online: 16 Mar 2018.

Submit your article to this journal

Article views: 609

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=rusi20

THE RUSI JOURNAL

Check for updates

INFLUENCE AND INTERFERENCE IN FOREIGN ELECTIONS

THE EVOLUTION OF ITS PRACTICE

PAUL BAINES AND NIGEL JONES

The use of influence or interference activities by one country to change the tide of elections in another has recently gained prominence due to alleged Russian influence in the 2016 US presidential election and the 2017 French presidential election. In this article, Paul Baines and Nigel Jones chart the evolution of influence and interference in foreign elections. With the rise of its modern digital form, they consider whether it is acceptable as a norm in international relations, or a violation.

This article considers how norms (and their violation) affect public trust of information, information systems and systems of government by analysing the ends, ways and means used in election interference (influence) interventions. How election influence might be countered is then considered. The article concludes by discussing whether election interference in the modern world might generate short-term gains, or whether it is likely to damage trust between states in the longer term, and therefore be harmful to both the target and the protagonist. Finally, the issue of whether election interference is an old phenomenon achieved by new ways and means or a new phenomenon achieved by old ways and means is considered.

New Context, New Norms?

Martha Finnemore and Kathryn Sikkink argue that norms as 'standards of appropriate behaviour' never emerge in a 'normative vacuum but instead emerge in a highly contested normative space where they must compete with other norms and perceptions of interest. Efforts to promote a new norm take place within standards of "appropriateness" defined by prior norms'.[1] In this context, Finnemore and Sikkink describe a 'norm life cycle', charting the emergence of a norm, its cascading effect through the conforming actions of other actors, and finally its internalisation or 'taken-for-granted' status.[2] Theirs is a social constructivist perspective, where norms and meaning are created in a social context through interaction with others. The use of cyberspace, cyber attack and social media to influence elections provides an example of the contested emergence of international norms, where they are yet to be established as taken-for-granted standards. Indeed, cyberspace is stress-testing norms of international behaviour, as politicians, diplomats and spies compete for influence.

For example, espionage is seen as an unpleasant but necessary norm, resourced and practised as an art in relation to national security – just make sure you do not get caught. This is widely understood as a norm because, as Finnemore and Sikkink suggest, when a norm is broken, 'it generates disapproval or stigma' and yet no country feels the need to explain the existence of espionage agencies.[3] State use of cyber-based industrial espionage for commercial advantage is one area where tentative steps towards new international norms are being taken. The US has shown success in dissuading China from pursuing commercially motivated cyber espionage after a period of messaging that included charging five Chinese military hackers with 'cyber espionage against U.S. corporations and a labor organization for commercial advantage'.[4] At the heart of this emerging norm is not that espionage should not be conducted, or conducted against commercial targets (as the Snowden papers indicate), but rather that the use of the resulting information should not be used for commercial advantage.[5]

State use of cyber attacks on military targets is emerging as an accepted norm in military practice, governed by the existing Law of Armed Conflict. In line with existing norms, this acceptance is not extended to cyber attacks on civilian critical infrastructure, such as financial institutions, and energy and utility networks. Nevertheless, US officials have expressed concern about

 DOI: 10.1080/03071847.2018.1446723

US Attorney General Jeff Sessions is sworn-in to testify before the US Senate Select Committee on Intelligence, June 2017. Sessions has firmly denied accusations that he colluded with Russians in the conduct of the 2016 presidential election. *Courtesy of PA Images*

how cyberspace may be used as a live laboratory for developing cyber weapons capable of paralysing a country's information and digital infrastructure and the services on which its people rely. The practice of covert and illicit activities, where the attacker's relationship with a state is often ambiguous to the public, by contrast, has no regard for accepted international norms.

These examples of emerging norms indicate the need for a highly contextual and nuanced assessment of the ends, ways and means adopted by protagonists. In this article, the terms 'ends', 'ways' and 'means' are used as a way of distinguishing intent from courses of action and the resources used in the contested norm of interference in elections.[6]

Historical Foreign Election Influence and Interference

Foreign influence in the domestic political contexts of other countries is not new, not least because election outcomes determine how a country's leaders allocate political and economic resources (the 'ends'). France, for example, sought to interfere in the 1796 US presidential election to overturn the Jay Treaty (the 'end'), a trade alliance with Britain (with whom France had just fought a war in 1793), which they saw as a violation of the 1778 alliance negotiated between the US and France. It did so by seeking to replace the pro-British Federalist George Washington with the pro-French Republican Thomas Jefferson ('the way'). To do this, the French ambassador, Pierre-Auguste Adet, led a campaign openly supporting the Republicans and attacking the Federalists ('the means'). Later, he made a letter written to Washington's secretary of state pleading with the US government to reject the Jay Treaty available to *Aurora*, a Philadelphia newspaper, and threatened to suspend relations with the US altogether. [7]

Elections represent part of the command-and-control system for the decision-making of a nation. Influencing an election can alter decision-making to align with a foreign power's interest, and states have been trying to influence each other in this way for centuries. What is new in the modern environment are the 'ways' and 'means'. For example, in the 1800s in the US, a practice known as 'cooping' was used to manipulate election results. Unwilling bystanders were taken from the street, kept in a 'coop' and forced to drink alcohol, and then they were coerced into marking the ballot several times in various disguises in favour of a particular candidate. One theory regarding the death of the famous writer Edgar Allen Poe is that he may have died in a cooping incident during a Baltimore election.[8]

Fast forward to the present and the shift has moved from physical force to coercive influence, including through disinformation and 'hybrid' campaigns, where deniable military assets are used to achieve a political objective. Despite running the risk of providing ammunition for state-owned propaganda channels, it is an inescapable fact that several foreign influence and disinformation campaigns in elections include some British and American examples, which are considered below. As an interesting exercise, the reader might conduct his or her own assessment of the legitimacy of the ends, ways and means in each of the examples.

The Zinoviev Letter, 1924

The Zinoviev Letter was a letter purportedly from Grigory Zinoviev, the head of Comintern in Moscow, to the

Communist Party of Great Britain to mobilise 'sympathetic forces' in the Labour Party to support an Anglo-Soviet treaty and loan to the Bolshevik government, and foment revolt in the British armed forces.[9] The letter was published in the *Daily Mail* a few days before the 1924 British general election. The resulting scandal had little positive impact on the Labour vote, and led to a surge in Conservative votes and to the collapse of the Labour government.[10] Although the letter was considered authentic at the time, it is now widely accepted to have been a forgery. According to MI5's official historian, Christopher Andrew, the letter was probably leaked to the Conservative-leaning *Daily Mail* by MI5 officers, after it was passed to them from the MI6 station in Reval (now Tallinn) from an anti-Communist White Russian source to sabotage the Anglo-Soviet trade treaty in development by Ramsay MacDonald's minority government.[11] The 'ends' and 'ways' are difficult to distinguish in this example. Was the 'end' the undermining of a weak government about to make a trade deal, in the interests of national security? The 'means' was allegedly intelligence officers leaking a false document to the press.

Italy, 1948

CIA covert action to undermine the 1948 Italian elections was detailed in an admission by the CIA to the US House Select Committee on Intelligence (the 'Pike Committee').[12] Funding for intervention in Italian elections between 1948 and the time of the committee hearings was $75 million, including $10 million in 1972 alone.[13] Forged letters said to have come from the Communist Party of Italy were used to discredit leaders (focusing on their personal and sex lives) to sway a close election when it looked like a united Marxist-left coalition would win – a prospect *Time* magazine labelled 'the brink of catastrophe'.[14] This prospect led to the development of the Office of Policy Coordination (which merged with the CIA in 1951), a covert psychological operations organisation, which began the propaganda action. It began with a ten-million-strong letter-writing campaign from the Italian diaspora in the US to their friends and family in Italy using mass-produced, pre-written templates and cables, urging the recipients to vote against the Communists.[15] Shortwave radio broadcasts were also used to discredit what would be a 'Communist dictatorship', allegedly ready to transport Italian workers to gulags if they were not sufficiently compliant. Here, the 'end' was to subvert the election of a Marxist government in Italy, the 'way' was a covert coordinated propaganda campaign and the 'means' was the use of the Italian diaspora to influence friends and family in Italy.[16]

Indonesia, 1963–66

With a view to influencing regional security in a post-colonial context, the UK allegedly interfered in Indonesia's elections in the mid-1960s. This was conducted through the Foreign Office's Information Research Department to overthrow the regime of President Sukarno because of his Konfrontasi policy and attempt to derail the British-backed Malaysian federation.[17] The 'means' for this interference exploited anti-Sukarno black propaganda operations, including persistent newspaper reports emphasising the Chinese nature of the communist threat. These were aimed specifically at the PKI,[18] the ethnic Chinese-based Indonesian communist party with which Sukarno had been flirting. The use of black propaganda helped to create the conditions which resulted in a coup by the pro-Western Indonesian army. Through a deluge of bad international press and his perceived association with Chinese communists, Sukarno was discredited to the point where he was forced to hand over power to General Suharto.

Chile, 1964–70

The US's Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (known as the 'Church Committee', reporting in 1975) uncovered how the CIA funded opposition parties, specifically the Christian Democrat Party under Eduardo Frei, in the 1964 Chilean election and propaganda campaigns to discredit the incumbent, Salvador Allende.[19] Later, in the 1970 election, the programme included seeking to discredit Allende and blocking him from office when he won the election. At the same time, the Soviet Union, through the KGB, was seeking to ensure the success of Allende, a Marxist-leaning political leader, funding him and his campaign, according to Vasili Mitrokhin, a KGB defector.[20] For the CIA, the 'end' was to remove Allende from office, the 'way' was to strengthen the opposition and the 'means' was to fund opposition activities.

Russian Interference in Montenegro, the US and France, 2016–17

One example of election interference, which Russia has denied, involved Serbian paramilitaries and two Russian organisers – which Montenegro's chief prosecutor alleges were Russian GRU (the military intelligence agency) officers – in an attempted coup scheduled for 16 October 2016 to assassinate Montenegro's prime minister, Milo Djukanovic. The intention was to install an anti-NATO candidate in parliament just as Montenegro was seeking to join the Alliance and the EU and move out of the sphere of influence of Serbia and Russia.[21] Russia opened a number of Serbian-language TV and radio stations to court Serbian public opinion in Montenegro in 2014.[22] Here, the 'end' was to stop Montenegrin accession to NATO, the 'way' was by removing the prime minister and the 'means' was assassination.

The 2016 US presidential election remains under investigation for alleged foreign influence by Russia. Allegations extend from collusion between individuals, campaign teams and the Russians to the generation of 'fake news' and expenditure of $100,000 on adverts from false sources on Facebook and Twitter.[23] They include the alleged hacking by Russia of Democratic Party systems. Regardless of the result of special counsel Robert Mueller's investigation, the media coverage through 2017 and 2018 demonstrates a debate about norms, trust and boundaries of acceptable behaviour in public life.

In May 2017, the US National Security Agency reported to the Senate's Armed Forces Committee that hackers leaking nine gigabytes of information from the campaign of France's presidential election candidate Emmanuel Macron on to the

web were likely to be Russian and affiliated with the GRU.[24] The leak was timed to cause maximum damage to the French election, by coinciding with the deadline on party campaigning, which would have ensured that En Marche! party executives were unable to respond to or rebut any attention the email dump generated. However, they did manage to make a statement about the hack an hour before the campaign communication blackout was imposed and before Marine Le Pen's campaign team could legally comment.[25] As far as the hackers were concerned, there were no revealing 'secrets' in the leaks, although some of the emails were said to be fake; for instance, one discussed Macron's 'Bahamian bank accounts' in a bid to tarnish his reputation and damage public trust in him, presumably to increase the chances of Le Pen's far-right Front National, a party with which Russian President Vladimir Putin would likely prefer to collaborate.[26]

Non-State Actors' Interference in Elections

It is worth also mentioning attempts by Islamic terrorist organisations to influence elections (the 'end' being Western withdrawal from Muslim territory), as they help to inform our assessment of the boundary issues by which acceptable norms might be judged. Al-Qa'ida, for example, has made crude efforts to influence elections (the 'way'). In a propaganda video in 2003, Osama bin Laden threatened 'prompt and severe actions' against Spain for participating in the war in Iraq (the 'means').[27] The Madrid train bombings occurred on 11 March 2004, three days before the Spanish general election.[28] The rush by then Prime Minister José Maria Aznar's Liberal-Conservative government to inaccurately blame ETA, the poor state of the economy and the failure to stop the terrorist attack all led to a surprise election win by the Socialist Workers' Party.[29] Under new Prime Minister José Luis Rodríguez Zapatero, Spain promptly pulled its 1,300 troops out of Iraq.

Other examples of Al-Qa'ida's attempts to influence elections include threats made in propaganda videos prior to elections in the US in 2004, Pakistan in 2007 and Germany in 2008.[30] Al-Qa'ida's line of argument within these videos was that Western troops were aggressors illegally operating in Muslim lands and that if they did not leave, Muslims had a duty to kill Western citizens. It is unlikely that Al-Qa'ida ever believed it could influence Western elections; rather, it sought to spoil elections (a symbolic Western target) and maximise the publicity that would be generated at a time of heightened media fervour.

More recently, Jason Burke speculated about whether the attack by Daesh (also known as the Islamic State of Iraq and Syria, ISIS) in Paris in April 2017 was an attempt to influence the French presidential election in favour of Le Pen to create an uprising among France's substantial Muslim population and gain media attention,[31] or simply a failed attempt at political sabotage, of the variety favoured by US President Richard Nixon and his henchmen in the lead-up to Watergate. Nixon's techniques involved more than disinformation (usually via 'leaked letters'). His campaign disrupted political conferences, paid people for votes, astroturfed activists,[32] and spied on others' campaigns.

Public and Media Reaction to Alleged Russian Interference in US Elections

The examples above indicate that foreign interference in elections is not new and has been funded on occasion through the covert operations budgets of intelligence agencies. It is clear that assassinations and intelligence agencies acting against their own democratic governments are unacceptable, or a violation of norms. However, recent alleged Russian interference in other countries' elections is arguably nothing more than a variation on an established norm of espionage. Similarly, it could be argued that all interference in elections is norm-violating, because it involves interference in a country's domestic affairs (which is covered by international law).

So how might the 2017–18 Western reaction to perceived Russian interference in recent elections be explained?

First is the proximity of the alleged interference to the timing of major events, in particular today's elections, which involves a high level of media reporting, and contemporary news is social and global. The allegations are salient in today's news, rather than the result of an exposé in a later inquiry.

Second, the 'always available' aspect of today's social media and digital news reaches many audiences beyond television and newspapers. This offers a degree of specific targeting of individuals and messages hitherto unknown in mass media, enhancing the salience to intended audiences through packaging and channels tailored to specific groups.

Third, and related to the second, is the revelation of the sheer comprehensiveness of the strategy employed by Russia. According to Clint Watts, Russian disinformation has five objectives, which are to: '[u]ndermine citizen confidence in democratic governments; [create] divisive political fractures; [e]rode trust between citizens and elected officials and democratic institutions; [p]opularize Russian policy agendas within foreign [and Russian diaspora] populations; [and create] general distrust … over information sources by blurring the lines between fact and fiction'.[33] Watts's view is that Russian interference goes beyond support of one candidate to attacking entire systems, at the basis of which is public trust in institutions, allies and information. Creating instability may be seen as a variant of the ancient tactic of divide and conquer. Social media makes a quantitative and qualitative difference to the way instability and distrust can be prosecuted, given its ubiquity and reach. By the same token, news of Russia's election interference also disseminates on the internet, affecting public perceptions and attitudes. Moral outrage, mistrust and disgust are more likely to be expressed on social media than by mainstream media, since the latter are much more likely to check their sources.

The 'means' to influence foreign elections via disinformation has tended to occur through character assassination, achieved via negative campaigning. Pre-internet, character assassination techniques made use of faked letters, designed to instil moral outrage in the electorate. The technique is exemplified in the way that the Okhrana (Department for Protecting Public Security and Order, the secret service of imperial Russia) developed the 'Protocols of the

Elders of Zion' – a fabricated document purporting to be a Jewish manifesto for world government – to justify pogroms in 1905.[34] The creation of the Zinoviev Letter was a similar activity, also in the pre-internet era. The Russians believe in the idea, according to an old KGB quote, of '[forcing] the enemy to take our strength for weakness, and our weakness for strength, and thus will turn his strength into weakness'.[35] As far as Western nations are concerned, Russia appears to believe that the West's weakness – its centre of gravity – is the democratic system and open accountability to the electorate.

The Russians may also believe that the West undervalues its hybrid warfare strategy, which Moscow might see as its strength and the West's weakness. Interfering in elections is therefore to the Russians simply one more element of the information dimension of a hybrid war strategy. What is different about recent alleged Russian interference in both the US and French elections is that it appears to have mixed elements of *dezinformatsiya* (disinformation, by hacking into Democratic National Committee and En Marche! servers and finding, leaking and/or doctoring contentious emails or documents) and *maskirovka* (military deception, by concealing their involvement through leaking the material via a third party, in the US via WikiLeaks[36] and in France through emLeaks[37]). Russian election interference fits within a 'hybrid warfare' strategy more generally.[38]

Fourth, there is a difference between a foreign country supporting a candidate in an election in that candidate's country (which is usually regarded as a breach of diplomatic protocol) and a perception that the foreign country is part of an opponent's 'team', as media revelations about Trump's campaign claimed links with the Kremlin allegedly reveal.[39] This is precisely the scenario in the allegations concerning meetings between Russian representatives and Trump's campaign team and family members (since the Republicans were then in opposition) and explains the furore surrounding the public reaction.

Fifth, when the allegation was made on the link between the Trump campaign team and Russia, there was a suggestion of manipulative intent (that Moscow supported Trump's campaign), making it more likely that the public would cease to be persuaded by covert Russian information sources (assuming there was any hint of such influence). One key element of negative campaigning – the kind of 'smear' campaigning that occurs in elections – is that it works effectively only when there are no 'fingerprints' left on it. If there are, the opposite effect of causing harm not to the person intended but to the source of the attack occurs, known as the 'boomerang effect'.[40] Conversely, a sophisticated smear campaign would leave few, if any, fingerprints such that it would not even be perceived as a smear campaign.

Sixth, to prosecute a case, the spreaders of the malicious falsehoods need to be identified, which is not easy if the acts were done anonymously via the internet. One somewhat weak line of defence against character assassination is the law on libel (published lies) and slander (spoken lies). Vigorously pursuing these where they relate to personal attacks on candidates in elections (as opposed to attacks on parties or policies) is an initial consideration. But this is difficult given that perpetrators are likely to be operating from outside the jurisdiction in which the election intervention has taken place. However, in the US, proving defamation, slander or libel is difficult as it is often set against the rights set out by the First Amendment, especially the rights to freedom of speech.[41] There is a higher burden of proof required that the defendant deliberately and maliciously spread the lies.[42]

Countering Foreign Interference in Elections

To counter election interference, several measures can be taken. Former British Prime Minister Margaret Thatcher assessed that one way to defeat terrorists and hijackers in the 1980s was 'to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend'.[43] In particular, she was thinking of the Provisional IRA. From 1988 to 1994, she instituted a censorship policy that stopped UK terrestrial broadcasters from airing the voices of representatives from eleven political and paramilitary organisations in Northern Ireland, including those of the IRA's political wing, Sinn Féin.[44] Censorship at the time was controversial and was met with incredulity by the public as actors were used to voice the words of the censored individuals. The censorship policy was eventually dropped after the government of the Republic of Ireland dropped their own similar policy in 1994 and the Provisional IRA declared a ceasefire.[45] In the internet era, such censorship is neither advisable, given the Northern Irish example, nor possible. The question arises: what might be done instead?

Part of the answer lies in the need for Western countries (and collectively as NATO) to build a stronger counter-influence capability, particularly against Russia. This is also a conclusion drawn by the US Senate Committee on Foreign Relations in its recent report on Russian election interference.[46] There are two main ways of dealing with such interference. First, political parties and their election campaigns could be regarded as critical national infrastructure, as are energy companies and transport networks, especially given that they represent the decision-making of a state in its most raw form. Political parties would therefore represent a vulnerability in the critical national infrastructure, suggesting that they should be encouraged to develop stronger cyber security procedures and processes to reduce their vulnerability and be subject to related stress-tests and checks.

Second, the West needs to build a more critical and resilient media and electorate. This is an interesting problem and one the West has faced before. For example, in 1937 in the US, the Institute for Propaganda Analysis was created to counter political propaganda, particularly from the Nazis, communists and domestic firebrands such as the fascist-supporting and anti-semitic Father Charles Coughlin, who used radio and newspaper so effectively to disseminate anti-New Deal propaganda, in 1936.[47] In 1938, Congress passed the Foreign Agents Registration Act, which required 'foreign agents' to disclose their involvement in US politics, especially where they produced 'informational material' (propaganda), in response to the perceived fear that there might be a large number of German propaganda agents in the US in the lead up to the Second World War. In the 1960s, foreign funding of US elections was banned for the same reason. In many

countries, it is now an offence either to accept foreign political donations or foreign support in election campaigns.

The West also needs to build an infrastructure to detect and disrupt foreign influence operations, whether it is focused on elections or otherwise. Just as counter-*intelligence* doctrine and departments have been developed, so should counter-*influence* doctrine and departments. The role of the intelligence community is central to election influence. The West needs to use its intelligence apparatus to identify and stop these influence attacks, and understand why they are happening, and to what end. This requirement is compounded by the fact that election influence operations often appear to be run by foreign (para)militaries, which means large-scale monitoring of elections through social listening and other means of intelligence collection.[48] The task also requires the development of an early warning system – a kind of radar for online disinformation – to identify the source and cause of the moral outrage that such disinformation usually seeks to inspire.

Western governments legislate to ensure social media companies work harder to identify the sources of duplicitous content and to expose them. Whether this requires legislation is open to debate. Social media companies can be regarded as publishers and should therefore act like publishers, within the bounds of the law, particularly around hate speech, since hate speech is not covered by the general protections for free speech. The West should also adopt an influence agenda that is diametrically opposed to Russian influence aims, namely to: rebuild confidence in democratic institutions; reduce political divisiveness; rebuild trust with citizens; and contrast fact and fiction in contexts where adversaries are running disinformation operations.[49] The West should also decide anew to promote their democratic ideals abroad.

Conclusions

This article provides examples of foreign interference in elections, seeking to draw conclusions regarding this contested norm. The distinction between national security and broader political and commercial interests is lost at our peril when militaries and intelligence communities target civilians (which is what 'electors' are as opposed to soldiers). The notion of trust-building, especially among one's own population (that which a foreign adversary is targeting), must be a counter to the trend in the promotion of instability and uncertainty. This is the challenge for today's internet-connected world where social media favours controversy and conspiracy and acts as a voice for both the scrupulous and unscrupulous.

Norms lie on a spectrum of activity, with the acceptable at one end and clearly unacceptable behaviour at the other. Such a spectrum highlights blurred boundaries when attempting to maintain a rules-based international system. At the acceptable end might be placed the activities of those militaries that stay within the bounds of the laws of armed conflict, taking heed of such principles as proportionality, military distinction and necessity. At the other end might be found the wanton violence of terrorist groups or political assassination by state entities. The polarities of such a spectrum are uncontroversial for those who believe in a rules-based international system. However, these obvious positions are neither sufficient nor worthy conclusions in helping with the problems of a more interconnected world. It is in the realm of covert actions and the deliberate obfuscation and ambiguity of sources and actors that the boundary issues lie across the spectrum.

As stated earlier, state espionage is a de facto international norm. As such it straddles a blurred boundary between what is acceptable or unacceptable behaviour. As mentioned, one attempt by the US at signposting a norm was about China's commercially motivated espionage. This provides tacit recognition of a blurred boundary, which does not undermine the existing norm of espionage per se, but highlights the appropriateness of the ends, ways and means. An assessment therefore needs to be made of the legitimacy of covert cyber operations intended to influence foreign elections that are conducted by intelligence communities and their proxies. How could the use of sock puppets as state messengers buying adverts on social media through fake avatars be assessed,[50] and how could this assessment help to establish international norms?

There are two dynamics that may offer a way forward, highlighted in all the examples discussed in this article. The first is similar to the distinction between civilian and military targeting in the Law of Armed Conflict and might be framed as national security interests versus, for example, commercial or political interests. The second dynamic is the end in itself, its ways and means of trust-building rather than the outcomes per se.

Regarding the first dynamic, the US, in its dialogue with China, has shown a distinction between national security and commercial ends in espionage, and the same should apply to elections. Therefore, civilians in cyberspace or their services and businesses should not be targeted, and only then, if at all, in the exceptional case that it is clearly a matter of national security. This means that the influence of democratic elections as a norm stays within the area of diplomacy and open debate, rather than a target for military and intelligence agencies. This is also consistent with the emerging norm that cyber operations under the law of armed conflict must focus on military necessity and distinction from civilian targets – something that, admittedly, technology does not make easy for decision-makers.

The second dynamic is a call for states to conduct themselves in ways and means that promote trust, and in accordance with the rule of law. The process of trust-building itself becomes the yardstick by which ends, ways and means are judged, and trust-building is an end in itself. This means preserving trust in digital infrastructure, since it serves everyone, rather than allowing its descent into a battlespace. It means preservation of ethical commercial interests, allowing people to generate economic value and to trade with confidence. The pursuance of an end that favours instability and damages public trust in an adversary state may be tempting in the short term, but in the longer term, it is trust between people and in institutions that brings about sustained political settlements that do not rely solely on the threat of punishment. This argument goes for Russia as much as for any individual Western state.

There are at least two instances where states are unlikely to follow this advice. First, in the pursuit of authoritarianism

and self-interested preservation of an elite and, second, when countries seek to incite revolution elsewhere. If either of these circumstances is ever justified, they lie outside the norm of international behaviour and are, by definition, exceptional. A state might make the political argument for one political end or one politician over another, but destroying trust, and the possibility of a negotiated settlement (such as through diplomatic means) between adversarial countries, is in nobody's interest. ■

Paul Baines is Professor of Political Marketing at Cranfield University and an associate fellow at the King's Centre for Strategic Communications, King's College London. Paul's most recent political book is Explaining Cameron's Catastrophe *(IndieBooks, 2017).*

Nigel Jones is a visiting fellow at King's College London, Department of Defence Studies, Chief Executive of the Information Assurance Advisory Council (IAAC), and Director at Accordance Associates.

Notes

1 Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization* (Vol. 52, No. 4, Autumn 1998), pp. 887–917.

2 *Ibid*., p. 896.

3 *Ibid*., p. 892.

4 US Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage', press release, 19 May 2014.

5 Martin Libicki, 'The Coming of Cyber Espionage Norms', 9th International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 2017.

6 See Jeffrey W Meiser, 'Are Our Strategic Models Flawed? Ends+Ways+Means = (Bad) Strategy', *Parameters* (Vol. 46, No. 4, Winter 2016–17).

7 Sarah Pruitt, 'That Time a Foreign Government Interfered in a U.S. Presidential Election – in 1796', *History*, 16 March 2017.

8 Natasha Geiling, 'The (Still) Mysterious Death of Edgar Allan Poe', *Smithsonian.com*, 7 October 2014.

9 Richard Norton-Taylor, 'Zinoviev Letter was Dirty Trick by MI6', *The Guardian*, 4 February 1999.

10 Laura Beers, *Your Britain: Media and the Making of the Labour Party* (Cambridge, MA: Harvard University Press, 2010), p. 64.

11 Christopher Andrew, *The Defence of the Realm: The Authorized History of MI5* (London: Allen Lane, 2009), pp. 148–52. See also Christopher Andrew, 'The British Secret Service and Anglo-Soviet Relations in the 1920s Part I: From the Trade Negotiations to the Zinoviev Letter', *Historical Journal* (Vol. 20, No. 3, September 1977), pp. 673–706.

12 Tim Weiner, 'F. Mark Wyatt, 86, C.I.A. Officer is Dead', *New York Times*, 6 July 2006. See also William Blum, *Killing Hope: US Military and CIA Interventions Since World War II* (London: Zed Books, 2014), p. 32.

13 The Pike Report was originally leaked by *Village Voice*. See *Village Voice*, 16 February 1976, available at <https://www.cia.gov/library/readingroom/docs/CIA-RDP03-01541R000200420004-8.pdf>. See also *CIA: The Pike Report* (Nottingham: Spokesman Books, 1977).

14 *Time Magazine*, 'Italy: Fateful Day', 22 March 1948.

15 Blum, *Killing Hope*. To see the content of the template letters, see: C Edda Martinez and Edward A Suchman, 'Letters from America and the 1948 Elections in Italy', *Public Opinion Quarterly* (Vol. 14, No. 1, Spring 1950), pp. 111–25.

16 For a definitive overview of the CIA's activities in this campaign, see James E Miller, 'Taking off the Gloves: The United States and the Italian Elections of 1948', *Diplomatic History* (Vol. 7, No. 1, January 1983); and Mario Del Pero, 'The United States and "Psychological Warfare" in Italy, 1948–1955', *Journal of American History* (Vol. 87, No. 4, March 2001).

17 See Paul Lashmar and James Oliver, *Britain's Secret Propaganda War* (Stroud: Sutton, 1998), pp. 1–10.

18 Black propaganda is false information and material purporting to be from a source on one side of a conflict, but which is, in fact, from the opposing side. It is typically used to vilify, embarrass or misrepresent an adversary.

19 US Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate: Together with Additional, Supplemental and Separate Views*, 6 volumes, Report No. 94-755 (Washington, DC: US Government Printing Office, 1976).

20 Kristian Gustafson and Christopher Andrew, 'The Other Hidden Hand: Soviet and Cuban Intelligence in Allende's Chile', *Intelligence and National Security* (Vol. 33, No. 3, 2018), pp. 407–21.

21 Ben Farmer, 'Russia Plotted to Overthrow Montenegro's Government by Assassinating Prime Minister Milo Djukanovic Last Year, According to Senior Whitehall Sources', *Daily Telegraph*, 19 February 2017.

22 Guy Delauney, 'Rumours and Spies in the Balkans as Russia Seeks Influence', *BBC News*, 12 December 2016.

23 Olivia Solon, 'Facebook Says Likely Russia-Based Group Paid for Political Ads During US Election', *The Guardian*, 7 September 2017.

24 Adam Nossiter, David E Sanger and Nicole Perlroth, 'Hackers Came, but the French were Prepared', *New York Times*, 9 May 2017.

25 Barney Henderson and Chris Graham, 'Russia Blamed as Macron Campaign Blasts "Massive Hacking Attack" Ahead of French Presidential Election', *The Telegraph*, 6 May 2017.

26 Alex Hern, 'Macron Hackers Linked to Russian-Affiliated Group Behind US Attack', *The Guardian*, 8 May 2017.

27 Elizabeth Nash, 'Madrid Bombers "Were Inspired by Bin Laden Address"', *The Independent*, 7 November 2006.

28 *The Telegraph,* 'Rush Hour Bombings Kill 190 in Madrid', 11 March 2004.

29 Lizette Alvarez and Elaine Sciolino, 'Bombings in Madrid: Election Outcome; Spain Grapples with Notion that Terrorism Trumped Democracy', *New York Times*, 17 March 2004.

30 Paul R Baines and Nicholas J O'Shaughnessy, 'Al-Qaeda Messaging Evolution and Positioning, 1998–2008: Propaganda Analysis Revisited', *Public Relations Inquiry* (Vol. 3, No. 2, May 2014).

31 Jason Burke, 'Was the Paris Attack an Isis Attempt to Influence the French Election?', *The Guardian*, 21 April 2017.

32 'Astroturfing is the attempt to create an impression of widespread grassroots support for a policy, individual, or product, where little such support exists. Multiple online identities and fake pressure groups are used to mislead the public into believing that the position of the astroturfer is the commonly held view'. See Adam Bienkov, 'Astroturfing: What it is and Why it Exists', *The Guardian*, 8 February 2012.

33 Clint Watts, 'Statement Prepared for the U.S. Senate Select Committee on Intelligence Hearing: "Disinformation: A Primer in Russian Active Measures and Influence Campaigns"', 30 March 2017.

34 Michael Hagemeister, 'The Protocols of the Elders of Zion: Between History and Fiction', *New German Critique* (Vol. 35, No. 1, Spring 2008).

35 Yevgenia Albats, *KGB: State Within a State*, translated by Catherine A Fitzpatrick (London: IB Tauris, 1995), p. 170.

36 'The DNC Database', from the Accounts of Seven Key Democratic Party Officials, documents obtained by Wikileaks, January 2016–25 May 2016, <https://wikileaks.org/dnc-emails>, accessed 30 January 2018.

37 Hern, 'Macron Hackers Linked to Russian-Affiliated Group Behind US Attack'.

38 'Hybrid warfare' refers to Russia's broad use of a range of subversive instruments, many of which are non-military, to further Russian national interests. See Christopher S Chivvis, 'Understanding Russian "Hybrid Warfare" and What Can Be Done About It', testimony before the House Armed Services Committee, 22 March 2017.

39 Emma Kinery, 'Timeline: Donald Trump Jr.'s Interactions with Kremlin-Linked Lawyer', *USA Today*, 11 July *2017*.

40 Damian McBride, an aide who famously smeared opponents with sexual lies for then British Labour Prime Minister Gordon Brown, was caught in the act of smearing and lost his job in the resulting scandal. See James Cusick, 'The McPoison Papers: Confessions of Rogue Labour Spin Doctor Damian McBride Laid Bare in Memoir', *The Independent*, 19 September 2013.

41 The First Amendment of the US Constitution states: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances'. See Legal Information Institute, 'US Constitution: First Amendment', Cornell Law School.

42 *The Economist*, 'Defamation Laws are Necessary. But They Must be Narrowly Drawn', 13 July 2017.

43 Margaret Thatcher, 'We Must Try to Find Ways to Starve the Terrorist and the Hijacker of the Oxygen of Publicity on Which They Depend', speech given to the American Bar Association in London, 15 July 1985.

44 Francis Welch, 'The "Broadcast Ban" on Sinn Fein', *BBC News*, 5 April 2005.

45 Rhys Williams, 'Broadcasters Welcome End to "Censorship"', *The Independent*, 16 September 1994.

46 United States Senate Committee on Foreign Relations, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security', 115–21, 2nd Session, 115th Congress, US Government Publishing Office, 10 January 2018.

47 Albin Krebs, 'Charles Coughlin, 30's "Radio Priest"', *New York Times*, 28 October 1979.

48 Social listening uses social media analysis to identify public and consumer trends. See Dominique Jackson, 'What is Social Listening and Why is it Important?', *Sprout Social*, 20 September 2017.

49 For a more detailed discussion on Russian disinformation, see Andrew Weisburd, Clint Watts and J M Berger, 'Trolling for Trump: How Russia is Trying to Destroy our Democracy', *War on the Rocks*, 6 November 2016.

50 A sock puppet is an online identity used for the purposes of deception.