DISINFORMATION IN SCOTTISH PUBLIC LIFE

AN OVERVIEW OF THE THREAT AND PROPOSED SOLUTIONS

Stewart McDonald MP

CONTENTS

FOREWORD BY STEWART MCDONALD MP

‘Facts are chiels that winna ding, and downa be disputed’, wrote Robert Burns almost 250 years ago. To translate from Scots, it means simply that facts are facts; the line exemplifies Burns’s belief – as a son of the Scottish Enlightenment – in objective truth and the importance of human reason.

Such ideas can, at times, seem as distant to us today as the bard himself, as we watch facts disputed, distorted and weaponised on a daily basis across the world, including in Scotland.

Disinformation is not a new problem. However, it is growing in sophistication, scale and reach and I have spoken and written on numerous occasions urging us as a society to call time on the false sense of security in which we continue to bask. Disinformation poses an urgent threat to all free and open societies, and Scotland is no exception. However, as other countries think seriously about how to combat hostile disinformation campaigns, Scotland has been uncharacteristically mute on the subject. Thankfully, that is starting to change: the manifestos of some parties at the 2021 Scottish Parliament election, including my own, show that there are those who have started to engage with the issue. The work, however, is just beginning.

In this paper I sketch out some examples of how Scotland’s information ecosystem has become polluted by disinformation actors. It is by no means a full-spectrum picture and, similarly, the solutions presented at the end are not a wholescale strategy. The purpose of this is to first answer my own challenge to get serious about tackling the threat of disinformation, but to present also a call to other political and civil society actors in Scotland to recognise the challenge it presents us with and to join together to combat that challenge. This paper is not an SNP policy paper or a paper about the constitution, but instead one that seeks to build much-needed consensus to help us move forward.

I want to give thanks to Elisabeth Braw for her valuable insight and contribution to this paper. I also want to thank Roddy McGlynn from my staff team for his work and input to the report.

SECTION I: THE DISINFORMATION AGE

Propaganda, 'fake news' and disinformation are tools which have been used by political actors to further their goals for centuries. However, the dawn of the globalised internet age, where information can travel across the world in seconds, has lent a qualitatively new dimension to their use, and disinformation – the deliberate, often covert, spreading of false information to manipulate public opinion and distort the truth – has become a fixture of the modern information ecosystem.[1]

Disinformation campaigns, note the European External Action Service, continuously evolve 'based on the success of their application, changes in potential adversaries' vulnerabilities and developments in measures to counter them'.[2] Indeed, between 2017 and 2021, alongside an increase in commercial actors offering their services to run domestic and international information campaigns, Facebook observed the emergence of information campaigns which seek to 'mimic authentic voices and co-opt real people into amplifying their operations.'[3] New advancements in Artificial Intelligence have seen the proliferation of these increasingly sophisticated methods of mimicry, including deep fakes and AI-generated faces – these new technologies mean that disinformation is not only a qualitatively new threat, but one which is constantly evolving as hostile actors locate new rifts to exploit in an increasingly online society.[4]

From the 2007 riots in Estonia to the recent storming of the United States Capitol, the death, destruction and disorder that disinformation has caused has been plain to see. This situation will likely only get worse: the 2021 Edelman Trust Barometer report painted a picture of 'an epidemic of misinformation and widespread mistrust of societal institutions and leaders around the world', with 57 per cent of those surveyed globally reporting a belief that government leaders and members of the media 'are purposely trying to mislead people by saying things they know are false or gross exaggerations.'[5] Without concerted action to turn this tide, societies run the risk of becoming trapped in self-reinforcing feedback loops of distrust and disinformation that tug at the threads which hold our communities together.

This report will sketch a picture of the information ecosystem in Scotland and, drawing on examples of best practice from around the globe, will suggest actions which could help build information resilience in Scottish society.

---

[1] House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news',* 14th February 2019; Alan Rusbridger, *News and How to Use It* (Edinburgh: Canongate, 2020), p. 65
[2] European External Action Service, *Food-for-thought paper: Countering Hybrid Threats* (2015), p. 3
[3] Facebook, *Threat Report: The State of Influence Operations 2017-2020* (May 2021), p. 4-5
[4] Kai Shu, Suhang Wang, Dongwon Lee, Huan Lui, *Disinformation, Misinformation, and Fake News in Social Media* (Cham: Springer, 2020), p. 96
[5] Edelman, *Edelman Trust Barometer 2021*. Accessed: https://www.edelman.com/trust/2021-trust-barometer

SECTION II: THE DISINFORMATION FOOTPRINT IN SCOTLAND

Disinformation campaigns allow hostile foreign states to discreetly target and influence citizens while remaining below the threshold of war, fomenting distrust and polluting the information ecosystem. Russia, China and Iran have all been credibly accused of attempting to distort the information ecosystem in Scottish public life, using a range of platforms and media to manipulate public opinion. These campaigns do not themselves create distrust or division, but instead exploit existing rifts in societies and capitalise on pre-existing feelings and beliefs. This section will outline the variety of tactics used by three hostile states.

Iran

Between 2018 and 2021, Facebook took down hundreds of pages, groups and accounts which were linked to the Islamic Republic of Iran.[6] These accounts – part of what 'appears to have been a short-lived experiment conducted with a relatively small number of accounts' conducted without 'the scale, the sophistication, or the duration of the later Russian efforts' – produced and shared content posing as members of political movements in Western democracies, including the 2012 Occupy Movement in the USA and the 2014 Scottish independence referendum.[7] While these accounts 'do not appear to have yielded viral impact or any other measurable form of success', the existence of 'a confirmed data point on attempted foreign interference in Western democratic exercises as far back as 2012, a full electoral cycle before the Russian interference of 2016' makes it clear that information operations by hostile foreign states have a longer history in Western liberal democracies than is often commonly believed.[8]

While Iran's disinformation operation is perhaps the least sophisticated of the hostile foreign states operating in Scotland, it serves as a potent reminder that – while Scotland may not yet be a fully-fledged global actor – hostile foreign states across the world are actively attempting to influence and manipulate public sentiment in Scotland. Given the attention focused on the independence campaign in 2014, it is reasonable to assume that Iranian action will resume or intensify in the run-up to any second independence referendum. It is therefore in the interests of the Scottish Government and the wider independence movement to meaningfully engage with the threat that disinformation poses to our democratic process and to take steps to counter it.

[6] Facebook, 'Taking Down More Coordinated Inauthentic Behaviour', 21st August 2018; Facebook, "February 2021 Coordinated Inauthentic Behaviour Report", 3rd March 2021
[7] Ben Nimmo, C. Shawn Eib, Léa Ronzaud, Rodrigo Ferreira, Thomas Lederer, Melanie Smith, *Iran's Broadcaster: Inauthentic Behaviour,* 5th May 2020, p. 1
[8] Nimmo et al, op. cit., p. 2

SECTION II: THE DISINFORMATION FOOTPRINT IN SCOTLAND

Russia

For decades, the Russian Federation has been one of the world's most notorious disinformation actors, setting the path that North Korea and Iran have followed.[9] Today, Russia remains the world's largest producer of disinformation and has been an active disinformation actor in Scotland since at least 2014.[10] Using a variety of techniques, including foreign broadcast networks and interference in electoral events, Russia has sought to push Kremlin-endorsed narratives into the Scottish public sphere.

Electoral interference

The Russia Report produced by the UK Parliament's Intelligence and Security Committee notes that 'credible open source commentary' suggests that the Russian government attempted to influence the 2014 Scottish independence referendum and the 2016 Brexit referendum.[11] The UK Government has refused to confirm or deny this, leaving a vacuum to be filled by speculation and conspiracy theories.[12] Indeed, 40 per cent of Scottish voters believe that Russia interfered in the 2014 Scottish independence referendum and highlighted that, across the UK, more voters than not believe that the Russian government has interfered in the last three General Elections, the 2014 Scottish independence referendum and the 2016 EU referendum.[13] Absent a clear statement from the UK Government on the scale and effectiveness of Russian electoral interference – like that given by Facebook regarding Iranian operations – a significant proportion of the Scottish public has concluded that their elections are not wholly free and fair. The storming of the US Capitol in January 2021 showed quickly these narratives can take root and how serious a threat to our democracy they represent. The UK Government must be more accountable and transparent with UK citizens if it is to ensure full public confidence in its electoral system.

Foreign broadcast networks

The Russian government has made extensive use of its state-backed media platforms in Scotland, platforming George Galloway and Alex Salmond on RT and Sputnik. These platforms exist to promote the Kremlin's line on issues of key concern to the Russian state: after the Skripal poisoning, RT was fined £200,000 for repeatedly breaching impartiality rules. A 2018 report from Kings College London on Russian-state backed media in the UK found that RT and Sputnik pushed a variety of narratives around the Skripal poisoning, including the idea that that the Novichok found at the scene was produced by the United Kingdom and that

[9] Facebook, *Threat Report: The State of Influence Operations 2017-2020,* 1st May 2021
[10] Ibid.
[11] Intelligence and Security Committee of Parliament, *Russia*, 21st July 2020, p. 7
[12] Ibid.
[13] Opinium, *The Political Report,* 23rd July 2020

the poising was a hoax orchestrated the by UK intelligence services.[14] While the threat from these platforms should not be underestimated, the relative failure of Russian disinformation to take root in Scotland had been demonstrated by the closing of the Sputnik office in Edinburgh in April 2021, citing a 'hostile environment'.[15] Nonetheless, RT and Sputnik continue to maintain offices across the UK, producing English-speaking content for a Scottish audience.

These platforms' coverage of European and North American democracies overwhelmingly focuses on social and political dysfunction, aiming to foment discontent with political elites - the increasing appeal of these narratives to the public speaks to a divided, polarised and fragmented society.[16] When surveyed by the Mental Health Foundation in February 2021, 18-24-year-olds in Scotland were the most likely to have felt loneliness during the pandemic: 43 per cent of young people had felt lonely compared to around 26 per cent of the population at large.[17] This phenomenon, combined with an increasing reliance on digital devices makes this group particular vulnerable to information operations which seek to capitalise on unhappiness and discontentment. In general, declining interaction with others, including people who may hold different opinions, makes citizens inclined to think ill of others, while less time spent with others and more with their digital devices strengthens the power and reach of disinformation.

COVID-19

Since before the COVID-19 pandemic, Russian bots and troll farms, in conjunction with Russia's foreign broadcast networks, have pushed anti-vaccination messages on Western social media.[18] This campaign has continued and increased in intensity during the COVID-19 pandemic, with Russian state authorities, state companies and state mass media engaging in 'almost daily interventions' to advertise and promote the Sputnik vaccine across Europe while attempting to cast doubt on the efficacy and safety of Western-made vaccines.[19] With the Scottish Chief Medical Officer warning that vaccine misinformation was amongst the 'biggest dangers' Scotland faces, Russian disinformation impedes efforts to inoculate the population and keep citizens safe from COVID-19 and other viruses.[20]

---

[14] Gordon Ramsay and Sam Robertshaw, 'Weaponising News: RT, Sputnik and Targeted Disinformation', KCL Policy Institute (2018)
[15] Moscow Times, 'Russian State-Funded Sputnik News Pulls Out of Britain', 2nd April 2021
[16] Rhys Crilley, Marie Gillespie, Bertie Vidgen, Alistair Willis, 'Understanding RT's Audiences: Exposure Not Endorsement for Twitter Followers of Russian State-Sponsored Media', *The International Journal of Press and Politics* (2021): 1-23
[17] Wave 10: Late February 2021 Coronavirus: Mental Health in the Pandemic. Accessed: https://www.mentalhealth.org.uk/research-and-policies/wave-10-late-february-2021
[18] D.A. Broniatowski, A.M. Jamison, S. Qi , et al. 'Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate', *American Journal of Public Health* 108 (2018): 1378–84; Katherine Kirk, 'How Russia sows confusion in the US vaccine debate' *Foreign Policy*, 9th April 2019
[19] European External Action Service, *COVID-19 Disinformation: EEAS Special Report,* 29th April 2021
[20] Andrew Learmonth, 'Covid: Gregor Smith warns vaccine misinformation is among 'biggest dangers' Scotland faces', *The National*, 18th January 2021

SECTION II: THE DISINFORMATION FOOTPRINT IN SCOTLAND

China

If 'Russia is a forest fire', said the former Deputy Director of the NSA in 2020, 'China is global warming'.[21] Rick Ledgett's words on the security threat posed by the two states have particular resonance when applied to their role in information warfare. While Russia often targets specific events, democratic processes or institutions, the Chinese government attempts to gradually shape the global narrative around key issues of importance to China.

Confucius Institutes

In a 2010 People's Daily article, the former head of the CCP's Propaganda Department stated that the goal of Confucius Institutes is to 'further create a favourable international environment for us' and to 'actively carry out international propaganda battles against issuers such as Tibet, Xinjiang, Taiwan, human rights and Falun Gong'.[22] Many Scottish universities, seeking new sources of funding amid tightening budgets, have welcomed this new income source offered from Beijing. Today, *The Times* reports that Scotland has the world's highest concentration of Confucius Institutes at universities and Confucius Classrooms at schools, language and cultural education facilities, all staffed with Chinese-trained and supplied teachers.[23]

Confucius Institutes appear similar to the British Council, Spain's Instituto Cervantes or Germany's Goethe-Institut. However, Confucius Institutes, located on university campuses and co-funded by the Chinese government, steer students away from discussing topics which are politically uncomfortable to the Chinese Communist Party, such as the Uighur minority in Xinjiang or the "three Ts": Tibet, Taiwan and Tiananmen Square. This attempt to launder China's international reputation includes a range of topics: one student at the University of Kentucky was told that reports of pollution in China were 'misinformation promoted in the US media.'[24] While Confucius Institutes may not engage in outright disinformation campaigns, their attempts to distort domestic political sentiment make them a key actor in the so-called information war. As Nina Jankovicz notes in *How to Lose the Information War* – her study of failed Central and Eastern European responses to Russian disinformation – these attempts to distort the information ecosystem mustalso be acknowledged and reckoned with. Without attention given to 'the spectrum of [information] threats beyond disinformation and an understanding that local actors are being manipulated', Jankovicz argues, anti-disinformation campaigns are doomed to fail.[25]

---

[21] Quoted in Susan Hennesey, and Jacob Schultz, 'Does the DHS Whistleblower Report Reveal an Election Interference Scandal?, *Lawfare*, 15th September 2020. Accessed via https://www.lawfareblog.com/does-dhs-whistleblower-report-reveal-election-interference-scandal

[22] Ethan Esptein, 'How China Infiltrated U.S. Classrooms', *Politico,* 16th January 2018

[23] Mark McLaughlin, 'Cut ties with "suppressive" China, leading academic tells Edinburgh University', *The Times*, 17th November 2020

[24] Esptein, op. cit

[25] Nina Jankovicz, *How to Lose the Information War* (London: Bloomsbury, 2020) p. 103

SECTION II: THE DISINFORMATION FOOTPRINT IN SCOTLAND

COVID-19

In May 2020, the European Commission stated for the first time that China had 'targeted influence operations and disinformation campaigns in the EU, its neighbourhood, and globally.'[26] These operations followed a path well trodden by its Confucius Institutes, attempting to manipulate and control the wider narrative around China while deflecting any criticism. While Russia has used information operations during COVID-19 to promote its Sputnik V vaccine, Chinese state media pushed stories which portrayed China as a transparent and responsible global actor which 'made sacrifices to buy time for the rest of the world' and aggressively rebuffed any suggestion to the contrary.[27]

The Scottish Threat Picture

As illustrated above, Scotland faces a range of disinformation actors who make use of a large and evolving toolbox of techniques to influence and corrupt the Scottish information ecosystem. There is no panacea for this problem.

From Russian state-linked television shows funded by the Kremlin and fronted by the former First Minister of Scotland to Confucius Institutes operated by the Chinese Communist Party, the Scottish public sphere is filled with hostile state actors who seek to contest the principles of openness and liberalism upon which our society is built. However, homegrown and domestic disinformation crises must not be discounted: conspiracy theories like QAnon or those related to the COVID-19 pandemic pose just as severe a threat to our national security and illustrate the urgent need to build national information resilience. The dis- and misinformation of the past year has shown how easily false information can disrupt our society, leading to shortages in supermarkets and panic among citizens; the events on the US Capital in January 2021 serve as a cautionary tale of how this story can end.

The Scottish and UK Governments should recognise that the past year has revealed just how vulnerable our societies are to disinformation – from within and outwith the state – and take urgent steps to build information resilience within the Scottish population. If hostile foreign powers use the state, businesses and private citizens to advance their disinformation campaigns, then liberal democracies' response must be similarly holistic. Transparency, accountability and truth must be the foundations upon which a response to information operations in Scotland is built. With this in mind, the following section will outline examples of best practice from abroad in tackling disinformation which the UK and Scottish Governments should draw on when formulating their strategy and policy responses.

---

[26] European Commission, *Joint Communication: Tackling COVID-19 Disinformation*, 10th May 2020)
[27] Wan Lin, 'Interventions avoid 7m infections in China', *Global Times,* 7th May 2020

SECTION III: INTERNATIONAL RESPONSES TO DISINFORMATION

While states across the world have spent recent years discovering the harm of disinformation and misinformation, no country has found – let alone established – structures that dramatically limit its reach and influence. In the absence of voluntary reform by social media companies and significant international legislation, countries are turning to the recipient side to limit the reach and power of information operations, with governments and civil society working together to inoculate citizens against disinformation and misinformation. While this alone is not sufficient, it is at least within governments' power. The primary defence against disinformation is maintaining a high level of public trust in the political system and mainstream media.[28] Supplementary to this, governments must spread public awareness of disinformation and implement policies to develop national and civic information resilience. This section will outline examples of policies from Finland, Sweden and Singapore which have been successful in achieving this.

Finland: Information Resilience Training and a Hybrid Ambassador

In the early 1960s, Finland – which knew it had to remain resilient to Soviet threats but had been banned in its "friendship treaty" with Moscow from operating any volunteer defence organisations of the kind that were common in Sweden – introduced an innovative concept known as *henkinen maanpuolustus* (HMP), or 'mental territorial defence'. While this programme was eventually replaced, its legacy is seen today in the Finnish focus on information literacy and national resilience. At the centre of this strategy is a governmental media education authority – the National Audiovisual Institute – which belongs to the Ministry of Education and Culture. The National Audiovisual Institute's Department for Media Education and Audiovisual Media oversees the development of a safe media environment for children and of children's media skills, helping schools teach media literacy. Similarly, Baltic states close to Finland (and Russia) have also taken similar approaches: Estonia has offered media education in its secondary schools since 2000 while Latvia teaches it in the national security curriculum which is being rolled out across the country.

Alongside childhood education, Finland has made efforts to tackle disinformation at the government level through the creation of an 'influence network' to co-ordinate counter-disinformation activities between Ministers and Departments. As part of this, Finland – like Spain, Sweden, Lithuania and Poland – has also appointed an ambassador for countering hybrid threats, who coordinates the cross-governmental response to national security threats like disinformation which straddles different areas of domestic and foreign policy. As part of Finland's whole-of-society approach, countering disinformation is also tackled outside government, with Helsinki becoming home to the European Centre of Excellence for Countering Hybrid Threats in 2017.

[28] Bennett & Livingston, 2018; Freelon & Wells, 2020; Garrett et al., 2020; Schia & Gjesvik, 2020

SECTION III: INTERNATIONAL RESPONSES TO DISINFORMATION

Sweden: Targeted resilience-building campaigns and mass awareness campaigns

Like Finland, Sweden takes a whole-of-society approach to countering disinformation, but pairs it with targeted information resilience training for key figures in the information ecosystem. In 2018, the Swedish government also announced the creation of a Psychological Defence Authority which would 'discover, counter, and prevent influence campaigns and disinformation, both nationally and internationally.'[29]

The same year, the Swedish government produced an emergency preparation pamphlet – 'If Crisis or War Comes' – which was sent to every household in Sweden. In addition to traditional threats, the document instructed Swedes to 'be on the lookout for false information' and identified it as a threat to national security.[30] Alongside mass awareness campaigns, the Swedish government has identified key groups to train in the battle against disinformation: it has produced a counter-disinformation handbook for communication staff in all parts of government and trains communication staff around the country in how to detect and counter ongoing influence operations.[31]

Singapore: Co-ordinated events by public bodies

Like Sweden and Finland, Singapore's response to information operations involves a whole-of-government and whole-of-society approach, with the Singaporean Total Defence doctrine involving 'every Singaporean playing a part, individually and collectively, to build a strong, secure and cohesive nation'[32] Each year on the 15th of February – the day Singapore fell to the Japanese in 1942 – Singapore marks Total Defence Day, marked in public institutions across the state. In 2019, the theme was digital defence, with a focus on disinformation and fake news: a national museum held an exhibition which showcased how propaganda and 'fake news' had threatened national security throughout Singaporean history, the National Library hosted a nation-wide competition to promote information literacy and a government minister gave a speech in which he implored citizens not to propagate or amplify disinformation or fake news.[33] By bringing together disparate public bodies, Total Defence Day reaches a wider public and reinforces Singapore's whole-of-society approach to countering disinformation.

---

[29] Library of Congress, 'Government Responses to Disinformation on Social Media Platforms: Sweden'. Accessed: https://www.loc.gov/law/help/social-media-disinformation/sweden.php#_ftn45

[30] MSB, *If Crisis or War Comes* (English Version) (2018). Accessed: https://rib.msb.se/filer/pdf/28706.pdf

[31] Gabriel Cederberg, 'Catching Swedish Phish: How Sweden is Protecting its 2018 Elections', Defending Digital Democracy Project, August 2018

[32] Singapore Ministry of Defence, *What is Total Defence?* Accessed: https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about.html

[33] Vanessa Lui, 'Total Defence Day to focus on Fake News', *Singapore Straits,* 29th January 2019; Aqil Mahmud, 'Don't forward fake news, use strong passwords: S Iswaran on putting Digital Defence into action', *Channel News Asia*, 16th February 2019; Singapore Ministry of Defence, *Fact Sheet: Digital Defence*, 15th February 2019. Accessed: https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2019/February/15feb19_fs

SECTION IV: PROPOSED SOLUTIONS

Previous sections have offered a sketch of the range and sophistication of information operations in Scotland and provided an outline of how three states have attempted to deal with the problem. The problems and their attempted solutions should illustrate that, while there is no panacea which will prevent disinformation operations from taking root, the three states above have all pursued policies which aim to build information resilience within their populations. While a coherent national strategy is required to tackle disinformation, the complex, country-specific and dynamic nature of the threats means that such a task is beyond the scope of this paper. Instead, and recognising the limited powers that the Scottish Government has to tackle this issue under the current devolution settlement, this paper proposes nine ways to tackle the problem of disinformation in Scotland:

1. The Scottish Government should appoint a commissioner for countering disinformation.
2. The Scottish Government should create and fund a Youth Information Initiative
3. Scottish media organisations should hold annual open days and/or media surgeries
4. The Scottish Government should commission an independent audit of the Scottish information ecosystem
5. The UK and Scottish Governments should introduce targeted literacy programmes for parliamentarians, civil servants and journalists
6. Political parties and faith groups should host disinformation workshops for their members
7. Scotland should host an annual Clean Information Summit
8. Scottish public bodies should host a series of co-ordinated anti-disinformation events and competitions
9. The UK Government should provide Parliament with an annual update of the threat assessment

1. A Commissioner for Countering Disinformation

In the UK, responsibility for countering disinformation is currently split across several departments and agencies: the National Cyber Security Centre, the Cabinet Office, the MoD, DCMS, FCDO and MI5/GCHQ. Despite the clear threat of Russian disinformation and political influence campaigns targeting the UK, the Intelligence and Security Committee noted in its Russia report that the issue of defending the UK's democratic processes has been 'something of a "hot potato", with no one organisation recognising itself as having an overall lead'.[34]

Drawing on the Finnish model of the hybrid affairs ambassador, the Scottish Government should take the lead on this issue by appointing a commissioner for countering disinformation. This may be done by extending the remit of the Scottish Information Commissioner or creating a separate commissioner's office.

[34] Intelligence and Security Committee of Parliament, *Russia*, 21st July 2020, p. 7

SECTION IV: PROPOSED SOLUTIONS

2. A Youth Information Initiative

As highlighted in the sections above, children and teenagers are a priority group for information literacy training. Alongside developing a comprehensive strategy for tackling disinformation and raising media literacy, the Scottish Government could offer information literacy training as an after-school activity, taught not by teachers but by professional journalists. To create distance between itself and the teaching, the Scottish Government could create a Youth Information Expertise Initiative, for which the Scottish Government would provide funding and set the parameters. Respected NGOs would bid for government contracts to deliver the teaching, which would involve recruiting and vetting the journalists teaching the courses. Participants who successfully completed the course would be rewarded with a voucher for a subscription to a quality news publication of their choice.

3. Media surgeries

Citizens often mistrust reporting by established news media.[35] In previous decades, the lack of trust may not have had a significant effect, as citizens were dependent on journalists for their information. Today, however, they turn to social media for alternative explanations to events. While the wider aim must be to ensure a successful and viable independent press in Scotland, in the short term this can be mitigated by creating more opportunities for interaction between journalists and ordinary citizens.

This could be achieved by building on MPs' surgery model. It would be in Scottish-based news media organisations' interest to pursue it independently of the government, perhaps under the auspices of a "clean Scottish news" initiative. News media would open pop-up mini newsrooms in rural and urban areas across Scotland, allowing citizens to see how the journalists work and be able to ask questions. This would allow news recipients the effort that journalists make to, for example, find sources and verify their stories. Journalists, in turn, would learn about citizens' concerns and frustrations by regularly interacting with them. [36] While this initiative would be independently led by the news organisations, it could be supplemented by other programmes such as an online 'Scottish clean news festival' or a series of panels and talks held at events such as the Edinburgh International Book Festival.

[35] Charlie Beckett, 'Coronavirus: why public trust is an issue for news media but don't trust those polls', *LSE,* 24th April 2020. Accessed: https://blogs.lse.ac.uk/polis/2020/04/24/why-public-trust-is-an-issue-for-news-media-but-dont-trust-those-polls/

[36] Elisabeth Braw, 'Vox populi? Citizen alienation and the political and media elite', Reuters Institute for the Study of Journalism Working Paper (August 2014). Accessed: https://reutersinstitute.politics.ox.ac.uk/our-research/vox-populi-citizen-alienation-and-political-and-media-elite

SECTION IV: PROPOSED SOLUTIONS

4. Information ecosystem audit

In 2020, the United States labelled Confucius Institutes 'foreign propaganda missions' which are 'owned or effectively controlled' by the Chinese Communist Party. The same year, Sweden became the first European state close all its institutes and classrooms. In Scotland, no such moves have been made to address the presence of Confucius Institutes or account for (for now) limited use of trolls, bots and foreign broadcast networks by hostile states and, because of this, there is no clear understanding of the threat these information campaigns pose.

In line with the remit given to the Swedish Psychological Defence Authority, the Scottish Government should commission an independent audit of the information ecosystem in Scotland, including an assessment of the availability of quality news to citizens and of the reach of foreign, state-backed bodies like RT and Confucius Institutes. Until we know more about how and why disinformation campaigns are undertaken in Scotland, work to counter them will be severely impeded.

5. Information resilience training

People will always exaggerate and embellish stories and politicians will always spin. However, elected members must be more cautious than most about what information they share. Sharing false information or 'unconfirmed reports' – as one MSP did in the Scottish Parliament in 2020 – erodes public trust in democratic institutions and the people who run them.[37]

The UK and Scottish Governments should, drawing on the Swedish experience and the model of the UK Parliament's 'Valuing Others' training, implement a course of information resilience training for politicians, political press officers and selected civil servants.

6. Inter-party, inter-faith and trade union workshops

While older citizens are more likely than younger ones to share false information on social media, they are often harder for resilience training campaigns to reach.[38] However, members of political parties, churches and trade unions represent a significant proportion of adult citizens who may be interested and willing to voluntarily sign up to information resilience training. These could take the form of intergroup events, with members of different faiths or political parties coming together in their city to take part in a workshop on identifying and countering false information in their communities. The intergroup nature of these events would also help to reduce polarisation and build community.

---

[37] George Allison, 'Local newspaper and MSP share misinformation on Army plans', *UK Defence Journal,* 19th March 2020

[38] Andrew Guess, Jonathan Nagler and Joshua Tucker, 'Less than you think: Prevalence and predictors of fake news dissemination on Facebook', *Science Advances* 5(1) (2019)

SECTION IV: PROPOSED SOLUTIONS

7. Clean Information Summit

Against the background of disinformation and misinformation being likely to increase ahead of a prospective second Scottish independence referendum, the Scottish Government should consider establishing itself as a leading government in the fight against disinformation. One of the ways it could do so would be by convening an annual Clean Information Summit, which would feature invited politicians from around the world, as well as academic experts, top media editors and social media executives. By doing so, the Scottish Government could position the fight against disinformation and misinformation as a global concern, become known as the place where pioneering efforts against disinformation and misinformation are presented and raise Scotland's profile as an independent actor on this key issue. Such a summit would also be a way for Scotland to prove its value to allies ahead of prospective independence. Indeed, it would also be a useful way for Scotland to present Edinburgh as a city where leaders from all walks of life meet to discuss a subject that poses a serious concern to liberal democracies across the world.

8. Co-ordinated exhibitions and competitions

Like Singapore, where Total Defence Day was marked with co-ordinated events in public bodies and a speech by a government minister, public bodies in Scotland could host events in the same month focused on propaganda, fake news and disinformation. Venues like the Glasgow Science Centre and the National Library of Scotland could organise competitions, exhibitions and talks to raise awareness of information literacy and the dangers of disinformation.

The Scottish Government could underwrite – again with NGOs in charge of the implementation – nationwide competitions for certain age groups where schools would select teams that would compete against other schools in Scotland. By hosting a series of co-ordinated events, the Scottish Government would drive home the message that disinformation requires a whole-of-society approach and help build resilience within its population.

9. Annual threat updates to Parliament

In refusing to confirm or deny Russian involvement in the 2014 Scottish independence referendum despite credible open source evidence, the UK Government creates a vacuum for speculation. [39] Drawing on the model of the annual Statements made to Parliament on the efforts to counter Daesh, the UK Government should provide Parliament with an annual update on its threat assessment regarding mis- and disinformation across the UK, and inform

[39] Intelligence and Security Committee, *Russia*, p. 7; Facebook, *Threat Report: The State of Influence Operations*

parliamentarians of measures taken to counter this. As mentioned above, without transparency, accountability and good governance, a vacuum is left to be filled by speculation, conspiracy theories and disinformation.

None of these policies will successfully counter disinformation on their own. However, as governments begin to take the threat of disinformation seriously and devise strategies accordingly, it is hoped that these ideas will contribute to a wider discussion about the role we can all play in building resilient societies.

GLOSSARY

AMPLIFICATION

Amplification involves the artificial spread of false, malicious or harmful information online. This can range from the intentional actions of a hostile actor or the unintentional coverage of extremist ideas by a journalist.[40] It could include an influencer publishing a paid-for article or video without disclosing the funding, or the purchase of false signatures on a petition.[41]

BOTS

Bots are automated social media accounts, designed to create and/or engage with content. Bot activity can be used to create the illusion of popular support for political figures or ideas, or to artificially amplify false or fringe narratives.

DISINFORMATION

Disinformation is 'false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.'[42]

DEEP FAKE

A **deep fake** is a video in which an existing image or video is replaced with someone else's likeness.

FAKE NEWS

Fake news is a term popularised by Donald Trump, who used it to describe media reports which he disliked or disagreed with. In other contexts, it refers to articles and news stories online which are promoted in such a way that they appear to be spread organically by other users and which are designed to influence readers' opinions.

INFORMATION OPERATIONS

Information operations, as defined by Facebook, are 'actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome.'

MALINFORMATION

---

[40] Gu, L., V. Kropotov & F. Yarochkin, The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public, Trend Micro (June 2017), p. 17

[41] Whitney Phillips, *The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists and Manipulators,* Data and Society Research Institute, 22nd May 2018

[42] European Commission, *A multi-dimensional approach to disinformation: Report of the independent High Level Group on fake news and online disinformation*, (Luxembourg: Publications Office of the European Union, 2018)

GLOSSARY

Malinformation is true and genuine information that is shared to cause harm, such as private or revealing information about a person or organisation.

MEME

This term was originally coined by the biologist Richard Dawkins in 1976 to describe an idea or behaviour that spreads person to person throughout a culture, evolving and changing as it does. The word now commonly refers to captioned photos or GIFs spread on messaging applications or social media networks.

MISINFORMATION

Misinformation is information that is false, but not intended to cause harm. For example, the myth that eating garlic protects one from COVID-19.

TROLLING

Trolling is the act of deliberately posting content online with the aim of causing offence or disruption. However, it has also been used to describe human-controlled accounts performing bot-like activities.

TROLL FARM

A **troll farm** is a group of individuals engaging in trolling or bot-like promotion of narratives in a coordinated fashion, such as the Russia-based Internet Research Agency which spread inflammatory content online in an attempt to interfere in the U.S. presidential election.