COI HYBRID INFLUENCE

Hybrid CoE Research Report 2

JULY 2021

Effective state practices against disinformation: Four country case studies

JEAN-BAPTISTE JEANGÈNE VILMER

Hybrid CoE

Hybrid CoE Research Report 2

Effective state practices against disinformation: Four country case studies

JEAN-BAPTISTE JEANGÈNE VILMER

Hybrid CoE Research Reports are thorough, in-depth studies providing a deep understanding of hybrid threats and phenomena relating to them. Research Reports build on an original idea and follow academic research report standards, presenting new research findings. They provide either policy-relevant recommendations or practical conclusions.

COI Hybrid Influence looks at how state and non-state actors conduct influence activities targeted at Participating States and institutions, as part of a hybrid campaign, and how hostile state actors use their influence tools in ways that attempt to sow instability, or curtail the sovereignty of other nations and the independence of institutions. The focus is on the behaviours, activities, and tools that a hostile actor can use. The goal is to equip practitioners with the tools they need to respond to and deter hybrid threats. COI HI is led by the UK.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978-952-7282-86-1
ISBN (print) 978-952-7282-87-8
ISSN 2737-0860

July 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

The responsibility for the views expressed ultimately rests with the authors.

Contents

Introduction

It is now a well-established fact that disinformation, defined as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm",[1] is a major threat for democracies. What can be done to counter it is the object of a growing subfield of research that could be called *Information Defence*, to which another broader and complementary report is devoted.[2] States, individually and collectively, as well as civil societies (understood as the aggregate of all nongovernmental organizations and institutions, including the private sector and therefore the digital platforms), have been taking many initiatives to counter disinformation in recent years. However, not all of them can be said to be effective. The present Research Report is focused on this issue of effectiveness, from the perspective of state-actors only, through the means of four country case studies.

What can states do against disinformation that actually works? Practitioners need to demonstrate that what they are doing is effective. For them, being able to say what works in a quantifiable evidence-based way would be the Holy Grail. It is easier to note the importance of effectively measuring success in countering disinformation than it is to clearly identify the criteria, however. This complexity exists for at least ten reasons that are intrinsic limits to the present study:

1. There is a great diversity of situations in which disinformation may emerge. Some countries, like the US, the UK or France, have been the target of significant foreign disinformation campaigns while others, like Canada or Sweden, are affected to a much lesser extent. However, countries which have "successfully" dealt with such campaigns cannot be assumed to be more effective than those which have not. Indeed, a lack of significant foreign disinformation campaigns may be a sign of effective mitigation or deterrence – just as it could be due to a lack of interest from potential adversaries, and it is difficult, perhaps impossible, to tell which one it is. In any case, there are at least two ways of understanding the question: on the one hand, effectiveness as an effective defence when attacked; on the other hand, as an effective deterrence or mitigation of attacks due to society's resilience. Moreover, as far as countries having been attacked are concerned, their relative success cannot be presumed to be the sole indicator of effectiveness, as one must consider the quality and vigour of the attack as well.
2. There are many actors that have a role to play in the spread and opposition of disinformation. While this Research Report focuses on the state's response, in liberal democracies the state is by definition only one of the respondents: journalists, NGOs, think tanks, academics, digital platforms and others also play an important, if not the greatest role in detecting and countering disinformation. A "successful" or "effective" response is always multifactorial, the result of combined efforts that are so intertwined that it is difficult, perhaps even impossible, to know for certain to what extent exactly the state's response contributed to it.
3. Measuring the impact of disinformation campaigns (to what extent does it really influence

[1] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, Brussels, 3 December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN, p. 18. Unless otherwise indicated, all links were last accessed on 6 July 2021.
[2] Jean-Baptiste Jeangène Vilmer, *Information Defense: Policy Measures Taken Against Foreign Information Manipulation*, Atlantic Council's DFRLab and Europe Center, July 2021.

hearts and minds and electoral votes?) is notoriously difficult for a number of reasons, including because: it depends on the attacker's intent (what are they trying to achieve?); we rarely see the entirety of the operation, only a piece of it; and the target audience's sentiment is complex and difficult to measure.[3] If measuring the impact of disinformation campaigns is difficult, then measuring the impact of countering those disinformation campaigns is logically even harder.

4. Effectiveness also depends on the ability to adapt a specific response to a specific attack, and therefore to understand who the attackers are exactly, and what their specificities, intent, motives, and so on are – which, most of the time, proves very difficult. That is why this Research Report is actor-agnostic: it is focused on measures taken to counter disinformation, wherever it originates from (from a state or non-state actor, a domestic or foreign source, etc.).
5. The perimeter of the question cannot be limited to disinformation, as it is only one of many tools in influence campaigns, often combined with other means. Attackers choose their toolset for a given campaign based on effectiveness and the relative vulnerabilities of the target. Avoiding death by a thousand cuts cannot be achieved by focusing on one or a few cuts, and countering disinformation requires a state to consider the big picture, and to understand disinformation's relation to other measures. For that reason, many of the actors mentioned in this Research Report are engaged in a whole-of-government effort to counter not only disinformation but information influence operations[4] or hybrid threats[5] in general. As it would be artificial to isolate disinformation from its ecosystem, it is all the more difficult to assess the effectiveness of countering disinformation *stricto sensu*.
6. There is no general rule, method or good practice *in abstracto*; it is always context-based, that is, in a given situation, at a certain time, and for a certain actor. In particular, effectiveness depends on a mandate. Even with a whole-of-government approach, where different teams in different ministries or agencies work towards a common goal, "effectiveness" does not mean the same thing. An intelligence service would say they were effective if they neutralized the threat, a Ministry of Foreign Affairs if they conducted the relevant diplomatic action, and the ones in charge of strengthening democratic institutions if they increased the level of trust in the institutions, improved media literacy, and so forth. To paraphrase Robert Cox,[6] effectiveness "is always *for* someone and *for* some purpose". In other words, to a certain extent, effectiveness is relative and subjective.
7. Subjectivism is also a problem for national experts because they tend to see their glass as half empty: they are aware of what is wrong in their system, and what could be done better with more money and human resources. Moreover, as bureaucratic politics theories teach us, because the various agencies and administrations are in constant competition with each other for budget shares, resources, recognition, and territory,[7] it is in the interest of their representatives to underestimate what they have in order to always request more. Some of those interviewed for this Research Report, quite critical of their own system, did not even view their country as an interesting "model". One should acknowledge that no system is perfect, but the perspective of this Research

[3] See Ben Nimmo's interesting attempt to deal with those challenges in *The Breakout Scale: Measuring the Impact of Influence Operations*, Brookings, September 2020.

[4] See European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, 18: "information influence operation refers to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation".

[5] See European Commission, *Joint framework on countering hybrid threats*, 6 April, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018: "the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare".

[6] Canadian political science scholar (1926–2018) whose famous dictum was "theory is always *for* someone and *for* some purpose". Robert Cox, 'Social Forces, States and World Orders: Beyond International Relations Theory', *Millennium*, Vol. 10, Issue 2 (1981): 128.

[7] Morton H. Halperin and Priscilla A. Clapp, with Arnold Kanter, *Bureaucratic Politics and Foreign Policy* (Washington, DC: Brookings Institution Press, 2006), 2nd Edition.

Report is to look at the glass as half full, and to focus on the interesting part of some national countermeasures as perhaps being more effective than others.

8. Subjectivism is also a challenge for the author of this Research Report, writing not only about his own country but also about three others, while not having "a view from nowhere".[8] This is a humbling exercise, and that is why each of those national sections has been previously discussed with national experts.[9]
9. There are of course national specificities: what works in Sweden, perhaps due to the fact that public trust is extremely high there, may not work in the US, where society is much more polarized. That limits the potential for the country case studies in this Research Report to be "models", as at least some of their good practices are context-based: they depend on a specific political, social or economic organization of society, and are therefore not replicable.
10. There is a consensus that disinformation is an international challenge, and that at least a part of the solution lies in international cooperation (also because, from a liberal democratic perspective, national countermeasures should be defensible internationally). Amongst the people working in national units countering disinformation interviewed for this Research Report, there is a largely shared belief that national campaigns are most effective when they are conducted in collaboration with international partners, having a shared understanding of the threat, but also a shared response. In that sense, a paper based on country case studies, highlighting what works or is interesting in four states, is inherently limited. It offers only a part – the domestic part – of a solution that also implies making those nations work together.

Keeping all of these caveats in mind, effective or successful counter-disinformation capability can be understood as being able not only to repel an attack, but also to detect, to monitor, to adapt (to the hostile activity that is constantly evolving, adapting our defences in a sword/shield dialectic), to inform senior decision-makers, and to share with our partners; to make vulnerable communities more resilient, to increase the consumption of quality independent media, to develop media literacy and critical thinking, and to strengthen the credibility of public institutions; to deter potential information attacks; and to avoid providing adversaries with fodder for influence campaigns.

To illustrate these points, this Research Report has selected four country case studies: Sweden, Canada, the United Kingdom, and France. Obviously, other cases would have been interesting, particularly the United States. But the United States is already at the centre of other works, including by Hybrid CoE. Being diverse in terms of power, geopolitical situation, and systems of government, the four selected countries offer a good sample of what liberal democracies, different in colour, shape and size, can propose to counter disinformation. Finally, this Research Report will attempt to draw some general lessons from these four cases, on what an effective state response to disinformation should involve.

[8] Thomas Nagel, *The View from Nowhere* (Oxford University Press, 1986).
[9] All unsourced information in this Research Report is from interviews with national experts, conducted in April 2021.

The Swedish standard

Sweden has not been the target of a significant/large-scale disinformation campaign of late,[10] which makes it difficult to say something about the country's ability to actually counter such attacks. Several factors could explain why Sweden has not been targeted as such. First, as one interviewee put it, "We're simply not important enough… there would have to be a situation, like a referendum on joining NATO, for us to matter". Another explanation, as far as Russian disinformation is concerned, is that there is no (sufficiently strong) pro-Russia faction to provide a domestic target population: as the Russian embassy in Denmark tweeted in July 2018, "Since there is no difference in the Russophobic approach between #DK Government and opposition, meddling in DK elections makes no sense" (thereby insinuating that, in another situation, it could have made sense).[11] Moscow could say the same of Sweden. Potential Russian attackers are also aware of the risk of a counterproductive action, as any major attack would have the consequence of pushing Sweden into the arms of NATO. However, they would definitely interfere if they saw an opportunity that was worth the risk, and they are nonetheless active, as evidenced by the confirmation that the GRU hacked Sweden's sports body.[12] Finally, the argument advanced in this Research Report is that Sweden's measures are effective in preventing or deterring such attacks.

The wake-up call for Sweden came during the Russian annexation of Crimea and the war in Donbas in 2014, and the subsequent publication of a fake letter from then Minister of Defence Peter Hultqvist in February 2015. He reacted by noting that Sweden had lost its robust ability to counter disinformation developed during the Cold War. Shortly thereafter, the 2016–2020 defence bill acknowledged that influence campaigns are a security threat for Sweden.

Sweden uses a concept of "information influence" (*informationspåverkan*), meant to refer to activities that "involve potentially harmful forms of communication orchestrated by foreign state actors or their representatives. They constitute deliberate interference in a country's internal affairs to create a climate of distrust between a state and its citizens. Information influence activities are used to further the interests of a foreign power through the exploitation of perceived vulnerabilities in society. Foreign state actors study the controversies and challenges of a society and exploit these vulnerabilities to disrupt and polarise".[13]

A bottom-up approach

The Swedish government structure is based on strong agencies and small ministries. In countering disinformation, most of the work has been done by the Swedish Civil Contingencies Agency (MSB). Since 2016, it has been tasked with identifying and countering information influence campaigns. Their notable work includes raising awareness and preventing election interference.

Much of the work on countering disinformation in Sweden comes from "below" the government, at the agency, municipality, and civil society levels, to the extent that the government is currently conducting a mapping exercise in order to know who is doing what, in an effort to develop a comprehensive understanding. The *raison d'être* of such a bottom-up approach is resilience: it gives agencies the

[10] There have been a number of incidents, involving forged documents (a fake letter from Swedish Defence Minister Peter Hultqvist in 2015, a fake *Dagens Nyheter* article in 2016), a fake Swedish Defence Minister Twitter account, and many fake images in social networks, but apparently no organized, coordinated campaign comparable to what happened in the US, the UK and France, for instance.
[11] See Twitter, https://twitter.com/RusEmbDK/status/1021688735677734912.
[12] Reuters, 'Swedish prosecutor says Russia's GRU hacked Sweden's sports body', 13 April 2021.
[13] James Pamment, Howard Nothhaft, and Alicia Fjällhed, *Countering Information Influence Activities: A Handbook for Communicators*, commissioned by the Swedish Civil Contingencies Agency (MSB), 2018, https://www.msb.se/RibData/Filer/pdf/28698.pdf, p. 11.

ability to counter foreign influence and disinformation without government support. This approach contrasts favourably with other countries (like the Czech Republic, where the effectiveness of the response is much more dependent on political will) and represents a clear strength of the Swedish approach. However, such a bottom-up approach also has its disadvantages, as it makes things more difficult when there is a need to coordinate, for instance.

An educated and interested population

From the Swedish perspective, the best way to counter disinformation – or information influence – is preventative action. Proactive measures are the most effective because the opponent is forced to work in a less permissive environment for their disinformation product. The MSB begins its work by looking at vulnerabilities within the population, deducing from this starting point the greatest Swedish disinformation vulnerabilities. These efforts allow Sweden to proactively create resilience in its society, building a psychological defence of sorts. Understood as a set of measures aimed at strengthening crisis management capabilities and resilience against hybrid threats, psychological defence has existed in one form or another in Sweden since the Second World War. The MSB integrated it as a core component of its work in 2009, but it is also a function that other units have. Starting in 2022, all of these efforts will be coordinated by a new Agency for Psychological Defence.[14] However, the focus of Sweden's psychological defence will still be built in municipalities, counties, and voluntary organizations. Regionalization is an important dimension of the Swedish approach: the MSB spends a lot of time informing, educating, training, and raising awareness in municipalities and regions, in cooperation with the Swedish Association of Local Authorities and Regions.

A cornerstone of Swedish democracy is individual engagement in different groups, for sport, culture, politics, and so on, which duly enjoy government funding. Some of them – the voluntary defence organizations – are an important part of the Swedish Total Defence approach. The general idea is that an educated and interested population promotes democracy and strengthens its resilience, particularly against disinformation. For instance, one voluntary defence organization was hired by the MSB to provide training on COVID-related disinformation and to conduct other outreach activities during autumn 2020.

The same preventative approach explains why the Swedish population is among the best educated in the world in terms of media literacy.[15] There has always been a strong focus on critical thinking, media and communication knowledge, and more recently on digital education in both schools and universities (since 2018, all primary schools have taught an introduction to computer programming, and how to distinguish between reliable and unreliable sources). The Swedish Media Council is responsible for media, information and communication issues among the population, and for training young people. As such, the MSB conducts many joint projects with them to capitalize on cooperative advantages.

Nor is the private sector overlooked. In the MSB, a staffer works closely with public relations (PR) and communications companies to raise awareness of threats in that industry regarding disinformation vulnerabilities. The MSB believes that hiring local PR firms is an easy way for influence campaign aggressors to pursue their ends. Partnerships and awareness are key in combating this vulnerability, and the MSB recently invested in rebuilding the capacity to offer direct training to PR and communications firms.

Research, training and exercises

The MSB has implemented a three-step process based on research, training and education, and exercises.

First, the MSB funds research from its crisis management fund. Since 2017, the standard figure

[14] The new agency will absorb the current competencies of the MSB on fighting information influence. It will have a team of approximately 50 people. The report that Anders Danielsson, former head of SÄPO, submitted to the Minister of Interior in May 2020 to support the creation of this agency, suggested that the new agency could have an intelligence capacity, notably by intercepting communications – which ignited a debate in Sweden because under the current law (FRA 2009), only the government, the armed forces, SÄPO and a certain section of the police are authorized to command intelligence. All of them are opposed to the possibility that the new agency could do this as well, making it very unlikely that it will.
[15] Open Society Institute in Sofia, Media Literacy Index 2021, https://osis.bg/?p=3750&lang=en.

for research financing has been approximately 1.2 million euros per year, with an additional 50,000 euros per year for short-term studies. This budget is likely to increase with the new Agency for Psychological Defence. With these funds, the MSB regularly commissions reports. In 2017, it asked Lund University's Department of Strategic Communication to produce "a manual describing the principles and methods of identifying, understanding, and countering information influence activities [...] directed primarily toward communicators working in public administration".[16] This became the now famous *Countering Information Influence Activities: A Handbook for Communicators* (2018). It was then used to conduct training sessions and organize joint workshops with Finland, which later adopted the handbook. The MSB also commissioned a report from the Institute for Strategic Dialogue, a London-based think tank, on foreign influence during the 2018 Swedish general election.[17] More recently, on April 21, 2021, the MSB published a report on *Conspiracy theories and Covid-19: the mechanisms behind a fast-growing societal challenge*, which it commissioned from Andreas Önnerfors, a professor in intellectual history at Uppsala University.[18] In December 2020, the government tasked the MSB and other agencies and authorities with monitoring and countering misinformation, disinformation and rumours about vaccinating against COVID-19.[19] Önnerfors' report, prepared in only three months, is part of this activity. The MSB publicized its release, Mikael Tofvesson appeared on national television[20] and radio,[21] and newspapers discussed it.[22] The MSB will also offer training sessions based on the report to increase awareness among the population.
The MSB also funds activities. For example, it commissioned the Swedish Defence Research Agency (FOI)[23] "to assess automated behaviour on social media, as well as to track and analyze online discussions about the 2018 elections"; and Lund University's Department of Strategic Communication "to develop counter-influence guidance and training".[24] The Agency also financed a significant amount of research regarding the Muslim Brotherhood and affiliated organizations in Sweden, Salafist movements, Iran-sponsored Shia groups, and others. In that sense, research is conceived as an operational countermeasure per se.

Second, all of this research is put to good use, first and foremost to serve as a basis for training, which is an important MSB activity. Since 2016, the Agency has trained 16,000 civil servants, with an awareness programme on information influence activities, ranging from half a day up to two days. This is customized training, adapted to the different agencies and authorities trained. In 2020, the MSB also set up a training event to counter COVID disinformation, where it trained 1,600 civil servants. On 1 March 2021, it initiated another training event, specifically to protect the vaccination work and, as of April 2021, 1,200 civil servants had received training. At the beginning of April 2021, the Agency also launched a two-hour web-based training course that anyone can take. It also has a specific, certification week-long training course on countermeasures, based on the Swedish handbook, which around 1,000 people have undertaken since the beginning of 2020. The MSB also funds training for journalists, although

[16] Cited by Alicia Fjällhed, James Pamment, and Sebastian Bay, 'A Swedish perspective on foreign election interference', in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, eds. Duncan Hollis and J. D. Ohlin (Oxford University Press, 2021), 148.
[17] Chloe Colliver, Peter Pomerantsev, Anne Applebaum, and Jonathan Birdwell, *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*, ISD/London School of Economics Institute of Global Affairs, commissioned by the MSB, 2018, https://www.isdglobal.org/isd-publications/smearing-sweden-international-influence-campaigns-in-the-2018-swedish-election/.
[18] Andreas Önnerfors, *Konspirationsteorier och covid-19: mekanismerna bakom en snabbväxande samhällsutmaning*, MSB, April 2021, https://www.msb.se/contentassets/555542e57381475cb26d6862dc7a543a/msb-studie.pdf.
[19] 'Konspirationsteorier i fokus i ny studie från MSB', MSB, 21 April 2021, https://www.msb.se/sv/aktuellt/nyheter/2021/april/konspirationsteorier-i-fokus-i-ny-studie-fran-msb/.
[20] 'Konspirationer om corona: Så synar du bluffen', TV4, 21 April 2021, https://www.tv4.se/artikel/11jKKTePxOZCLNvh8jTF5C/sa-genomskadar-du-en-konspirationsteori.
[21] 'Konspirationsteorier i pandemin', Sveriges Radio, 23 April 2021, https://sverigesradio.se/artikel/konspirationsteorier-i-pandemin.
[22] See for instance 'MSB: Konspirationsteorier vilseleder opinionen om vaccineringen', *Dagens Nyheter*, 21 April 2021.
[23] Funded mostly (75%) by the armed forces but also by other agencies, FOI is another important contributor to counter-disinformation efforts in Sweden. For example, the FOI data science group, under the leadership of Lisa Kaati, is mapping the digital landscape, looking at digital extremism and some related issues, and has produced quite a number of reports in the last few years. Sebastian Bay, from the Department of Asymmetric Threats, is another expert on disinformation, currently spending most of his time on a project (run by the election authority and partially funded by the MSB) to safeguard the 2022 elections.
[24] Fjällhed, Pamment, and Bay, 'A Swedish perspective on foreign election interference', 147.

this is conducted through an intermediary, the Fojo Media Institute, to protect the freedom of the press.[25]

Finally, the MSB has been organizing a yearly training event since 2015 as part of the strategic national intelligence course conducted by the National Defence University, gathering together top-level civil servants (heads of sections or departments at agencies and authorities) and training them on hybrid threats and disinformation, including exercises that they have to coordinate themselves. The training ends with the participation of a couple of ministers, who interview the students on their lessons learned.

To sum up, the MSB's approach is three-tiered: at the first level, it visits agencies and authorities and tells them about the threats; at the second level, it organizes preventative training; and at the third level, it arranges specific training on countermeasures where everyone prepares to fight together. The training starts with threats, even though it would make more sense to start with vulnerabilities, but this is done for pedagogical reasons, namely because the Agency found that people were more motivated when they knew what the threat was.

A rights-based approach

The MSB does not scrutinize its own population, as it is legally prohibited from registering Swedish citizens in its database. Rather than monitoring the Swedish social media, it focuses on foreign-based emitters of disinformation. The Agency is familiar with the emitters' infrastructure – their channels – and they listen to what they are saying. However, the MSB also realized that there was a need to know what was going on in their own information environment, whether or not they could scrutinize their population directly. Therefore, in spring 2021, the Agency set up a new mini-cell that works to identify disinformation domestically (in the sense of the Swedish information space, which goes beyond the geographical borders). For example, the MSB tries to identify the major narratives connected to COVID-19 and vaccination, and produces a weekly report in which all indications about the sender, the author of an article, or the person behind a social media account are removed, and all data anonymized. This report, about the narratives only, is sent to all government agencies and authorities at local, regional and central levels so they can adapt, focus their communication, increase awareness, and foster resilience. Additionally, this "domestic" team is not allowed to work together with the other, foreign interference team. It is compartmentalized because, as one MSB manager put it, "We have to be clear and transparent to our population and to parliament that we don't use the same methods on our population and on foreign actors."[26]

From transparency to deterrence

Another Swedish strength is that they often share details of what they do. Even intelligence and security agencies like the Swedish Security Service (SÄPO), the Military Intelligence and Security Service (MUST), and the National Defence Radio Establishment (FRA) publish annual reports giving detailed accounts of their activities and of their threat assessment. These reports regularly mention the risks posed by disinformation and hybrid or "non-linear" threats in general. Occasionally, they also publish joint reports.

As we have seen with the example of its April 2021 report on conspiracy theories, when the MSB releases a report, it often promotes it publicly. Mikael Tofvesson regularly intervenes in the media. In general, the MSB has a global communication strategy, its goal being to reach the whole population, including the less connected. The Agency also sends text messages (to all Swedish mobile phone numbers during the pandemic), and has resorted to "physical" means like the brochure *If War or Crisis Comes*, mailed to 4.8 million households in 2018, as well as posters in the underground or in the streets in several languages.

All of this activity is not only about raising awareness. It is also about signalling to potential adversaries that Swedish society possesses a high degree of preparedness and determination. Publishing many reports, national strategies,

[25] See FOJO:Media Institute, https://fojo.se/en/.
[26] Interview with an MSB manager, April 2021.

interviews and op-eds (like the one titled "How we will protect the election from foreign state influence" by the Swedish PM in March 2017)[27] is actually a "part of the Swedish counterstrategy – an example of deterrence", the objective of which is "to deter actors from contemplating interference in the Swedish elections",[28] but also more generally in the democratic life of the country.

Going international

The MSB's approach is actor-specific. It has an obvious focus on Russia, for example. China is increasingly monitored as well, considering the high level of Chinese influence activities in Sweden. Iran has always been a problem for counter-intelligence (not because Tehran is interested in Sweden, but because of the Iranian diaspora living there); and the MSB has focused quite heavily on Islamic extremism. The priorities flow directly from Swedish national security directives. At the same time, the MSB is also actor-agnostic, both because its focus is on building resilience (which is a strong cultural specificity: "we like building resilience more than anything else"[29]), and because it develops 360° surveillance, including of non-state actors. For example, QAnon-inspired movements became a target as soon as they tried to influence the Swedish population. In this worldwide monitoring, the Agency works very closely with the Swedish Institute, an agency under the Ministry of Foreign Affairs (MFA), responsible for promoting Sweden abroad. Since 2020, the Swedish Institute has been given the specific task of monitoring disinformation and narratives against Sweden or harming Sweden's image abroad. The MFA itself is another relevant actor with its Communications Department and, since 2018, a new unit and the creation of an ambassador and special envoy for hybrid threats.[30]

Aware that the level of foreign-originated disinformation in Sweden is fairly low compared to other European states (Baltic and Central European ones in particular), MSB personnel spend a lot of time abroad, learning from the experiences of others. Sweden is particularly close to the UK in many areas, and that is true also in this field: for example, James Pamment, the author of the Swedish handbook from Lund University, is also the author of the RESIST British handbook.[31] The EU is also considered a cornerstone in the Swedish fight against global disinformation: the MSB has two experts at the European External Action Service (EEAS), one in the East StratCom Task Force, and the other in the Western Balkan StratCom Task Force. They also have an expert at the NATO Centre of Excellence in Riga. In a spirit of division of labour, it is the National Defence College and the MFA that handle the relationship with Hybrid CoE in Helsinki. The MSB's relationship with the US, Australia, and Singapore is also excellent. The latter in particular is a focus for cooperation as there are many similarities between the two nations (not only because Singapore has also adopted the Total Defence approach, but also in its aim to learn best practices from all over the world). In general, international cooperation is a priority, and it is stressed as such in the new Agency's directives.

Overall, Alicia Fjällhed, James Pamment, and Sebastian Bay have usefully summarized the main lines of the Swedish approach: "1. Conduct comprehensive risk and vulnerability assessments; 2. Focus on resilience-building based on the risk and vulnerability assessments; 3. Consider deterrence factors; 4. Establish comprehensive and effective coordination and cooperation mechanisms; 5. Establish and test early warning and detection mechanisms; 6. Conduct education and training for relevant actors; and 7. Conduct strategic communication to deter antagonists."[32]

[27] Cited by Fjällhed, Pamment, and Bay, 'A Swedish perspective on foreign election interference', 145.
[28] Ibid., 151.
[29] Interview with an MSB manager, April 2021.
[30] Fredrik Löjdquist, 'An Ambassador for Countering Hybrid Threats', RUSI Commentary, 6 September 2019, https://rusi.org/explore-our-research/publications/commentary/an-ambassador-for-countering-hybrid-threats-. In 2021, Fredrik Löjdquist was appointed Head of the Stockholm Centre for Eastern European Studies (SCEEUS); at the time of writing, the seat of the Hybrid Ambassador is still vacant.
[31] UK Government Communication Services, 'RESIST Counter Disinformation Toolkit', https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/.
[32] Fjällhed, Pamment, and Bay, 'A Swedish perspective on foreign election interference', 158.

The Canadian preparedness

Like Sweden, Canada has not yet been a primary target of foreign state-sponsored information manipulation. Canada also relies on its existing resilience, including an extant high level of confidence in mainstream media and institutions (much higher than in the US).[33] However, the Canadian authorities know that this resilience cannot be taken for granted, so they prepare in anticipation of being targetted at some point. They are also closely monitoring the UK and Australian models. The 2016 Brexit campaign and the US presidential election served as a wake-up call for the Canadian authorities, and the 2017 election interference in France reinforced Ottawa's growing awareness, particularly on the election front.

Protecting elections: the example of the 2019 federal election

Considering that Canada's 2015 federal election was targeted by "low-sophistication cyber threat activity",[34] and that several more significant cases of electoral interference happened in the United States (2016) and France (2017), Canada prepared accordingly to protect its democratic process and to prevent the risk of foreign interference during the 2019 federal election. On the one hand, the intelligence and security apparatus was reinforced in 2018 with a National Cyber Security Strategy published in June[35] and the creation of a Canadian Centre for Cyber Security in October, with a budget of CAD$155 million over five years.[36] On the other hand, the Ministry of Democratic Institutions was tasked with preparing a "Plan to Safeguard Canada's 2019 Election". To avoid perceptions of politicization, the Ministry involved all federal political parties in the process. The Plan was made public on 30 January, 2019,[37] and includes four pillars:

1) Enhancing citizen preparedness,[38] with the implementation of a Critical Election Incident Public Protocol[39] according to which, if national security agencies became aware of election interference, they would brief a "Panel of Five" composed of the most senior civil servants[40] (their function is apolitical, again to avoid suspicions of politicization). The Panel would duly evaluate the threat and, if they found that Canada's ability to conduct a free and fair election had been jeopardized, they would inform the prime minister, political party officials, and Elections Canada. All Canadians would then be informed by a public announcement. Additionally, the government established a Digital Citizen Initiative, dedicating CAD$7 million "to support digital, news and civic literacy programming… skills development, awareness sessions, workshops and learning material".[41] It also invested CAD$19.4 million

[33] See Shelley Boulianne, Stephanie Belland, Chris Tenove, & Helsey Friesen, *Misinformation: Across Social Media Platforms and Across Countries*, a study funded by the Government of Canada, March 2021, https://roam.macewan.ca/islandora/object/gm:2822, p. 6: "Canada is grouped with countries with higher resilience because of its media regulation and publicly funded broadcasting system".

[34] Government of Canada, Democratic Institutions, 'Protecting Canada's democracy from cyber threats', 16 June 2017, https://www.canada.ca/en/democratic-institutions/news/2017/06/protecting_canadasdemocracyfromcyberthreats.html.

[35] Government of Canada, Public Safety Canada, 'National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age', 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

[36] Julie Dzerowicz, Member of Parliament for Davenport, 'Question to Prime Minister Justin Trudeau about Cyber Security', 3 October 2018, https://juliedzerowicz.libparl.ca/question-to-prime-minister-justin-trudeau-about-justin-trudeau-about-cyber-security/.

[37] Government of Canada, Democratic Institutions, 'The Government of Canada's Plan to Safeguard Canada's 2019 Election', 30 January 2019, https://www.canada.ca/en/democratic-institutions/news/2019/03/speech-thegovernment-of-canadas-plan-to-safeguard-canadas-2019-election.html.

[38] Government of Canada, Democratic Institutions, 'Enhancing citizen preparedness', https://www.canada.ca/en/democratic-institutions/news/2019/01/enhancing-citizen-preparedness.html.

[39] Government of Canada, Democratic Institutions, 'The Critical Election Incident Public Protocol', https://www.canada.ca/en/democratic-institutions/news/2020/10/the-critical-election-incident-public-protocol.html.

[40] Composed of the Clerk of the Privy Council; the National Security and Intelligence Advisor to the Prime Minister; the Deputy Minister of Justice and Deputy Attorney General; the Deputy Minister of Public Safety; and the Deputy Minister of Foreign Affairs.

[41] Government of Canada, Democratic Institutions, 'Enhancing citizen preparedness'.

over four years in a Digital Citizen Research Program led by Canadian Heritage, and accelerated a national public awareness campaign to inform the population about cyber security ("Get Cyber Safe"). Canadian Heritage also funded the training of approximately 70 journalists on disinformation and digital literacy for a couple of days: as in Sweden, and for the same reasons (a rights-based approach, attentive to protecting press freedom), they were not trained by government officials but by an academic intermediary, McGill University's Media Ecosystem Observatory.[42]

2) Improving organizational readiness,[43] by providing technical advice for political parties and election administrators on how to better protect their cyber installations, sensitizing decision-makers to the risk of foreign interference, providing classified briefings for political party leaders, and organizing whole-of-government simulations and tabletop exercises on a regular basis to prepare for potential incidents or scenarios.

3) Combatting foreign interference,[44] by creating a Security and Intelligence Threats to Elections (SITE) Task Force composed of the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), the Communications Security Establishment (CSE), and Global Affairs Canada (GAC). The task force's mission is to build awareness of foreign threats to Canada's electoral process and to prepare the government to assess and respond to those threats. It also benefits from feedback from other countries, including through the G7 Rapid Response Mechanism created in summer 2018. Additionally, on the legal side, these efforts can rely on the *Elections Modernization Act* (Bill C-76, December 2018, which entered into force in June 2019) prohibiting "false statements" regarding a candidate, prospective candidate, party leader, or prominent figure associated with a party; prohibiting the use of foreign funds for partisan advertising or activities; and requiring that large digital platforms publish a public registry of their partisan advertising published during the pre-election period, and all election advertising during the election period.

4) Expecting social media platforms to act:[45] the Canada Declaration on Electoral Integrity Online, resulting from discussions between the Ministry of Democratic Institutions and social media companies, expects those platforms to take a number of concrete measures in terms of integrity, transparency and authenticity.[46]

In terms of whether this highly comprehensive Plan has been effective, the 2019 federal election went smoothly, without any major incident. Even a golden opportunity like the "blackface" controversy[47] was not fully exploited. The most significant disinformation effort was made by the American *Buffalo Chronicle*, which attempted to undermine PM Trudeau's credibility.[48] In general, a particular threat in Canada is the porosity of the "border" (since there is none in the informational space) between Canada and the US: the American information space bleeds over significantly into the Canadian one.[49] This sometimes makes it difficult to disentangle the domestic from the foreign,[50] as these efforts receive local support from small

[42] See Media Ecosystem Observatory, https://mediaecosystemobservatory.com/.
[43] Government of Canada, Democratic Institutions, 'Improving organizational readiness', https://www.canada.ca/en/democratic-institutions/news/2019/01/improving-organizational-readiness.html.
[44] Government of Canada, Democratic Institutions, 'Combating foreign interference', https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html.
[45] Government of Canada, Democratic Institutions, 'Expecting social media platforms to act', https://www.canada.ca/en/democratic-institutions/news/2019/01/encouraging-social-media-platforms-to-act.html.
[46] Government of Canada, Democratic Institutions, 'Canada Declaration on Electoral Integrity Online', https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html.
[47] Following the publication by *Time Magazine* of a picture of PM Justin Trudeau wearing brownface makeup at a party in 2001. See https://time.com/5680759/justin-trudeau-brownface-photo/.
[48] Jane Lytvynenko, Marco Chown Oved, and Craig Silverman, 'The Canadian Election's Surprise Influencer Is A Buffalo Man Targeting Canadians With Viral Disinformation', BuzzFeed News, 18 October 2019, https://www.buzzfeednews.com/article/janelytvynenko/matthew-ricchiazzi-buffalo-chronicle-trudeau-claims.
[49] Aengus Bridgman et al., 'Infodemic Pathways: Evaluating the Role That Traditional and Social Media Play in Cross-National Information Transfer', Frontiers in Political Science, 29 March 2021, https://internal-journal.frontiersin.org/articles/10.3389/fpos.2021.648646/full; McGill University 'Americans are super-spreaders of COVID-19 misinformation', Newsroom, 6 April 2021, https://www.mcgill.ca/newsroom/channels/news/americans-are-super-spreaders-covid-19-misinformation-330229.
[50] To the point that an argument could be made that this is a false distinction. If the far right in the US communicates with the far right in Canada, is that foreign influence? Or has the digital space created a broader influence marketplace in which domestic actors freely partake?

alt-right Canadian movements: there are a fair number of Canadians who have political views that are aligned with those of former President Trump and his political base. This resonance creates a market of willing consumers when it comes to the disinformation and conspiracy theories that exist in these ecosystems. In this sense, the fact that the *Buffalo Chronicle* is an American outlet is secondary: there are other domestic alternative/disinformation media outlets that resonate with the MAGA ecosystems, which also published stories similar to the topic of the PM's past actions. In any case, these disinformation efforts did not reach the threshold of jeopardizing a free and fair election.

The 2019 election was a success, although it is impossible to know whether this was a result of a successfully executed plan or due to disinterest on the part of potential attackers (making this a good illustration of the methodological difficulties mentioned in the introduction). Not knowing makes it more difficult to adapt and prepare for the next election, which is all the more problematic as, in the Westminster system shared by Canada and several other countries, the next election could come at short notice. What is certain, however, is that the instruments deployed by the Canadian government to protect its democratic process can only help, and they constitute an interesting model.

They are not perfect, however, and one of the issues that emerged from the 2019 experience is that attacks could remain under the threshold of compromising the election, and therefore activating the Critical Election Incident Public Protocol. The Government of Canada's *Guidelines on the conduct of Ministers, Ministers of State, exempt staff and public servants during an election* outline the "caretaker convention" observed during the election period. Under this convention, the government acts with restraint during an election period, including with respect to communciations. Senior civil servants must make careful decisions with regard to any public communications but are permitted to do so if they relate to: a significant international or domestic event where the failure to have the prime minister or a minister comment would damage Canadian interests or prestige; announcements relating to the health and safety of Canadians; and public notices for legal purposes.

Foreign affairs at the centre of a network

Global Affairs Canada (GAC), the Canadian Ministry of Foreign Affairs, hosts the Centre for International Digital Policy (CIDP), which has two teams: the Rapid Response Mechanism Unit (RRM Canada) and the Digital Inclusion Lab (DIL). DIL examines the intersection of foreign policy and digital technology more broadly: all things related to platforms, content moderation, artificial intelligence, digital inclusion, and so forth.

The mandate of RRM Canada has three components: 1) lead the G7 Rapid Response Mechanism (G7 RRM) established in 2018 to counter foreign threats to democracy, including disinformation; 2) work with international partners, including governments, civil society, academia and industry to counter foreign state sponsored disinformation; and 3) monitor the digital information ecosystem for foreign state sponsored disinformation related to Government of Canada priorities. Leading the G7 RRM includes convening monthly G7 meetings to discuss both threats and best practices, organizing analytical exchanges and ensuring real-time information sharing. It also entails coordinating an "RRM Canada Table" to ensure that whole-of-government approaches are reflected in international engagements and that lessons learned from G7 partners are shared across the Canadian government. Meanwhile, monitoring the digital information ecosystem includes building in-house tools to collect and analyze data.

RRM Canada provides situational awareness for decision-makers on how foreign policy narratives and potential foreign interference evolve in the digital media ecosystem. Being hosted at GAC, RRM Canada is by definition focused on foreign state sponsored information manipulation; the team leverages its expertise in the context of federal elections, where it is part of the whole-of-government effort, participating in safeguarding the integrity of the election. In general, but especially during the election period, the team works very closely with the intelligence community through SITE to flag indicators of potential foreign information manipulation attempts.

Other relevant state actors contributing to countering disinformation are the intelligence services (CSIS, CSE), Canadian Heritage (promoting the resilience of the population to disinformation, and implementing the Digital Citizen Initiative), Elections Canada (the agency responsible for Canadian federal elections and referendums, having their own monitoring capabilities), the Commissioner of Canada Elections (the independent officer responsible for ensuring compliance with and enforcement of the *Canada Elections Act*); and, especially since 2020, the Public Health Agency, which has been scrutinizing COVID-related disinformation. Last but not least, the Privy Council Office (PCO, supporting the PM and the Cabinet) has a democratic institutions secretariat (previously, between 2003 and 2019, there was a Minister of Democratic Institutions). This secretariat has a specific mandate to work with domestic and international partners to strengthen Canada's whole-of-society preparedness, resilience and civic engagement in the face of evolving threats to democracy, as well as to conduct research and policy development on online disinformation in Canada, and lead an international initiative aimed at building consensus and developing guiding principles on how to strengthen citizen resilience to online disinformation.[51] Obviously, the fact that this has not been a huge issue in Canada up to now means that there is no pressing need to improve a system that already works well.

An open, civil-society-oriented approach

Like Sweden and the UK, Canada demonstrates a high level of transparency and openness in its efforts to counter disinformation. Public institutions and agencies, including intelligence services, regularly release public reports to raise awareness. Notable examples are *Who Said What? The Security Challenges of Modern Disinformation* (Canadian Security Intelligence Service, CSIS, February 2018) and *Cyber Threats to Canada's Democratic Process* (Communications Security Establishment, CSE, updated yearly since 2017).[52]
Canada is also very much open to external expertise, including at the highest political level: in August 2018, as the prime minister was holding a cabinet retreat in Nanaimo, British Columbia, they invited three experts – Taylor Owen (Canada), Ben Scott (United States), and myself (France) – to brief the entire cabinet, the PM and about 40 ministers and deputy ministers, on countering disinformation, for an hour. We also had additional time with PCO members, including the national security and intelligence advisor to the PM. This unique experience, which would have been highly unlikely in many other countries, illustrates the accessibility and openness to research of the Canadian government.

There are also a number of initiatives to support civil society, as already mentioned in the specific case of preparing for the 2019 election. An additional example is the fact that, in February 2018, the Canadian government pledged CAD$50 million over a five-year period to support local journalism, in an attempt to reduce the influence of untrustworthy sources of information within certain communities[53] – an important and perhaps unprecedented effort, not only by Canadian standards, but also internationally.

Finally, it should also be noted that the Canadian government maintains a productive relationship with social media platforms, as the cooperation ahead of the 2019 election showed. The Ministry of Democratic Institutions was in charge of the relationship with Facebook Canada which, in response to the CSE's previously mentioned report, launched a Canadian Election Integrity Initiative in 2017, including a two-year partnership with MediaSmarts (Canada's Center for Digital and Media Literacy), the publication of a *Cyber Hygiene Guide* for politicians and political parties;[54] the creation of a Cyber Hygiene training session open to all federal political parties, and the creation of a special email to reach Facebook quickly in the event of a crisis.

[51] See President of the Queen's Privy Council for Canada Mandate Letter, 13 December 2019: https://pm.gc.ca/en/mandate-letters/2019/12/13/president-queens-privy-council-canada-mandate-letter.
[52] See also CSIS, *Public Report 2020*, https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report.html; and National Security and Intelligence Committee of Parliamentarians, *Annual Report 2020*, https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_en.pdf.
[53] Karen K. Ho and Mathew Ingram, 'Canada pledges $50 million to local journalism. Will it help?', *Columbia Journalism Review*, 28 February 2018, https://www.cjr.org/business_of_news/canada-journalism-fund-torstar-postmedia.php.
[54] Facebook, *Cyber Hygiene Guide: Politicians and Political Parties*, https://facebookcanadianelectionintegrityinitiative.com/files/Cyber-Hygiene-Report-en-ca.pdf.

The British productivity

A formidable network of pockets of expertise

One of the UK's strengths is the number of pockets of expertise it has with many teams across departments involved in the collective effort to counter disinformation. The most well-known are the following:

- The National Security Communications Team (NSCT) under the joint authority of the Cabinet Office and the Prime Minister's Office (No. 10). It was "significantly expand[ed]"[55] after the Salisbury attack in 2018. Its purpose is "to allow government to tackle more effectively the communications elements of complex, interconnected challenges to our national security, including (but not limited to) disinformation".[56] One of its notable public realizations is the "SHARE Checklist" (now a DCMS lead), which provides the public with five easy steps to identify false content, encouraging users to stop and think before they share content online and to be careful not to contribute to spreading disinformation.[57]
- The Rapid Response Unit (RRU), created in April 2018, also part of the Government Communications Service (GCS) and based in No. 10 and the Cabinet Office. Its role is to "scour the web for disinformation to help government departments counter it or push for removal".[58] In 2018, it comprised "specialists including analyst-editors, data scientists, media and digital experts".[59] When, after the 2018 strikes in Syria, disinformation was spread online and dominated the Google search results as no government-sourced information was present in the first 15 pages, the RRU reacted and "improved the ranking from below 200 to number 1 within a matter of hours".[60] In general, the RRU examines the kind of conversation that is trending online. It does not focus specifically on disinformation, but it would be in a position to capture disinformation gaining popularity online.
- The Media Monitoring Unit (MMU), also based in No. 10/Cabinet Office, producing "daily social media briefings relating to specific topics and monitoring reports on traditional media".[61]
- The Open-Source Unit (OSU), created in 2016, based in the Foreign, Commonwealth & Development Office (FCDO). Mixing data science, behavioural science and open-source intelligence methods, its mission is to improve how the FCDO better leverages open source data. It provides "open source monitoring and assessment of international social media and other open source material".[62]
- The Russia Unit, also in the FCDO, implements a £29.75 million Counter Disinformation and Media Development (CDMD) programme, launched in April 2016. Its goal is to protect UK national security by reducing the harm to democracy and the rules-based international order caused by Russia's information operations. The programme adopts a comprehensive, whole of society approach to reduce citizens' vulnerabilities, increase resilience in the information environment and deliver a strong response to

[55] UK Government, 'National Security Capability Review, March 2018', https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf, p. 34.
[56] UK Parliament, 'Mass Media: Standards: Written question – 134225', 26 March 2018, https://perma.cc/RNL4-FQWE.
[57] SHARE for Source, Headline, Analyse, Retouched, Error. See https://sharechecklist.gov.uk/.
[58] Emilio Casalicchio, 'UK gears up for coronavirus anti-vax battle', *Politico*, 16 November 2020, https://www.politico.eu/article/uk-gears-up-anti-vax-battle/.
[59] UK Government Communication Service, 'Alex Aiken introduces the Rapid Response Unit', 19 July 2018, https://perma.cc/837J-UF2U.
[60] Ibid.
[61] UK Government Communication Services, 'RESIST Counter Disinformation Toolkit'.
[62] Ibid.

Russian information operations. This is achieved through a range of international projects, which support the collection of open-source information and the development of independent media in vulnerable countries. The CDMD programme supports the transfer of knowledge and capabilities to inform the UK's domestic response, thus increasing government expertise and ensuring greater coordination and integration between its domestic and international efforts. The Russia Unit also operates within a strategic communications framework to build support for cooperation, increase the resilience of audiences, and increase the costs for hostile states of conducting malign activity.

Obviously, coordination is a challenge with so many different units across the government working on parts of the picture. It also poses a significant challenge in the United States for the same reason.[63] The United Kingdom seems to perform well in this respect, however, and the coordination does not seem to be a problem thanks to well-defined roles and good internal communication.

Like Sweden, the UK combines actor-agnostic and actor-specific approaches. At the initial level of investigation, these teams do not necessarily know the origin of the threat or any particular link to a state actor. The domestic response is based on harm, whatever its origin, and some of those teams, like the cross-departmental unit created to coordinate the fight against COVID-related disinformation (see below), are by definition not actor-focused. On the other hand, others are by definition actor-specific, like the Russia Unit. This is why the FCDO plays a significant role in the British approach. Moreover, historically, the UK's awareness has been actor-specific, mostly linked to Russia because of a number of incidents (including Litvinenko's assassination, Perepilichnyy's death, the annexation of Crimea and the war in Donbas, and the attempted assassination of the Skripals).

The example of countering COVID-related disinformation

A good example of how this network can be put to good use and complemented with ad hoc measures can be found in the UK's government reaction to false and misleading narratives about the coronavirus. The RRU quickly identified and countered "up to 70 incidents a week".[64] For example, the unit was "monitoring false claims such as that children will be vaccinated without parental consent; that the army will force people to take a vaccine; that people taking part in a vaccine trial died; and a claim pushed by Russia that the vaccine could turn people into chimpanzees".[65] The first reaction was to spread public health information and to work with social media platforms and search engines to limit the diffusion of inaccurate COVID-related news. The government also relaunched its "Don't Feed the Beast" public campaign, and created an additional unit – a cross-departmental counter-disinformation unit (CDU), housed in the Department for Digital, Culture, Media and Sport (DCMS) and set up in March 2020 "to provide a comprehensive picture of the extent, scope and the reach of disinformation and misinformation linked to COVID-19, and to work with partners to stamp it out".[66] The unit covers at least two different key functions: on the one hand, monitoring analysis (its function is to ensure – based on the analysis that the previously mentioned teams are producing – that the DCMS unit can produce a single version of the analytical trends). On the other hand, it is also in charge of engagement with social media platforms, which is a particular strength of the UK's approach in the sense that the DCMS has developed relationships over the past couple of years with these platforms. In particular, it developed a "trusted flagger" status with all the main social media platforms. This includes flagging content that violates terms of service. The unit works closely with social media platforms to help them identify and take action to

[63] See Vilmer, *Information Defense*.
[64] UK Government, 'Government cracks down on spread of false coronavirus information online', 30 March 2020, https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online. On the role of RRU, see Subhajit Banerjee, 'How we are fighting the spread of false coronavirus information online', UK Government Communication Service, 16 April 2020, https://gcs.civilservice.gov.uk/blog/how-we-are-fighting-the-spread-of-false-coronavirus-information-online.
[65] Casalicchio, 'UK gears up for coronavirus anti-vax battle'.
[66] UK Parliament, 'Internet: Disinformation', question for DCMS, UIN 124329, 2 December 2020, https://questions-statements.parliament.uk/written-questions/detail/2020-12-02/124329.

remove incorrect claims about the coronavirus, in line with their terms and conditions. Apart from this day-to-day engagement with the platform, there is also longer-term strategic engagement.

This DCMS unit has been working closely with the Communications team of the Department of Health and Social Care on vaccine campaigns to promote information and advice and increase uptake, particularly amongst certain groups within the population. They have regular meetings and share insights on narratives that we have seen emerging which may drive hesitancy that might affect vulnerable groups in particular.

A particular challenge that is worth mentioning is the increasing amount of offline disinformation: groups distributing leaflets publicly or targeting venues such as schools with false or misleading claims about the vaccine. The problem is that it does not fall under the specific remit of the DCMS as they focus on online disinformation. Therefore, working closely with the Department of Health and Social Care, the UK Vaccine Security working group has been set up across business and health departments to look into all physical/offline threats to vaccine deployment. The cooperation between the DCMS (online) and the DHSC UK Vaccine Security group (offline) is also a good example of the British adaptability.

Among other actors reported to be playing a role in countering COVID-related disinformation, the intelligence organization Government Communications Headquarters (GCHQ) has been tasked with "disrupt[ing] anti-vaccine propaganda being spread by hostile states […]. The spy agency is using a toolkit developed to tackle disinformation and recruitment material peddled by Islamic State",[67] according to *The Times* newspaper. Another actor is Ofcom, the UK's communications regulator, which provides a range of information, including weekly and then monthly surveys showing "how people are receiving and acting on information during the current pandemic, including which sources they trust most".[68]

Additionally, in December 2020, the DCMS established a Counter-Disinformation Policy Forum, bringing together social media platforms, experts from civil society organizations and academia[69] to consider the best way to share information within the COVID context: participants are asked "to share insights and data on the issues identified on an ongoing basis". In particular, platforms are expected to "provide as much detail as they are able". They meet approximately every six weeks. Based on this experience, the DCMS is currently working on a draft framework about the different kinds of intervention that we can make in the information environment, from policy changes to content moderation, fact-checking labels, and so forth. At the moment, this policy forum is limited to COVID-19 disinformation, but the objective is to use this experience to improve the long-term organization. One of the thoughts in the Full Response to Online Harms White Paper[70] was that the regulator could establish an expert working group. In advance of that, there could be ways to have a longer-term version of the counter-disinformation policy forum – a completely different version of it, because how you operate in a crisis differs from how you operate in "peacetime".

The UK also acted on the international front, pushing for COVID-related disinformation to be a priority within both the G7 and NATO, even deploying two British Army experts in countering disinformation to advise and support NATO in the international fight against COVID-19, "in ensuring its citizens have the right information to protect themselves and its democracies are protected from malicious disinformation operations used by adversaries", explained the UK Secretary of State for Defence Ben Wallace in April 2020.[71] Furthermore, over the last year, the FCDO's CDMD programme also provided support for independent

[67] Lucy Fisher and Chris Smyth, 'GCHQ in cyberwar on anti-vaccine propaganda', *The Times*, 9 November 2020, https://www.thetimes.co.uk/article/gchq-in-cyberwar-on-anti-vaccine-propaganda-mcjgjhmb2.
[68] See Ofcom, 'Combatting Covid-19 misinformation', https://www.ofcom.org.uk/research-and-data/media-literacy-research/coronavirus-resources.
[69] UK Parliament, 'Supplementary written evidence submitted by Sarah Connolly, Director Security and Online Harms, Department for Digital, Culture, Media and Sport', 12 January 2021, https://committees.parliament.uk/writtenevidence/21305/html.
[70] UK Government, 'Online Harms White Paper: Full government response to the consultation', 15 December 2020, https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response; OfCom, 'Covid-19 news and information: consumption and attitudes', 27 April 2021, https://www.ofcom.org.uk/research-and-data/tv-radio-and-on-demand/news-media/coronavirus-news-consumption-attitudes-behaviour.
[71] UK Government, 'Army experts boost NATO fight against COVID-19 disinformation', 15 April 2020, https://www.gov.uk/government/news/army-experts-boost-nato-fight-against-covid-19-disinformation.

media outlets in countering disinformation about the response to the COVID-19 pandemic.

Overall, the measures taken against COVID-related disinformation seem to have been effective, if one believes surveys finding a reduction in exposure to mis/disinformation, as well as vaccine hesitancy. It certainly contributed to the UK's speedy COVID-19 vaccine rollout.

A rights-based approach

Like others in this Research Report, particularly Sweden and Canada, the UK has adopted an approach that is quite attentive to respect for democratic values, especially freedom of expression. That is why the goal is to respond to mis/disinformation while focusing on harm. In the context of COVID-19, the specific aim is to look at mis/disinformation, narratives or content that could pose a risk to public health, public order or safety, or to minority or vulnerable groups. For example, regarding the public debate on the use of so-called vaccine passports or certification, which is a political issue, it is deemed inappropriate for the government to attempt to influence it, so intervention is limited to false claims with a potential for harm.

The French light footprint

The 2017 experience

The wake-up call for France was the so-called "Macron Leaks" operation, a coordinated attempt to undermine Emmanuel Macron's candidacy during the 2017 French presidential election, involving a disinformation campaign and a hack-and-leak operation two days before the final round of voting. It failed for a number of reasons, detailed in a previous report.[72] This case represents another example of the difficulty, mentioned in the introduction, in distinguishing between an effective response and an ineffective attack. Indeed, some of the reasons why the attempt failed were contextual (France's political and media environment), others were due to the attack's flaws (the attackers were sloppy and made a number of mistakes), but a part of the success was also due to appropriate measures taken by both governmental and non-governmental actors. In such a multifactoral situation, it is obviously difficult, perhaps impossible, to assess the weight of the state reaction alone. The summary below will try to examine what can be said about the state response.

First, the French authorities anticipated the threat. France benefited from knowing about previous election cyberattacks and disinformation campaigns, most notably the 2016 US presidential campaign. Paris benefited from the mistakes it witnessed during the campaign: the disdain for and neglect of the threat of disinformation campaigns, a reluctance to address and frame the hacking of the Democratic National Committee (DNC), and a delayed response by the government. It also benefited from operational cooperation with the US authorities (intelligence sharing). At the end of summer 2016, the Secretariat-General for National Defence and Security (SGDSN), a cross-departmental organ under the French Prime Minister, and the National Cybersecurity Agency (ANSSI), alerted the political parties and candidates to the risk of cyberattacks and disinformation during the presidential campaign. On October 26, 2016, ANSSI organized a workshop on cybersecurity, open to all political parties represented in the French and European parliaments. Its aim was to draw lessons from the 2016 American presidential election, to evaluate the risks in the context of the 2017 French presidential election, and to highlight good practices.[73] During the campaign, in early February 2017, ANSSI visited the Macron campaign headquarters to warn about the risks.

From the start of the electoral campaign, the government also signalled – both publicly in a number of speeches and through a more discreet, diplomatic channel – its determination to prevent, detect and, if necessary, respond to foreign interference. For instance, in January 2017, the French defence minister, aware that the presidential campaign was under attack, declared that "France reserves the right to retaliate by any means it deems appropriate. This could be through our cyber arsenal but also by conventional armed means".[74] A similar message was conveyed privately by the minister to his Russian counterpart and by President Hollande to President Putin. US Senate Democrats, drawing lessons from the French elections in their January 2018 report for the Foreign Relations Committee, concluded that "direct diplomatic engagement clearly pointing

[72] Jean-Baptiste Jeangène Vilmer, *The "Macron Leaks" Operation: A Post-Mortem*, Atlantic Council/IRSEM, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/.
[73] Hearing of Louis Gautier (SGDSN) at the National Assembly, 21 February 2018, in 'Rapport fait au nom de la commission de la défense nationale et des forces armées sur le projet de loi (n°659) relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense', http://www.assemblee-nationale.fr/15/rapports/r0765-tII.asp.
[74] Jean-Yves Le Drian (Minister of Defence), interviewed in *Le Journal du Dimanche*, 8 January, 2017.

to malicious actors and the consequences of their actions can act as a deterrent".[75] "Deterrent" may be too strong a word, as these precautions were obviously not enough to deter the attackers behind the Macron leaks; but given the amateurism of the attack, it can safely be assumed that the foreign power behind it exercised restraint in the face of the hard stance taken by the French authorities, who also took technical precautions such as withdrawing electronic voting for citizens abroad because of the "extremely high risk" of cyberattacks.[76]

Second, as far as the reaction is concerned, when the leaks occurred, the French authorities moved swiftly. At 10 p.m. on the night of the dump, Macron's team alerted the Superior Audiovisual Council (CSA), the French regulatory media authority. Reacting fast, at 11.30 p.m., the CSA emailed TV and radio correspondents asking them to refrain from disseminating any information on the election coming from digital platforms. "The aim of this preventive action was to rapidly alert publishers against the dissemination of false news that could have an impact on the conduct of the electoral weekend", the CSA later explained.[77] Macron's team also alerted the National Commission for the Control of the Electoral Campaign for the Presidential Election (CNCCEP), a temporary body set up two months before the presidential election to serve as a campaign watchdog, which issued a press release the following day. Titled "Recommendation to the media following the computer attack on Macron's campaign team", the press release drew "the attention of the media to what is expected of them, because the free expression of the electorate and the sincerity of the ballot are at stake". The president of the CNCCEP asked the media "not to report on the content of this data, especially on their websites, reminding the media that the dissemination of false information is a breach of law, above all criminal law".[78] The CSA also forwarded this message to the broadcast media.[79] The public prosecutor's office also opened an investigation into the leaks within hours of their release, which was entrusted to the Information Technology Fraud Investigation Brigade of the Paris police.

Overall, the French response to the 2017 Macron Leaks operation inspired other governments, particularly the Canadian government, as they were preparing their own plans to prevent election interference. The author of this Research Report had the opportunity to present the French experience to Minister Karina Gould, the Minister of Democratic Institutions, in June 2018 in Ottawa and, as already mentioned, to the entire Canadian government during their cabinet retreat in Nanaimo, B.C., in August 2018. Unveiling its plan to fight potential election meddling in February 2019, Karina Gould said the plan was "modeled on what France has in their Conseil d'État, their kind of State Council, that kind of weighs in in elections if they see something that they think needs to be alerted to the public. And they did, in fact, when the Macron leaks happened. … they kind of weighed in and told the media not to report on it, right? Because it was, they believed, from foreign interference. And so, we tried to learn from successful examples of ways of being able to block foreign interference and say, 'How can we apply that in the Canadian context?'".[80]

The 2018 momentum

In September 2017, the Foreign Ministry's Policy Planning Staff (Centre d'analyse, de prévision et de stratégie, CAPS) and the Defence Ministry's Institute for Strategic Research (Institut de recherche stratégique de l'Ecole militaire, or IRSEM, of which I am the director), launched a joint working group. This work was not commissioned by the government, contrary to a rumour later spread by certain outlets – and even the Russian government itself –in the hope of discrediting our efforts. Rather, we

[75] United States Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security*, A minority staff report prepared for the use of the Committee on Foreign Relations, 115th Congress, 2d session, January 10, 2018, p. 125.
[76] ANSSI, *Rapport d'activité 2017*, p. 18.
[77] CSA, *Rapport sur les campagnes électorales. Election présidentielle (23 avril – 7 mai 2017), Elections législatives (11-18 juin 2017)*, Paris, April 2018, p. 23.
[78] Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle, 'Recommandation aux médias suite à l'attaque informatique dont a été victime l'équipe de campagne de M. Macron', Paris, 6 May, 2017, http://www.cnccep.fr/communiques/cp14.html.
[79] CSA, *Rapport sur les campagnes électorales.*
[80] Karina Gould, interviewed by Chris Hall on CBC Radio, 2 February, 2019.

acted on our own initiative. The main result was a 200-page report titled *Information Manipulation: A Challenge to our Democracies*, launched at the beginning of September 2018 and available online in French and English.[81] This report rejects the phrase "fake news" for being both vague and itself manipulated by populist leaders, who call all news they dislike "fake". It prefers the term "information manipulation", described as involving a coordinated campaign, the diffusion of false information or information that is consciously distorted, and the political intention to cause harm. CAPS and IRSEM have been advocating for this terminology in their internal memoranda since the beginning of 2018. Minister for Europe and Foreign Affairs Jean-Yves Le Drian publicly advocated it in his speech on 4 April, and in May, an amendment was made to the proposed bill then under consideration before the Parliament, which allowed its name to be changed from "Against false information" (*contre les fausses informations*) to a law "relating to the fight against information manipulation" (*relative à la lutte contre la manipulation de l'information*). The French terminology is therefore coherent on this matter. The report explores the causes and means of information manipulation, the responses, and future challenges. It concludes with 50 recommendations, including 20 for states. These include:

- Avoiding heavy-handedness: Civil society (journalists, the media, online platforms, NGOs, experts and academics) must remain the first line of defence against information manipulation in liberal, democratic societies. The most important recommendation for governments is to retain as light a footprint as possible – for the sake of their values but also out of a concern for effectiveness.
- Creating a dedicated structure, inside the government, to detect and counter information manipulation.
- Increasing transparency: making registration compulsory for foreign media, following the American example; conducting parliamentary inquiries; holding platforms accountable (for example by demanding that they publicize the sources of their advertising and requiring them to contribute to media literacy and quality journalism).
- Going international: states must increase their participation in existing initiatives such as the EU East StratCom Task Force, the European Centre of Excellence for Countering Hybrid Threats in Helsinki, and the NATO Strategic Communications Centre of Excellence in Riga. They should also send experts to compare notes and experience in important annual meetings in Prague, Riga, Washington, DC, and Singapore, to name a few.
- Teaching media literacy and critical thinking to children as well as adults; states could also support research (increase funding) on this issue, and so forth.

A number of measures were also implemented in 2018. First, a law against the manipulation of information was approved by the National Assembly on 20 November 2018. One month later, the Constitutional Council confirmed its legality. Under this law, information manipulation is defined as the "inexact or misleading allegation of a fact that could alter the sincerity of an upcoming vote and that is spread deliberately, artificially or automatically and massively to the online public through a communication service".[82] Second, as recommended, a dedicated network has been created, coordinating whole-of-government efforts against information manipulation. However, in stark contrast to the other national approaches presented in this Research Report, it has not been made public, and even its name is supposed to be secret. Third, the culture minister also pledged to double her ministry's budget for media and information literacy, from 3 million euros to 6 million euros, to support civil society initiatives.

An inclusive approach, civil society oriented

As recommended in the CAPS/IRSEM report, the French authorities adopt a light-footprint

[81] Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, CAPS/IRSEM, 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

[82] For a detailed analysis of the French law, see Marine Guillaume, *Combating the manipulation of information – a French case*, Hybrid CoE Strategic Analysis 16, 3 May 2019, https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-16-combating-the-manipulation-of-information-a-french-case/.

approach to countering information manipulation, considering that it is and should remain first and foremost a role for civil society, particularly journalists and NGOs. From that perspective, a criterion of success or effectiveness would be for non-governmental actors within civil society to be able to respond to the influence campaign without state intervention. That point has not been reached yet and, in France as elsewhere, a state response is still needed. The French authorities have pushed this civil-society-first approach to the point (not recommended by the report) that, until recently, they communicated very little, particularly compared to states like the UK, Sweden, Canada, or the US, about what the state has been doing on that front, especially about its internal organization. This secrecy makes it difficult, for a public document like the present one, to be detailed and to reveal what actions are being taken by specific departments or units.

What can be said is that, within the Ministry of Europe and Foreign Affairs, the team of the Ambassador for Digital Affairs, himself coming from civil society, has been working very closely with non-state actors. Their website disinfo.quaidorsay.fr, available in French, English and traditional Chinese (a sign of excellent cooperation with Taiwan's Digital Minister Audrey Tang), hosts many resources (including home-built and open-source tools) available for anyone to use.

In June 2019, the Ambassador for Digital Affairs, with the support of the Directorate for Information Systems (DSI) of the same ministry, and the SGDSN, organized a two-day event on countering online information manipulation, with approximately 50 people coming from civil society, particularly journalists, academics, developers and NGOs, but also private companies, including social media platforms, other members of governmental agencies and representatives of four other countries.[83] During the first day, 16 workshops of 5–10 people were organized on different themes (the targeting process, disinformation techniques, detecting and countering disinformation techniques, etc.). On the second day, a hackathon took place, where computer programmers and software developers were put to the test and challenged to design tools to counter concrete information manipulations. What is more, for the first time outside the US, Facebook offered a training session on its Social Science One programme (allowing selected social science researchers to have access to anonymized data). Nathaniel Persily, academic supervisor of the programme, said: "What we are trying to do today, here with the French government, creates a precedent and should serve as an inspiration for other countries around the world".[84]

Another sign of this civil-society approach is the support President Macron provided for Reporters Without Borders' (RSF) International Initiative on Information & Democracy, pushing twelve Heads of State and Governments to commit, during the first edition of the Paris Peace Forum (November 2018), to launching a political process based on this initiative,[85] and promoting it within the G7.[86]

The 2021 turn

A major announcement was made in June 2021, followed by several press indiscretions: a new national agency, named "Viginum" (standing for Vigilance and protection service against digital interference), will be operational in September 2021. Its role will be to "monitor, detect and characterize foreign digital interference operations aiming at manipulating information on social networks", as well as to "provide any useful information" to the CSA and to the National Commission for the Control of the Election Campaign.[87] Of significant size, with a staff of 40 people in the first months, and 65 by April 2022, it will operate under the SGDSN,

[83] See Ambassadeur pour le numérique, 'Disinformation unconference digest', https://disinfo.quaidorsay.fr/assets/2019_disinformation_unconference_digest_HD.pdf.
[84] Ibid., 27.
[85] RSF, Information & Democracy Commission, https://rsf.org/en/information-and-democracy.
[86] RSF, '"Unanimous" G7 support for RSF's Information and Democracy Initiative', 26 August 2019, https://rsf.org/en/news/unanimous-g7-support-rsfs-information-and-democracy-initiative.
[87] Pierre Alonso and Amaelle Guiton, '"Les dessous de Viginum", la future agence contre les manipulations de l'information', *Libération*, 30 June, 2021, https://www.liberation.fr/societe/police-justice/les-dessous-de-viginum-la-future-agence-contre-les-manipulations-de-linformation-20210630_NFTB6CNJ6ZGDDFBMZRZKBBANYA/.

itself under the Prime Minister's authority.[88] According to a newspaper article, its annual budget would be around 12 million euros.[89]

This is important news. The author has been advocating such an initiative since 2017 in internal memos and the CAPS-IRSEM report.[90] The build-up has been gradual. First, in 2018, following the publication of the report, France created a "Committee against information manipulation",[91] a cross-departmental network based at the SGDSN, coordinating whole-of-government efforts against information manipulation. Then, in autumn 2020, the French government response to several terrorist attacks, including the beheading of a teacher in a Paris suburb, triggered a number of anti-French campaigns in the Muslim world, amplified by a couple of state actors manipulating social networks. In order to combat this specific threat, France experimented with a small temporary cell, called the "Honfleur Task Force".[92] Both the network and the task force were under-the-radar, discreet initiatives. This decision to create a permanent, publicly acknowledged structure, of such a size, is therefore a significant change. It is all the more timely considering that there are two important electoral deadlines coming up, likely carrying high risks of foreign information manipulation: the New Caledonian independence referendum in December 2021, and the presidential election in April 2022.

[88] France Inter, 'Que sait-on de la future agence de lutte contre les manipulations numériques venues de l'étranger?', 2 June, 2021, https://www.franceinter.fr/monde/que-sait-on-de-la-future-agence-de-lutte-contre-les-manipulations-numeriques-venues-de-l-etranger.
[89] Alonso and Guiton, '"Les dessous de Viginum"'.
[90] Vilmer et al., *Information Manipulation*, 170.
[91] Alonso and Guiton, '"Les dessous de 'Viginum"'.
[92] *Le Monde*, 'La France va créer une agence nationale de lutte contre les manipulations de l'information', 2 June, 2021, https://www.lemonde.fr/pixels/article/2021/06/02/la-france-va-creer-une-agence-nationale-de-lutte-contre-les-manipulations-de-l-information_6082561_4408996.html.

General lessons

None of the four examples presented in the previous pages is a perfect model. For the purpose of this Research Report, we focused on their strengths, but they obviously have weaknesses as well. Moreover, as mentioned in the introduction, the practices are context dependent. They work in a given national environment, with various strategic interests, and may not be replicable elsewhere. However, they could inspire other countries, which could adapt them to their specific political, social, and cultural context. Some nations already have. The Swedish approach has been exported to other countries, not only across the Nordic-Baltic region, but also in Singapore for example. Not only are the various approaches presented here not mutually exclusive, but many partially overlap. Some of them develop the same good practices, like a rights-based approach, the combination of actor-agnostic and actor-specific approaches, or a civil-society-first approach. Alternative examples could have been used: for instance, this Research Report used Canada as an example of effective preparation against election interference, but Sweden is also a good case in point.[93] In the final analysis, principles distilled from these experiences tell us (in a non-exhaustive list) that an effective state response likely involves:

- An ability to clearly define the threat: what are we talking about? Disinformation, information manipulation, information influence, foreign interference, hybrid threats?
- At least one state structure entirely dedicated to detecting and/or countering disinformation, and a cross-departmental network sharing information on a regular basis, all able to function irrespective of the political will of the moment.
- A posture whereby the state is reactive and ready to adapt any organization to an unexpected change, in the event of a crisis for instance.
- Having a permanent or ad hoc format allowing this internal organization to meet and work with experts from industry, civil society and academia.
- Combining an actor-agnostic 360° approach with actor-specific expertise.
- Staying updated on the evolution of the global information space (new actors, strategies, and tactics).
- An awareness of the state's own vulnerabilities, within both society (vulnerable populations and communities, particularly corrosive narratives) and state (lack of transversality, reactivity or adaptability, among other issues).
- Increasing society's resilience by resorbing the identified vulnerabilities, strengthening the credibility of public institutions, developing media literacy, digital education and critical thinking (for all ages, not only children and students), increasing the consumption of quality independent media both domestically and abroad (by supporting investigative and local journalism in terms of funding and information sharing), and so on.
- Communicating regularly about disinformation and the measures taken to counter it, by publishing national strategies, speeches, interviews, and op-eds, including on social media platforms, for both awareness and deterrence purposes.
- Working at all levels, not only national/federal but also provincial/regional and local, with both authorities and civil society organizations.

[93] Fjällhed, Pamment, and Bay, 'A Swedish perspective on foreign election interference'.

- Developing international cooperation, through participation in existing formats or initiatives (G7, EU, NATO CoE Riga, Hybrid CoE Helsinki), and tracking regular think-tank-organized meetings, but also through an offensive benchmarking attitude (constantly sending, possibly even posting, personnel abroad to learn from others), and capacity-building measures in countries where strategic interests are at stake (by supporting local journalism, reaching out to local influencers, experts and researchers, developing social media analysis tools, etc.).
- Funding research on disinformation by commissioning reports from universities or think tanks, then publishing and promoting them in the media.
- Giving decision-makers access to this research, and more generally to civil society expertise, by translating it into digestible memos and briefings.
- Using this research as a basis for training a maximum number of civil servants, in a variety of courses on vulnerabilities, threats, and countermeasures.
- Training journalists through an intermediary, by funding an academic research centre or a think tank to organize a customized course for them.
- Organizing regular cross-departmental exercises and simulations, occasionally involving civil society actors.
- Valuing transparency and respect for privacy and press freedom by adopting an approach focused on harm, possibly with the help of a human rights officer incorporated into teams working on domestic issues.
- Having at least one dedicated cross-departmental permanent unit or temporary task force working on the protection of elections and referendums, learning from past election interference from all over the world, digesting the academic literature on the topic, designing public awareness campaigns and specific training sessions, and so on.
- Working closely with social media platforms, asking them to take concrete measures in terms of integrity, transparency and authenticity, but also to allow access to their data to help in analyzing an incident.
- Being ready to spend money, as effectiveness comes at a price: many of the initiatives presented in this Research Report, from staffing internal teams to funding research and civil society activities, cost several million euros.

Author

Dr Jean-Baptiste Jeangène Vilmer is director of the Institute for Strategic Research (IRSEM) at the French Ministry for the Armed Forces, and a nonresident Senior Fellow at the Atlantic Council, Washington DC. He is also an Adjunct Professor at the Paris School of International Affairs (PSIA) and an Honorary Ancien of NATO Defense College.

Hybrid CoE