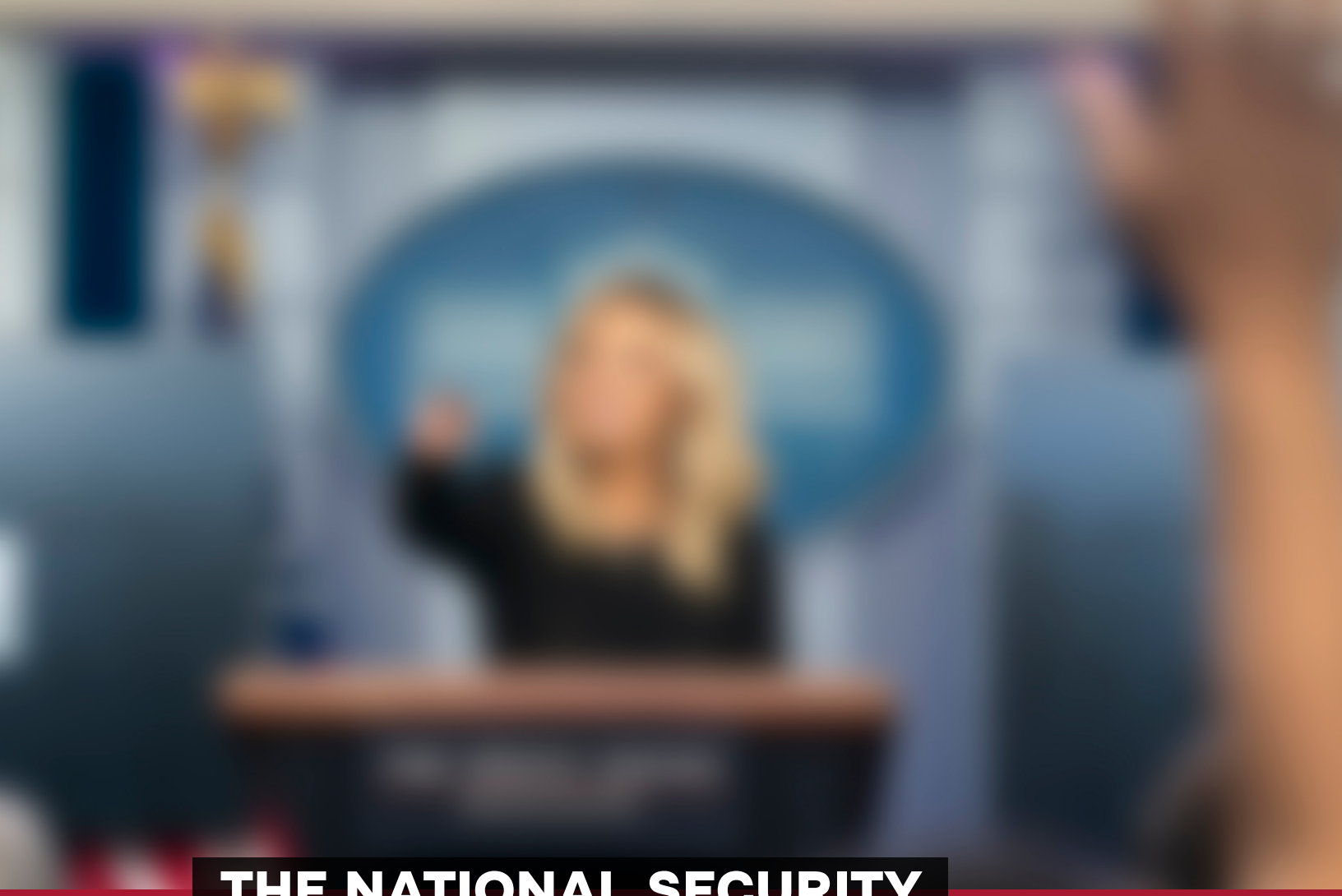

THE NATIONAL SECURITY IMPERATIVE FOR THE MODERNISATION OF GOVERNMENT COMMUNICATION STRUCTURES

Camilla Monckton
Shorenstein Fellow / Head of Strategic Communications
UK Cabinet Office (2021 - 2024)

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy

Table of Contents

INTRODUCTION

The democratic duty to inform citizens in the digital age

The information environment has changed dramatically in the last 20 years, calling for an equally dramatic shift in the way that the Governments operate within this new information environment, a shift that is largely yet to occur in many democracies. A failure to modernise communication structures to effectively engage citizens in a more crowded and complex information environment reduces access to reliable information. Healthy democracy is contingent on this access. It is built on *"the crucial compact that citizens will have access to reliable information and can use that information to participate in government civic and corporate decision-making".*[1]

When this compact is broken and Governments struggle to effectively communicate with their citizens–the democratic process is weakened. This threat to democracy exists independently of any adverse actors operating in the information environment. The threat is even greater when Governments are failing to communicate effectively with their citizens, while adversaries are investing in efforts to do so. Hostile state actors are deploying existing and emerging capabilities in information manipulation to actively engage audiences in foreign countries — with the aim of undermining global cooperation and weakening support for liberal democracy. These narratives gain more traction in the absence of reliable information, disseminated effectively, from a host nation.

Government Communication Structures need to modernise to engage citizens effectively in the digital age to minimise the impact of foreign interference in their domestic information environment. Yet to date, despite the increasingly well recognised threat of Foreign Information Manipulation and Interference (FIMI), public communication reform has too rarely been instigated as a necessary response to this threat.

Efforts to tackle FIMI, and disinformation more broadly, have focused on developing a healthier information ecosystem, and less on how Governments should operate in the new and evolving information environment as it currently is. Some initiatives have been developed to improve the rules and setup of the information environment (tech regulation, supporting independent media). Others work on generating accountability in the information environment (fact-checking, content labelling, tackling advertising models). Another set focus on analysing

Hostile state actors are deploying existing and emerging capabilities in information manipulation to actively engage audiences in foreign countries...these narratives gain more traction in the absence of reliable information, disseminated effectively, from a host nation.

hostile actors in the information environment (open source intelligence analysis) and shaping how citizens interact with this information (media literacy). Insufficient effort has been put towards understanding how Governments operate and communicate within the new information environment and its associated threats.

Where national security concerns have spurred communications reform, these have often been isolated to foreign affairs, public diplomacy and defense. Less attention has been paid to addressing vulnerabilities in the domestic information environment, which have been exacerbated through a deficit of effective public communications.

It is crucial to shift the conversation away from strategic communications in foreign affairs and defence and toward how governments effectively engage their own citizens in the domestic information space—especially in the face of adversaries operating within it. The discussion on countering FIMI must not remain confined to public diplomacy, soft power, or influence-building abroad. Equally it should not be narrowly focused on identifying and "tackling" disinformation nor engaging in a battle of narratives in a global power struggle or domestic politics.

Instead, greater attention must be given to a government's democratic duty to inform its citizens—ethically and effectively—in the digital age. Doing so not only upholds democratic principles and participation but also strengthens national resilience by mitigating the impact of FIMI.

The Evolution of the Information Environment

The technological advances of the last 20 years have revolutionised the **production**, **consumption** and **dissemination** of information transforming the way individuals, governments and citizens and states interact. The same technologies that serve as a positive force for participatory discourse that democracy is rooted in, are also shaking its very core–disrupting the ability for citizens to rely on a shared body of knowledge.

Production has diversified news sources providing broader perspectives, but at the expense of editorial oversight and quality control.

Consumption patterns enable individuals to access precisely what they are seeking, leading to a more informed and engaged populace, but in doing so have limited exposure to diverse viewpoints creating filter bubbles that reinforce existing beliefs and can spur polarisation.

Dissemination mechanisms have enabled real-time broadcasts and real-time citizen mobilisation, enhancing awareness and facilitating global conversations, but at the expense of accuracy and reliability, intensifying the spread of misinformation.

So normalised and integrated in our daily lives are the interoperable products, systems, and devices of Web 2.0 that it is easy to forget that as little as 20 years ago Facebook, YouTube and Twitter had not even entered the public domain. Apple had barely launched 'Project Purple' to build what came to be the iPhone. Only 15% of the world had internet access. These facts alone should be enough for Governments to recognise that public communication structures built two decades ago are simply not fit for use in today's information environment.

Strategic Communications Vs. Public Communication - how are they currently valued in democracies?

Public Communications: The Organisation for Economic Cooperation and Development (OECD) defines Public Communications as *"the Government functions to deliver information, listen and respond to citizens in the service of the common good."* It is distinct from *"political communication which is linked to partisan debate, elections or individual political figures."* Public communication refers to the function, structures, and policies that shape Government Communication machinery, within which strategic communications is as a discipline.

Strategic Communications (Public Diplomacy): Strategic communications is a more nebulous term when used in discourse on countering FIMI. Originating in the Cold War, it evolved as Joseph Nye coined 'Soft Power' to encompass media, cultural exchanges, and discreet efforts to share ideologies and garner international support. It distances itself from political persuasion, election campaigns or commercial marketing, and propaganda – where the purpose is understood as deception.[2] It is rooted in understanding actors and audiences and how they communicate. Its popularisation in terminology, if not always in practice, comes in recognition of the importance of not just transmitting information but persuading and engaging an audience. The UK Government Communication Service defines it as:

"Influencing audiences for public good by marshalling the necessary resources to achieve agreed goals. This is achieved through organisational unity; the co-ordinated use of all the communication tools available, underpinned by research and given coherence in a story and communication products. This is set out in a single plan, working to milestones and properly evaluated."[3]

Strategic Communications 'StratCom' (Defense): In public diplomacy the principle is *"it is not just what you do, but how you say it."* In the Military context, in contrast it emphasizes that *everything* sends a message—equipment choices, training locations, and alliances. The UK Ministry of Defence defines it as:

> ***"Advancing national interests using Defence as a means of communication to influence the attitudes, beliefs, and behaviours of audiences (JDN2/19)."***[4]

Strategic communication is well-studied in the context of defense and public diplomacy, with growing research on its techniques—tailored content, audience targeting, and behavioral science. However, less data exists on the *public communication structures* needed to effectively implement strategic communication strategies, particularly in the domestic information environment to engage citizens in a democracy. To address this, a 2021 OECD report analyzed communication structures across 46 countries.[5] It found that 38% of countries did not have disinformation guidelines and 26% did not tailor messaging to audiences at all —an approach hostile states exploit at scale, including in other nation's domestic audiences. Overall it identified weak integration of communications in government with less than 50% of communicators engaging regularly with policy teams, and 76% citing resource constraints. This disconnect, along with outdated communication structures, leaves democratic governments struggling to remain authoritative in an increasingly complex information environment, let alone capable of countering foreign interference.

WHY HAVE DEMOCRATIC PUBLIC COMMUNICATION STRUCTURES BEEN SLOW TO ADAPT TO THE NEW INFORMATION ENVIRONMENT?

A combination of both ideological and bureaucratic challenges has hindered the development and modernisation of many democracies' communications structures.

The ideological challenges are the result of 1.) a slow wake-up call to the national security threat of a borderless information environment and 2.) concerns that the expansion of government communications is at odds with free speech.

The bureaucratic challenges are the result of 1.) slow adaptation to technological change, and perceptions of communications as a profession and 2.) the coordination challenges of responding to a national security threat with reform of a civilian response such as day-to-day public communications.

Ideological Challenges

The internet as a democratising force?

A slow wake up to threats in the information environment.

The national security implications of failing to fulfil the democratic duty to inform were not as pressing to democracy 20 years ago. In fact, at its dawn, any threats associated with the internet's uses and users, were not to democracy, but to non-democratic states whose coercive governing tactics might be exposed. While the Arab Spring might have seen social media mobilisation disrupt authoritarian regimes, Bill Clinton's claim that China's early attempts to censor the Internet were like 'trying to nail Jell-O to the wall' has certainly not rung true[6]. The Great Firewall of China and Russia's Roskomnadzor have proven to be highly effective. In contrast, the open internet of democratic countries allows foreign states to communicate freely within others' domestic information environments–creating a very different threat picture than once anticipated.

Democratic nations have not met this challenge with complete inertia, and lessons have been learnt. In 2014 the West failed to coordinate a meaningful response to Russia's annexation of Crimea. Russia polluted global information spaces with hundreds of false and conflicting narratives and denied any connection to the 'Little Green Men.'[7] The West was unable to ascertain and communicate an understanding of what was happening on the ground, nor its stance, before it was too late. Cut to Russia's full-scale invasion of Ukraine in 2022 and the false narratives setting up the pretext for war were exposed and effectively 'pre-bunked.' Timely communication on the intelligence picture was disseminated from credible sources, and critically, the West was unified and coordinated in its response. This was a result of significant investment in understanding the information environment and how to communicate better within it. Integral to this ability to communicate better was the strengthening of networks and alliances in the recognition that the threat of state-backed disinformation knows no borders and attacks are coordinated across multiple territories–demanding coordinated responses.

The development of these alliances is critical. They were critical to the UK when the Russian state poisoned Sergei Skripal, the Russian defector turned British citizen, on British soil in 2018. Firstly, the UK was better prepared for the information operations that accompanied the attack, and told the public to anticipate false narratives, and indeed saw the flood of false narratives as proof of Russia's involvement rather than a deflection. Secondly and crucially, the UK did not stand alone. They were joined by 28 partners and NATO in expelling more than 150 Russian intelligence officers–a direct response to deter and degrade Russia's ability to conduct future operations and reduce GRU networks.[8] This would not be possible without the prior

development of communication structures and alliances that enabled better understanding of the threat and appropriate responses.

These alliances were critical to President Volodymyr Zelensky when Russian troops crossed into Ukraine in the early hours of February 24th, 2022. Zelensky is an exceptionally charismatic leader with a background in media and entertainment rare for a Head of State. These skills proved invaluable in communicating his country's plight and garnering support. This alone did not enable him to beam into multiple parliaments in the weeks after the invasion began. Ukraine's ability to elicit such a rapid response stemmed from years of investment in internal communications reform and the construction of international partnerships and alliances. This success was built on the often-overlooked, day-to-day work of assembling the right teams—ensuring core scripts were drafted to keep officials aligned, external affairs teams had established strong networks, media monitoring teams were in place, and graphic design capabilities were developed to swiftly deploy visual assets. This was a key difference between 2014 and 2022. Structures had been built, staff had been hired and trained, and networks were developed. These structures are needed across the board, not just in international engagement and not just in times of war.

Understanding how information operations interact with specific hybrid and traditional warfare attacks is vital. These information operations are, however, just the tip of the iceberg. What is constantly happening in and around these events, is of equal if not greater concern. Foreign interference is also rife in day-to-day communication on seemingly benign topics to more contentious policy areas that matter to electorates, such as climate change, migration, and LGBTQ rights. This has the ability to shift public sentiment at scale and poses a significant threat, particularly around election cycles. Democracies need to ensure that they are effectively communicating their policies - both domestic and foreign - to their citizens before other states do.

The same concerted efforts that have improved democracies' external strategic communications responses, needs to be put into modernising internal communication structures. Especially when hostile states are investing heavily in communicating in their adversaries' information environments. The instigation of internal communication reform is more challenging - both logistically and bureaucratically (as discussed later) - but also ideologically, on account of a false perception that it might be at odds with free speech.

Free Speech and Governments role in the information environment

The Harvard Belfer Center's paper on the Geopolitics of Information argues that democracies have largely considered any type of information strategy to be unnecessary, stating that "government involvement in the domestic information environment feels Orwellian," with democracies believing that their 'inherently benign' foreign policy didn't need extensive influence operations."[9] There of course have been instances when robust information strategies have been executed – the US, UK, Germany and France's communication efforts were significant during the Second World War, for example. The information strategies deployed by the Global Coalition against Daesh serve as a more recent example.

Efforts to expand day-to-day communications with citizens, particularly in times of relative peace, have often been viewed as Orwellian and at odds with free speech, or, as above, unnecessary.Government involvement in the domestic information environment does not have to be at odds with free speech. Modernising government communication structures to operate effectively in an evolved information environment *is not* expanding an existing share in an arena in any Orwellian fashion. It would rather be recognising that to maintain the same level of communication with citizens in a new digital order, a new and transformed capability is needed. Only then can the basic democratic duty to inform be fulfilled.

When reform is discussed in the context of *countering* disinformation, as opposed to a duty to inform, its intent becomes skewed, opening it to politicisation and complicating reform efforts. It comes from a reactive place of correction and implies that a government can discern what is true and what is false and choose which narratives to correct or counter. This raises legitimate concerns. A democratic government cannot and should not operate as an arbitrator of truth. It can and should however expand its communication functions to effectively engage its citizens in an ever-expanding information environment.

Reform needs to come firmly from the place of correcting a deficit of public communication to build resilience to disinformation, not 'correcting narratives to counter disinformation.' If changes to communication structures are framed as responsive to disinformation, rather than correcting a deficit, concerns around censorship or free speech will inevitably arise–hindering simple and essential reforms.

In the US, Republican lawmakers raised concerns over "the potential serious consequences of a government entity identifying and responding to 'disinformation'"[10] when the Biden administration sought to establish a 'Disinformation Governance Board' in 2022. One of the core functions of this board would have been to increase public communications on key national security priorities that would build resilience to hostile state narratives. Its framing, however as a countering-disinformation initiative, over a public information and safety effort, stopped it in its tracks.

There is a fine balance to be struck. There are legitimate concerns about a government entity determining what is and isn't disinformation. On the other hand "a chimera of censorship can chill legitimate academic inquiry into disinformation" as Nina Jankowicz, the Executive Director of this Disinformation Governance Board, warned. This, she argues, "undermines public-private cooperation in investigating and addressing the problem, and halts crucial government responses. The result is an information ecosystem that is riper for manipulation than ever."[11].

The challenges need to be addressed from two angles: addressing a deficit of government information created by a failure to adapt to a new information environment, and responding to a threat of foreign interference that is exacerbated by this deficit.

Bureaucratic challenges to public communication reform

Perceptions of the Communications profession and bureaucratic battles with technological change.

When the forces driving rapid change in technology and data use increasingly are global organisations with resources far greater than those of a communication function, keeping up is a perpetual challenge. This is felt across government functions.

A specific challenge to the communications function is that the perception of its role is not evolving to match the demands technological changes are putting on the function. Historically communications held more of a subsidiary function, or at least was secondary to policy. In the traditional media environment, public communication was defined by the press office. Its core role was to update on political and policy developments and respond to journalists' queries. It was more perfunctory; focused on the dissemination of information with a limited role in policy implementation.

Today with 24-hour news cycles and democratic life playing out online, the nature of this dissemination has changed as has the role in which communications can and should play in policy implementation. Yet when a function has historically been seen as secondary and not as hard-hitting, shifting the weight it holds and the respect it garners is neither easy nor quick. This hinders its ability to gain the necessary weight and respect within government structures. Communicators rarely have the same level of seniority as policy officials and don't always have a seat at the policy table affecting their ability to be prioritised.

Additionally, few democratic governments even have a centralised government function - with each ministry managing their communication outputs separately. This lack of centralisation hinders coordination of both outputs and reform, both logistically and on account of protectionism within Ministries.

Many countries employ political appointees rather than career civil servants as communication directors and staff, blurring the line between public and political communication. The separation of these two functions will always be a tension that needs to and can be managed. Beyond the obvious impact of political interference on objectivity, neutrality, and public trust - the short-term nature of political appointments hinders long-term communication reform. Governments have hesitated to develop robust communication capabilities that could be co-opted by future administrations for political gain. Short-term political objectives often take precedence over the democratic imperative of effectively informing citizens.

The perception of communications as a secondary function, coupled with the lack of centralization and the short-termism of political appointments, has created a persistent barrier to reform. Some change is of course happening, but without urgency. New technology is enhancing abilities to monitor and evaluate campaigns, improving communications teams' ability to demonstrate their value through proof of Return on Investment. COVID-19 saw communication and policy teams having to work much more closely, and the role of communications in policy implementation was clearly demonstrated. And, as laid out previously, significant strategic communications capability has been built across Europe in Foreign Affairs and Defence Ministries., r. The challenge that remains however, is transferring this understanding of the National Security threat so that it leads to the modernisation of day-to-day public communications in civilian domestic facing structures.

Instigating Domestic Public Communication reform as a response to a National Security Threat.

The recognition and deep understanding of the threat of FIMI and communication responses have often been isolated to the Ministry of Foreign Affairs or Ministry of Defense. sThis has enabled stronger responses to FIMI surrounding geopolitical events cited earlier but largely remains reactive and international facing. There are also instances where this capability has been used to build resilience to disinformation in the domestic environment, but this is not always possible. At the time of the Skripal poisonings in 2018, the UK Foreign Office was able to run a campaign to warn the public of associated Russian-backed disinformation. The US State Department, on the other hand, is legislated against communicating in the domestic information environment under the Smith-Mundt Act of 1948. Its applicability today has, however, been called into question as the line between domestic and foreign audiences is blurred.

Regardless, to effectively mitigate against FIMI in the domestic information environment, a whole of government response is needed and, indeed, one that is broader than just communications reform. Even where states do have National Security Councils or equivalent structures to coordinate

whole-of-government responses, it remains an internal coordination challenge to enable a foreign threat to national security to necessitate the reform of a civilian day-to-day capability such as public communications. Reform is rarely going to happen overnight with one whole-sale re-allocation of resources and design of structures. It tends to be more organic. One capability might be built in one ministry often in response to a particular crisis. This can then lead to a proof of concept spurring further reform, or the recognition of overlapping capabilities being developed, which then requires some form of centralisation to ensure coordination. All of this takes time.

Estonia's raft of responses to mitigate against hybrid warfare and more day-to-day attempts to disrupt social cohesion have been lauded. They are,, ahead in their journey having had a much earlier wake-up call. Their impetus for reform came in 2007 following a slew of cyber and information attacks launched by Russia after the relocation of a Soviet WWII memorial, the 'Bronze Soldier.' It took ten years, however, for the communications capability that began in the Ministry of Defence and Ministry of Foreign Affairs to translate into a centralised communications remit in their central Government Office, mandated by the 2017 National Defence Development Plan.[12]

For the UK, the Skripal poisonings in 2018 served as a pivotal moment. They spawned the expansion of communication and media monitoring teams, and the development of the UK's counter-disinformation framework used to upskill communicators–RESIST.[13] For Poland, the hybrid attacks launched by Belarus on the Polish-Belarus-Lithuania border in 2021 and the accompanying information operations,[14] produced a recognition that the efforts they had been building in the defense context since 2014 were not sufficient and needed further coordination. In 2022, a new office was established in the central government in charge of 'enhancement of Poland's information space resilience through coordinating communication activities of institutions responsible for shaping Poland's information policy'[15] However, these efforts later fell foul of the 'chimera of censorship' and Ministry of Truth allegations, halting communication reform. Though short-lasting it was a a physical hybrid attack that instigated efforts to reform and coordinate communication activities.

Physical elements of hybrid attacks on home soil have spurred greater coordination of communication capability in some countries,-centralising efforts that began in defence and foreign affairs ministries in 2014. 2014. The same concerted efforts that have improved democracies' external strategic communications responses, needs to be put into modernising internal communication structures. This is where a significant threat lies. Governments cannot and should not wait for the impetus created by a physical attack to instigate central communication reform, when hostile state influence operations are far from exclusively linked to physical attacks. Foreign states are communicating daily in the domestic information environment of other states, and this activity thrives in the absence of effective, modern communication by any state in their own domestic information environment.

Despite this threat, and because of the ideological and bureaucratic challenges listed above–democratic government communication structures are not prioritised and invested in as a critical part of democratic governance or national security infrastructure. The result is a dangerous level of state silence that paves the way for other states to shape perceptions and interactions.

CONCLUSION

THE COST OF STATE SILENCE AND PATHWAYS TO REFORM

The modernization of government communication structures is not just a matter of keeping pace with technological change—it is a critical imperative for maintaining the health of democratic societies in the face of evolving national security threats. As we have seen, the failure to adapt to the new information environment creates a dangerous vacuum that adversaries are all too eager to fill.

When democratic governments fail to effectively communicate their values, services, and purposes, they leave the field open for other actors—including hostile states—to shape public perceptions. This state silence can have profound real-world implications:

If only Russia is communicating with citizens in a NATO member state about what NATO stands for, and not the Government of that state -- who is shaping the opinion of NATO? Russia or that NATO member state? What are the real world implications of the electorate losing support for NATO?

If only China is communicating about the investments that it makes in any chosen country, through Op-Eds, billboards, and art installations -- while the EU simply places a small flag on a sign next to a rural hospital it has built -- who will the citizens of that country see as a key supporter, investor and partner? What are the real world implications of a population knowing about Chinese investments, but not those of the EU?

Democratic states and alliances cannot simply decry foreign interference without also addressing their own communication deficits and analysing how this information power imbalance has arisen.

A significant part of this is of course attributed to the very different rulebooks that democratic and authoritarian states abide by in the information environment — with authoritarian states having many more tools at their disposal which are at odds with democratic values and governance. However, currently, many democratic states are not effectively exploiting the tools that are available to them. By focusing on deploying transparent, ethical, and effective communication practices, democracies can rebuild public trust and build resilience to disinformation and FIMI. This approach not only upholds democratic values but also addresses the root causes of vulnerability that adversaries exploit.

The starting point to building information resilience must be addressing structural deficiencies to fulfil the democratic duty to inform, and, overcoming the identified ideological and bureaucratic barriers to reform. This begins with reframing the issue as a fundamental democratic responsibility, that in turn protects against FIMI, rather than a reactive measure against disinformation. This day-to-day communication function is critical for democratic resilience. A more targeted National Security Communications function is critical to tracking and defending against FIMI. This function should track areas of attack in the information environment, and instigate and coordinate strong communications from relevant ministries so that citizens hear their governments views on these topics, ahead of other states' messaging. If hostile states are seeking to destabilise another country by nefarious communications onadversaries migration policy or climate agenda, for example, then that country needs to prioritise communications on these topics - ensuring the intent behind their existing policy and its operations are understood among its own citizens.

To modernize their communication strategies, governments should invest in data-driven approaches and enhance digital content creation capabilities. Recruitment should focus on diverse talent with expertise in marketing and digital content alongside traditional journalism skills. Implementing multi-channel strategies that utilize both digital and traditional media platforms is crucial. Communications should be tailored to citizens' needs, ensuring messages reach audiences on their preferred platforms. There is a wealth of research out there on what works, from the OECD Public Communication Guidelines to private sector research, and existing modern government frameworks such as that in the UK.

The challenge lies not in the knowledge base, but securing the political will and impetus to act. This requires strong leadership that can recognise existing failings in fulfilling the democratic duty to inform, overcome the identified bureaucratic and ideological challenges, and instigate bold and necessary reform.

The stakes are high, and the time for action is now. As the information environment continues to evolve, so too must the structures and strategies that democracies use to engage with their citizens. Only through effective, modern, and ethical communication can governments hope to maintain the crucial compact of informed citizenship upon which democracy depends and build resilience to foreign interference in the borderless information environment.

ENDNOTES

1 Eric Rosenbach and Katherine Mansted, "Can Democracy Survive in the Information Age?" (October 2018), Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/can-democracy-survive-information-age.

2 Neville Bolt, "Understanding Strategic Communications," Terminology Working Group Publication No. 3 (NATO Strategic Communications Centre of Excellence).

3 GCS. (n.d.). Strategic Communication: MCOM Function Guide. [online] Available at: https://gcs.civilservice.gov.uk/publications/strategic-communication-mcom-function-guide/#:~:text=The%20Government%20Communication%20Service%20

4 UK Ministry of Defence. *Joint Doctrine Note 2/19: Defence Strategic Communication: An Approach to Formulating and Executing Strategy.* May 23, 2019. PDF. https://assets.publishing.service.gov.uk/media/5ce7fc2fe5274a4873de09e5/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communication_jdn_2_19.pdf.

5 OECD (2021), *OECD Report on Public Communication: The Global Context and the Way Forward*, OECD Publishing, Paris, https://doi.org/10.1787/22f8031c-en.

6 William J. Clinton, "Remarks at the Paul H. Nitze School of Advanced International Studies." (Washington, D.C., March 8, 2000), http://www.presidency.ucsb.edu/ws/index.php?pid=87714

7 'Little Green Men' is the name given to soldiers that helped illegally annex Crimea in March 2014 that did not bear any insignia. The Russian state repeatedly denied their affiliation with Russia at the time. Evidence later confirmed they were Russian and Putin admitted Russian involvement in the annexation later in 2014.

8 Pierce, Karen. "Evidence of Russia's Involvement in Salisbury Attack." Speech at the Security Council Briefing following the UK Prime Minister's update on the Salisbury incident and the charges brought against two Russian nationals, [06/09/2018]. https://www.gov.uk/government/speeches/you-dont-recruit-an-arsonist-to-put-out-a-fire-you-especially-dont-do-that-when-the-fire-is-one-they-caused.

9 Eric Rosenbach and Katherine Mansted, "The Geopolitics of Information," (Belfer Center for Science and International Affairs, Harvard Kennedy School, May 28, 2019), https://www.belfercenter.org/publication/geopolitics-information

10 Barr, L. and Owen, Q. (2022) 'DHS plays defense over Disinformation Governance Board', ABC News, 5 May. Available at: https://abcnews.go.com/Politics/dhs-plays-defense-disinformation-governance-board/story?id=84520182

11 Nina Jankowicz, "The Coming Flood of Disinformation: How Washington Gave Up on the Fight Against Falsehoods," Foreign Affairs, February 7, 2024.

12 Arold, U. (2021). *Põhjala ja Balti riikide psühholoogilise kaitse süsteemide kontseptuaalsed ja praktilised alused* [Master's thesis]. Sisekaitseakadeemia. Available at: https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2698/Arold%2CUku.pdf?sequence=3&isAllowed=y

13 UK Government Communication Service, "RESIST.20: The UK's Counter-Disinformation Framework" https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/

14 In 2021, Belarus opened up multiple flights a day from Baghdad to Minsk and its security forces escorted the migrants to the EU border (Poland, Lithuania, Latvia) on arrival. The aim was to destabilise the security situation within the EU. This event was accompanied by information operations stoking divisions and debates about the EU's ability to control migration and what this might mean for Polish citizens.

15 *Maciej Makulski, Assessment of the Strategic Communication Structure in Poland and its Potential, March 20204* https://www.kew.org.pl/wp-content/uploads/2024/03/Assesment_StratCom-structures-capabilities-FINAL.pdf

THE NATIONAL SECURITY IMPERATIVE FOR THE MODERNISATION OF GOVERNMENT COMMUNICATION STRUCTURES

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy