Tim Hayward
(University of Edinburgh)

Intelligence Agencies' Communications with the Public

https://cdoi.org/1.2/065/000027

Abstract

This article outlines concerns about the involvement of intelligence services in public communications, particularly those aimed at affecting public opinion in their home nation. It differentiates the main kinds of activity, assessing their anticipated benefits and disbenefits both for the agencies and for the public. Section 1 considers the kind of communication intelligence agencies can directly address to a public audience, and finds this is mainly limited to public relations statements on the organisation's own behalf and affirmation of intelligence that governments have already publicised. Section 2 looks at how sometimes positive intelligence is disseminated publicly, as was notably the case as Russian forces gathered on Ukraine's border prior to the 2022 invasion, and sets out reasons for regarding this as necessarily a limited exception rather than the norm. Section 3 examines the rationale for intelligence agencies to coordinate counter-disinformation activities as part of their counterintelligence mission, highlighting the significant coordinated steps that countries in the NATO alliance have taken to support these. It identifies as a central problem that the definition of disinformation operationalised in this work can include true information if that serves an adversary. This does not help the public become better informed. In fact, as shown in Section 4, because counter-disinformation operations allow the subsumption of reasoned dissent under the label of adversarial interference, they arguably constitute a more real, present and rigorously describable danger than is presented by the alleged problem of 'disinformation'. For they are largely unaccountable, often unethical, and sometimes illegal and unconstitutional. In the worst of cases, they can support unjust war and crimes against humanity. Accordingly, there are good reasons for citizens, and certainly for academic researchers, to maintain rigorous critical distance from communications of intelligence provenance.

"fidarsi è bene e non fidarsi è meglio …"
– Vittorio Imbriani

Introduction

The intelligence services have a distinctive and well-established role in a polity. This is to gather intelligence related to national security and other important national interests, which has then to be reported to appropriate state officials. They are also expected to engage as necessary in counter-intelligence activities. For good reasons that are readily accepted by the public, intelligence agencies need to be able to operate in secrecy. Although some kinds of intelligence products which are closer to social scientific research than espionage may be made available to a public audience, like the CIA's World Factbook, informing the public has not traditionally been a major role of the agencies. Yet there is evidence that in recent years they have come to see involvement in certain aspects of public communication as part of their remit. This is certainly the case in UK, where heads of the intelligence services have

addressed themselves directly to the public about their commitment to contribute to public understanding of contemporary affairs.

Part of the explanation for this appears to be the accessibility of open-source materials, made possible by the internet, which can reveal information of kinds traditionally requiring intelligence experts to gather. Certainly, a reason cited by intelligence chiefs for their increasingly public profile is a concern that the public not be misled or confused by unofficial communications. The Head of MI5, for instance, has spoken publicly of his pride at the part the UK's Intelligence Community has been playing 'in calling out disinformation attempts'; and he has expressly signalled that 'extremist influencers' who 'amplify conspiracy theories' come within the purvey of UK's domestic intelligence service (McCallum 2022). The Head of GCHQ, Jeremy Fleming (2022), has similarly expressed a commitment to ensuring that 'disinformation campaigns' that aim to 'cause confusion', 'sow mistrust in information sources', and 'promulgate false narratives' do not succeed. The head of MI6 has even taken to using Twitter as part of an evident campaign to give an impression of public accountability, while reinforcing the specific view – of what should and should not be considered 'disinformation' – that is supported by Western governments. He affirms that a key role of his service is 'to assert and defend Western democratic values.' (Moore 2021) Furthermore, the Head of the British Army, General Sir Nick Carter, has extolled the work of its 77th Brigade which has the core mission of 'combatting disinformation' in an 'information war' (Carter 2018) – a role that notably it performed during the Covid situation (Baker 2020).

To 'counter disinformation', then, is regarded as a core aim. What is potentially problematic about this, however, is that the operational understanding of 'disinformation' does not necessarily coincide with what people would ordinarily assume it to mean, namely, false information. For 'disinformation' can be conveyed by the strategic deployment of selected truths, which means, as a consequence, some truths will be regarded as problematic and in need of 'contextualising'. But how far the intelligence agencies can go in providing 'context' is a question with dimensions of both legitimacy and competence. For the very project of 'countering disinformation' is problematic in several ways I have set out elsewhere,[1] and engagement in it by intelligence agencies adds substantial further layers of concern. If they adopt a role of informing – or even seeking to educate – the public, they do so without a key kind of assurance that is offered by more open forms of communication, namely, checkability. The purpose of intelligence services is to generate knowledge in ways that are not normally replicable by members of the public. It has to be taken on trust. But since we must assume that one of their necessary capabilities is winning the trust of people who they may deceive or betray, the public would be justified in treating their communications with caution.

The discussion of this paper relates to a broad field sometimes referred to as *public diplomacy*, but it is organised around three quite distinct ways in which intelligence activities can involve engagement with the public. The first of these involves heads or representatives of the agencies addressing themselves directly to a public audience. This can be regarded as the most accountable form of engagement, but also the least informative. For as Section 1 notes, their direct communications tend either to involve rather bland PR, or else they echo official statements that government offices have already released into the public domain. Clearly, any such communications are intended to show the agencies in their best light, but their concrete purpose seems to be that of widening their recruitment base rather than using

their distinctive capabilities to enlighten the public in a meaningful way.

Insofar as genuinely new and potentially significant information is imparted to the public by intelligence agencies, this normally comes not direct from the agencies themselves but as mediated in statements from authorised government officials. This mode of public communication is examined in Section 2, where it is noted that when intelligence assessments are quoted, the language used is typically carefully guarded, with words carefully chosen. The affordances of bureaucratic nuance provide appreciable latitude for creative interpretation, or *spin*, in the delivery of selected messages by official spokespersons. This can sometimes just mean emphasising the genuine drift of the intelligence provided, but, when desired, the spin imparted can serve to mislead or deceive. The question of whether political agendas could be at work within the intelligence services themselves is difficult to investigate, but it is of some significance in relation to counter-intelligence operations. For, as argued in Section 3, the possibilities of deception are all the greater when intelligence agencies engage in such activities as 'countering disinformation', purportedly on behalf of the public interest, by using covert operations. In the nature of the case, researching these activities can be difficult, but Section 4 draws on information that has surfaced into the public domain and shows a worrying degree of deceptive activity being conducted or condoned by intelligence agencies not just against designated adversaries or security threats but also against ordinary members of the public. Such activity, which allows the subsumption of reasoned dissent under the label of adversarial interference, might arguably be regarded as a more real, present and rigorously describable danger than that presented by the alleged problem of 'disinformation'. For it certainly affects public understanding, but does so unaccountably, sometimes unethically, and even on occasion illegally and unconstitutionally. In the worst of cases, it supports not the institutions of a democratic state but the agendas of powerful interests which, in pursuit of their ends, are prepared to resort to war and crimes against humanity.

For these reasons, it is affirmed in conclusion that academics who believe in the value of free inquiry should exercise active epistemic diligence with respect to information that reaches the public from quarters that are not themselves open to deliberative evaluation.

1. In their own voice

If members of the intelligence services are to address the public directly, what sort of benefit might the public anticipate could be derived from this? The ostensible role of intelligence services in a modern democracy is to protect its institutions and way of life against attack or subversion. Allegiance to the core values of democracy, including freedom of expression and a free press would be at the heart of that protective mission. Perhaps intelligence communications could enhance public understanding of events in the world, particularly those that posed some threat to the peace and stability of society. Insofar as attempts to undermine democracy might be directed via 'information warfare', there could be a role for the intelligence services in publicly identifying hostile communications. In all these activities, members of the services should be expected to conduct themselves ethically – just as they articulate an aim to do even within the constraints of their more traditional activities of espionage and counter-intelligence.

In principle, then, intelligence services might provide a valuable service of enlightening, informing and educating the public. What also needs to be acknowledged, however, is that this mission is so far removed from their core business as to be potentially at odds with it in important ways. For real education in a free society involves the sharing of readily accessible and in principle checkable knowledge, supporting learners not only to acquire knowledge but also to learn how to generate it themselves; learners should also be able to ask questions, even critical and challenging ones. Yet it is not clear how far intelligence agencies might go towards providing such educative support, even in principle. Their own communicative remit is itself quite narrow and restrictive: it is mainly about matters of national security and specifically on what the public needs to know, in their estimate, primarily in order to 'combat disinformation'. So, before even considering how far one might expect the practice of intelligence activities to live up to the potential claimed for them, one has to be aware of tensions at the level of basic principles that inherently limits that potential. Some of these can be gleaned from the public utterances now emanating from the British intelligence agencies themselves.

The intelligence service chiefs have made clear that they want the public to feel assured of their commitment to having a positive impact on the quality of information available to the public. In recent times, the heads of British spy agencies have taken to the media and social media to engage in Public Relations activities. While doing so they have articulated a commitment to ethics, democracy and the importance of free speech. However, they are rather non-specific about what this might mean. The one area where their messaging is a little more substantial is in relation to their commitment to 'equality and diversity', and here they go into some specifics about their recruitment goals and strategy. It may therefore be that some of this publicity might primarily have the relatively restricted objective of broadening the base of new recruits. This progressive-sounding concern to seem in tune with the society they serve may well be grounded in the operational advantages to an intelligence service of having officials and agents who are able to exercise a wider range of human sympathies and understandings than is available to a narrower cultural spectrum. Spies often need to be able to fit into milieux other than those of people with cultural affiliation to solid establishment circles.

According to the description offered by McLoughlin et al (2020: 236), public engagement is important to the agencies not just for diversity but also for education. Yet the 'educational remit of GCHQ's social media' is apparently fulfilled with

> 'content related to raising awareness of the organisation's activities and role, promoting a particular type of culture, and promoting trust in their functions. For instance, linking the current day organisation to its famous Second World War past at Bletchley Park, or by highlighting positive news stories and officially backed GCHQ media content.' (McLoughlin et al 2020: 241)

More earnest, though, are some of the public proclamations issuing from the top of the intelligence agencies. In particular, we hear that they have ethical principles they are keen to uphold. Indeed, in his first speech as the current Head of MI6, Richard Moore (2020) stated the aim of recruiting only the 'most ethically literate' to the service. On Twitter, he has approved the message of Cecile Fabre's (2022) recent book that 'spies must have an ethical compass', and he has claimed that 'Ethical principles infuse SIS operations, marking our difference from our adversaries.' (Tweet 12 May 2022) The MI6 in-house Ethics Counsellor, reviewing Fabre's book, has similarly claimed that many of those actively working in the UK

intelligence community 'take very seriously the ethical dimensions of their work.' (Anonymous (MI6 Ethics Counsellor) 2022) In fact, the MI6 Ethics Counsellor argues that intelligence has inherent ethical potential:

> 'The better the intelligence, the less the uncertainty and the more likely it is that the decision will be taken on sound moral grounds.' (Anonymous (MI6 Ethics Counsellor) 2022)

Yet appealing as that general proposition may sound, it involves a leap of logic to assume it will always hold in any given situation: for there is no reason why being better informed will necessarily lead to making a more moral decision, since people seek to get informed for all sorts of reasons, including some highly immoral ones. The likelihood of moral vs immoral intent is independent of levels of uncertainty. Also overlooked by the attempt to associate intelligence with ethics is the inconvenient complexity of both knowledge and morality, as well as of the connections between them. In reality – and this is important for sincere public communicators to be aware of – a reduction of uncertainty is not an inevitable outcome of better intelligence. Sometimes better intelligence yields awareness of how a situation is altogether more complex and less certain than one might have imagined. Conversely, a very real problem that concerned citizens are alert to is the oversimplification imposed through narratives promulgated as 'official stories' (see Hayward 2022b). There is thus an argument that the public might be better served by spy agencies sticking to the job of conveying awareness of the deeper intelligence to those authorised to act on it, rather than by supporting the public promulgation of superficial narratives that may serve political interests. It is not as if the intelligence agencies are at liberty to publicise intelligence that contradicts government statements. So in this context, however ethically serious individual members of the intelligence community may be, they are not necessarily in a position to do what they might believe morality would require. The very fact that they are provided with ethics counsellors serves to remind us that given the broader character of their work they must face hard choices which may inevitably involve some compromise of principle. So, the intelligence agencies are just not in a position to pronounce openly on what morality requires.

This is a point that bears also on the public pronouncements by intelligence service chiefs about democracy and the importance to it of free speech and a free press. Such sentiments flow readily from the Twitter feed of the head of MI6:

> 'Freedom of press and expression is the cornerstone of a functioning democracy.'

> 'Freedom of expression is the foundation of democracy'.

> 'Freedom of press and access to a range of views are crucial in a democracy.'

Yet, worthy as these statements in themselves are, the cast of mind actually operative in these utterances of them is glimpsed in Moore's response to a tweet from a non-Brit who tells him "we don't want your democracy":

> 'Not my democracy. Democratic standards represent universal values. Don't you want those?' (Moore 2016)

What is revealed by this glib rejoinder is the occupational inability of a secret services chief to accept that a specific meaning of democracy as understood by a representative of a seat of colonial power, and especially when it claims universality, can be contested. At a stroke, his tweet reveals the hollowness of professed commitments about a range of views being crucial

in a democracy. It signals that the range is strictly delimited and not up for discussion.

Not up for discussion, either, is whatever spin on intelligence a government might choose to impose or what is to count as disinformation. This is evident from examples the secret service chiefs offer when mentioning their fight against it. So, for example, Richard Moore has cited these instances of 'disinformation':

> 'the Kremlin has been using disinformation campaigns around the chemical weapons attack in Douma and the assassination attempt in Salisbury. The Salisbury attack saw the UK become the focus of a sustained disinformation campaign that saw over 30 different conspiracy theories sown by the Russian State directly or through its proxies.' (Moore 2018)

What is interesting here is how alleging disinformation from others displaces a commitment to providing actual information. Moore will be well aware that members of the public have articulated serious questions about what is actually known of the events both in Douma and in Salisbury. Allegations of disinformation serve to deflect attention from questions about the UK's own accounts of them. Since the Head of MI6 is not going to say anything to contradict his government, he accordingly must choose his words and their focus with due care. He implies that to question the UK's version of the events is to impart disinformation: he implies this by referring to unspecified 'disinformation campaigns' used by the Kremlin. Yet even if we accept that Russia did make statements that muddied the waters around these events, it would involve a leap of logic to infer from this that the UK version of these events is necessarily reliable. For no matter how many 'conspiracy theories' might be attributed to Russia, or anyone else for that matter, their number has no bearing on the question that the domestic public has an interest in knowing, namely, what really happened and how it can be decided that the official story of the UK is the most reliable one. Attentive members of the public have noticed that the puzzling Skripal story has undergone a number of revisions and plot twists, with big questions left unanswered (McKeigue et al 2018); they know that the Douma story has been challenged, from within the very organisation responsible for publishing the official account, by scientists directly involved in the investigation informing it (Hayward 2019b).

A further disconcerting consideration, though, is that intelligence service chiefs seem simply to have a low opinion of the intelligence of ordinary members of the public. For instance, when Ken McCallum, Head of MI5, was speaking in 2022 of his pride in the part the UK has been playing 'in calling out disinformation attempts', he added a mention of 'recent Russian public statements pointed at the UK which', he says, 'include silly claims, such as alleging UK involvement in attacking the Nord Stream pipelines' (McCallum 2022). For although such speculative claims about the US's ally might well be mistaken, there is enough information available to the public through other channels to show that they are no sillier than attempts to suggest Russia blew up its own pipeline (Cooper 2023). All McCallum has shown here to an attentive citizen is that ensuring deference to the official position is an obligation of the secret services in any public utterance they make. This fact alone suffices to show why critics believe the involvement of spy agencies in the sphere of public communications should be minimised or eliminated, not expanded.

It falls to the MI6 Ethics Counsellor, when reviewing Fabre's rather sanguine assumptions about spies' commitment to ethical values, to make explicit the bottom line: 'intelligence agencies are tasked to defend the national interest for its own sake, against others who do not share the same values. … ultimately, we have to know which side we are on and what we are

prepared to fight for.' (Anonymous (MI6 Ethics Counsellor) 2022) This non-negotiable commitment of the intelligence and security services to defend their government's position cuts very bluntly through any debate about ethical and epistemological matters: what is right or true is never going to be publicly declared by those services to be the contrary of what the government declares to be so. The authority that the services recognize as binding on them is political, not epistemic or ethical.

Thus, the point that has so far been established is that when speaking in their own voice, representatives of the intelligence services say little that would help a citizen work out who to trust in this era of distinctive epistemic challenges.

2. Publicly quoted intelligence outputs

There are, of course, well established limitations in principle on how much intelligence can be publicly shared and reasons why confidentiality is the norm. But even where intelligence is publicised, it is normally delivered in mediated fashion: what to share of reports is decided by officials under constraints imposed by government. For this reason, there is always some selection involved; and selectivity facilitates the inherent possibility of spin. This is the case even when officials are scrupulous in avoiding false statements, for spin allows the conveying of a favoured message that is not clearly supported by the raw intelligence. Sometimes spin can shade into outright deception. An example of this that has remained in the public mind was the false allegation of weapons of mass destruction in the 'dodgy dossier' which were referred to as justification for the invasion of Iraq in 2003. A lot of public debate since has polarised around the question whether this was a terrible exception to a rule of more general probity caused by a particular US administration, which was then restored by the new presidency of 2008 – a position widely argued by liberal internationalists (see Hayward 2019a, 176–7) – or whether it was indicative of a more deep-seated problem of elements with bipartisan influence ready repeatedly to manipulate public opinion in support of the wars the US has continued to be involved in post-2008. Whatever one's view on that particular debate, one can appreciate that any political decision – whether to share or withhold intelligence – will have some political motivation. What this means is that sometimes intelligence may be distorted for political reasons, while other times the faithful communication of reliable intelligence might itself serve a political purpose. From this it follows that bad experiences from the past do not necessarily mean that public communications of intelligence can never be trusted again; but it also means that if reliable communications are released on a certain occasion, this is not necessarily any precedent for the reliability of communications on subsequent occasions. Hence the central claim here is that we should always be alert to the political context of the release.

A notable example of a success referred to in the current literature is the highly publicised intelligence that provided a 'running commentary on Russia's growing threat to Ukraine from November 2021' and predicted the invasion that was to take place in February 2022 (Dylan and Maguire 2022, 34). During that period, many neutral commentators had been sceptical about the claim of an imminent invasion, and critical commentators had been inclined to dismiss it as symptomatic of the generally hostile and sometimes alarmist Western accusations against Russia. Yet the prediction proved accurate. Also to be noted is that this

came with a rather unusual – indeed, quite unprecedented – degree of exposure of intelligence. This was an 'intriguing development' which itself 'provoked a number of commentators – from journalists to former security practitioners – to remark on its originality.' (Dylan and Maguire 2022, 34) We should, however, be mindful of the reasons why it was also relatively unusual in relaying quite substantial positive intelligence, and especially in doing so in real time. For there are not only reasons why publicising intelligence at all is normally avoided, but also reasons why positive intelligence is less likely to be publicised than counterintelligence alerts about adversaries' disinformation. By appreciating these reasons for its relative rarity, one can then understand why this particular case might be regarded as exceptional rather than typical.

The reasons why publicising intelligence is generally avoided altogether are many. For there are numerous ways in which it risks being counter-productive: it can expose sources, which may be harmful for them and render them unusable for accessing further information; it can warn adversaries about what is known and enable them to prepare a response; it can consequently be self-defeating in serving to avert what it predicts – which can also bring reputational damage to the agency for its falsified prediction; and even if that particular consequence does not ensue, there remains the risk that if the intelligence proves in any way at all to be mistaken, this can be used to discredit the competence and reputation of the issuing agency. In short, publicising valuable intelligence is a high stakes activity – and much more so, as we shall shortly discuss, than is quoting intelligence sources for the purpose of criticising the disinformation of an adversary.

Evidently, then, in the run-up to the Russia-Ukraine war, the stakes for the Western allies were deemed high. A clear and convincing intelligence victory would serve two significant strategic objectives in the information war with Russia. For one thing, if the West's intelligence was to have a reputation for credibility as events developed, then establishing this would require shifting the public perception that had remained influential since flawed intelligence reports had been used to justify the popularly-resisted invasion of Iraq in 2003. A conspicuous success would go a significant way to achieving that, and would help carry allies and publics with them in the anticipated contest with Russia. The UK Joint Intelligence Committee (JIC) launched a process, in parallel with US counterparts, whereby intelligence outputs were prepared for external consumption:

> 'Given memories of the politicisation and costs suffered in the Iraq War episode, rigorous procedures were used to assess the deployment of intelligence as quickly as possible, to the point where – according to one British intelligence insider – "highly classified material would be on his desk one day and then emerge in the public domain the next".' (Dylan and Maguire 2022, 55)

So, evident care was taken to get it right, and the success was widely aired in the media, attracting affirmative comment from within academia too. But as well as the strategic objective of burnishing the agencies' reputation, a second was that of incriminating the adversary.

This second strategic communication objective involved establishing not only that the invasion was unjustified, which few would dispute, but also that it was *unprovoked*. This is a significant claim given that there are commentators who, while accepting that the invasion was unjustified – both in international law and morally – regard the question of provocation as a quite distinct one, and not so clear cut. Against a backdrop of fighting inside Ukraine that had already caused more than 50,000 casualties and more than 14,000 deaths in the eight

years before the 2022 invasion, the 'unprovoked' claim is met by a contrasting view, as notably argued by John Mearsheimer (Chotiner 2022). He maintains that the fighting within Ukraine could have been ended, and the risk of war with Russia averted, if there had been implementation of the 2015 Minsk agreement, which would have guaranteed Ukraine's neutrality and non-accession to NATO. For it was the prospect of Ukraine joining NATO that Russia had consistently referred to as an 'existential threat' that they would respond to. Although this reference to what Russia perceived as provocation could not justify the invasion, it did have the potential to sway public opinion towards accepting a view that an early settlement of the conflict involving some approximation to what had already been agreed to in the Minsk accords might be justified. This was evidently not a view endorsed by foreign policy makers in the West, who accordingly sought to keep public attention on the more immediate fact of Russian aggression. So, the view reported by the BBC, for instance, was that 'the unprecedented outpouring of intelligence … made it much easier for other countries to rally round tougher measures than if there had been a confused and disputed picture of who was the real aggressor.' (Corera 2022) On that view, the assessment was that 'publicising this material robbed Moscow of the ability to justify the invasion to its own people and other countries as a defensive move.' (Corera 2022)

In order to maintain this perception, however, the case against 'appeasing' the aggressor by allowing negotiations had still to be maintained, even in the face of the inevitable horrors of continuing the war. So, the active management of public communications remained an imperative. Ukraine itself was early credited by Western observers with conducting an outstanding strategic communications campaign (Ryan et al 2022). Western officials said that 'while they cannot independently verify much of the information that Kyiv puts out about the evolving battlefield situation, including casualty figures for both sides, it nonetheless represents highly effective stratcom.' (Ryan et al 2022) A senior NATO official told the Washington Post of the impressive media, information, and psychological operations involved, while articulating the 'hope Western countries take their lead from them.' (Ryan et al 2022). Particularly in the weeks immediately following the invasion, considerable discipline was exercised in the Western media to amplify anti-Russian messaging. The very suggestion that the public should hear more than one side of the story was stamped on by the mainstream press and even denounced in the UK parliament (Hayward 2022c). Russian reporting was condemned even when it was accurate, while false reports from the Ukrainian side were glossed over. The standards applied to public intelligence communications in the West were now notably relaxed with multiple officials acknowledging that the US, for instance, had 'used information as a weapon even when confidence in the accuracy of the information wasn't high … about things that are possible rather than truly likely.' (Dilanian et al 2022).

In these communications, the emphasis was placed on 'debunking' and 'pre-bunking' Russian disinformation. That is to say, there was a certain shift from publishing positive intelligence, as had been the case in the specific instance of the Russian military build-up prior to the invasion, to criticising the adversary's *disinformation*. The ratio of benefits to costs of this negative messaging for the intelligence agencies and their principals was more reliably favourable than attempting to keep ahead with the provision of positive intelligence under the conditions of confusion and uncertainty that inevitably prevail across war zones.

However, insofar as debunking enemy claims still involves appealing to evidence, there

remains a certain risk of rebuttal. This is particularly significant now that so much material can be uploaded online from war zones where intelligence actors themselves may not have access. Open-source intelligence (OSINT) is now recognized as a major factor in any information war. As state and mainstream monopolies of control over information flows have eroded, non-state third parties, including OSINT investigators like Bellingcat, 'have been gaining greater capabilities to independently collect, analyse and disclose publicly available and commercial information on state actions, including a range of overt and covert influence activities, thereby imposing their own incrimination costs.' (Dylan and Maguire 2022, 44) A rational response to this situation, for governments and intelligence agencies, is to partner with, rather than compete against, such investigative groups. Hence, we find governments providing funding to groups like Bellingcat, and officials in turn sometimes leaning on their work (Dylan and Maguire 2022, 54–55). Notwithstanding their usefulness, however, it is also rational to allow such groups to remain formally independent, especially given the complication that sometimes communications that serve the national interest may not be the most truthful ones. Accordingly, if such groups are to be relied on to serve the national interest, then they need to be at arm's length from government to allow for deniability if and when their own outputs are debunked. For a risk indicated in a report commissioned by the UK Foreign and Commonwealth Office was that Bellingcat, for instance, was not rated highly for either independence or integrity and in fact 'was somewhat discredited, both by spreading disinformation itself, and by being willing to produce reports for anyone willing to pay.' (Expose 2018, 71–2).

For the most part, nonetheless, this arrangement can work rather well from the officials' point of view; and with the support of a cooperative press corps, the official narrative can be maintained across most or all of mainstream media. The view that anything Russia says is presumptively disinformation has acquired traction in the Western public consciousness. Even in academia, the presumption widely prevails that giving either epistemological or ethical credit to the Russian perspective in any matter at all is not appropriate when it differs from the official Western perspective. In this way, consent continues to be satisfactorily manufactured.

Accordingly, what the MI6 ethics counsellor reminds us is the primary objective of the intelligence services, namely, to defend the national interest, is thereby fulfilled. But this means that certain important kinds of question about where the national interest lies, and how it relates to other perceptions of the public interest, can go unheeded. Worse, they may be viewed as hostile.

3. Organised public influence

Intelligence agencies' work involves not only gathering intelligence but also engaging in counter-intelligence. This can involve a variety of activities and objectives, but increasingly today an important dimension of the 'hybrid thread' to be countered is what they designate as *disinformation*. 'Countering disinformation' has become a high-level strategic goal throughout the West. In this section, accordingly, I outline how counter-disinformation activities are understood as part of a counterintelligence strategy, showing then why this has come to include the subsumption of reasoned dissent under the label of adversarial

interference.

To begin with, one needs to understand the working definition of 'disinformation' as adopted by those guided by a strategic goal of countering it. The matter, they consistently argue, is not a simple one. Daniel Hinšt summarises why:

> 'Disinformation is much more than just false information. It would be easy to argue that the world's history, as well as social, and especially political, relations have been full of false information and lies. That way, the geopolitical problem of modern-day disinformation could easily be relativized and even ignored. In fact, the goal of actors behind disinformation is to undermine and relativize liberal democratic institutions of the transatlantic world and its democratic allies. The analytical approach toward disinformation requires deep understanding of the context, political risks and the motives of actors. While fake news and false information can be relatively easily debunked, disinformation requires stronger and more systematic analytical efforts to detect and reduce the risks of promoting massive false dilemmas, often combined with populist narratives, conspiracy theories, public apathy and hostile intelligence influence from authoritarian powers.' (Hinšt 2021: 89-90)

The risks associated with disinformation, on this view, are extensive and potentially grave, even if they are somewhat underdefined. We are told that disinformation can confuse public communication, manipulate perceptions of reality, exacerbate political polarization, intensify social conflict and promote distrust in democratic political institutions (Hinšt 2021: 90). A general worry is that its dissemination can lead toward 'ideological authoritarianism and "deep state" narratives' which can 'undercut democratic processes and erode confidence in institutions like the EU and the NATO' (Hinšt 2021: 95) On this view of disinformation, then, it is regarded as a threat to the legitimacy and security of the institutions which are held to provide the necessary support for maintaining democracy. For this reason, an argument figuring prominently in public communications, and also in some academic publications, is that the risks associated with disinformation are such as to require a response coordinated at national and international levels.

Accordingly, to support this response, we have seen the establishment of Centres of Excellence in Europe, including the NATO Counter Intelligence Centre of Excellence in Poland and the European Centre of Excellence for Countering Hybrid Threats in Finland under the auspices of the EU and NATO. These complement the work of the Strategic Communications Center of Excellence (StratCom COE) established in Latvia in 2014. StratCom COE is a NATO-accredited military organization, which, according to Nina Jankowicz, 'informs and equips NATO to be more effective in fighting disinformation, with a secondary mission of building public awareness about the tools and tactics of Russia and other malign actors in the transatlantic space.' (Jankowicz 2019) Additionally, Polyakova and Fried (2019) recommend the creation of a transatlantic Counter-Disinformation Coalition to bring together relevant governments and social media companies to share insights into how to disrupt foreign influence operations. Similarly, the U.S. Senate Committee on Foreign Relations has argued for a coalition to 'build awareness of and resilience to the Kremlin's malign influence operations' and for the Organization for Security and Co-operation in Europe (OSCE) to serve as a forum for exposing disinformation attacks (Committee on Foreign Relations, 2018: 159). In the US, where the Global Engagement Center coordinates counter-disinformation activities, ostensibly against foreign sources, there has also been a call for 'a new US inter-agency 'Centre to Counter Foreign Malign Influence' that would counter influence operations not just abroad but at home too (Murphy 2022). In fact, in 2021, 'one of the Biden

administration's first priorities was to unveil a National Strategy for Countering Domestic Terrorism. It described the loss of faith in government and extreme polarisation as "fuelled by a crisis of disinformation and misinformation often channelled through social media platforms".' (Cook 2023) Within the UK, a new inter-departmental unit, the Government Information Cell, was set up in February 2022 'to counter Russian narratives; to expose Russian fabrications and actions through ongoing "pre-bunking"; and to boost the morale of Ukraine's government, military and civilians.' (Dylan and Maguire 2022, 55) The cell draws on expertise in analysis, communications, disinformation and behavioural science by being 'built on an existing strategic-communications capability to counter hostile narratives through the Counter Disinformation Unit in the Department for Digital, Culture, Media and Sport (originally formed to tackle COVID-19 disinformation), the Home Office's counter-terrorism-focused Research, Information and Communications Unit, and the British Army's 77th Brigade.' (Dylan and Maguire 2022, 56)

Given this very substantial commitment of the Western powers to 'countering disinformation', it is clearly important to try and understand what kinds of activity it may involve. Central among the general objectives of their activities are detecting and disrupting 'foreign influence' operations. To*detect* such operations, a 'basic need is the development of the requisite expertise to be able to identify and monitor adversary information operations.' (Helmus and Kepe 2021) To this end, some recommend 'that the intelligence community establish formal and informal relationships with social media platforms; doing so could enable more-effective sharing of threat information.' (Helmus and Kepe 2021) States can 'distribute intelligence through independent, controlled or notional non-state intermediaries – who themselves may constitute initial targets of influence – to more indirectly reach ultimate target audiences through more authentic, credible, secure or deniable channels. These might be a trusted or controlled journalist or editor, a sympathetic civil-society organisation or political party, or a fabricated front website or social-media account.' (Dylan and Maguire 2022: 38-39) In order to*disrupt* foreign influence, a substantive strategy is to disseminate intelligence that serves to 'expose, embarrass or "call out" an adversary, or occasionally an ally, for its past, present or anticipated actions, intentions or even beliefs.' (Dylan and Maguire 2022, 42)

Something to underscore here is how the label of foreign interference has come to be applied to domestic dissent. In the US, at the end of 2016, just before leaving office, President Obama signed into law the Countering Foreign Propaganda and Disinformation Act, 'which used the language of defending the homeland to launch an open-ended, offensive information war.' (Siegel 2023) 'Disinformation' was now officially regarded as an existential threat from the perspective of national security, and one which justified restricting rights and liberties of citizens in response: government insiders were quoted as arguing 'that laws written to protect U.S. citizens from state spying were jeopardizing national security.' (Siegel 2023) In UK, a similar process has been underway. Although, officially, operations of information warfare are targeted only at foreign, not domestic, actors, the untenability of maintaining this distinction in operations is revealed in the very logic of the perceived online threat itself: if online actors can post from anywhere in the world, disguising their location and identity, then any attempt to counter their activities could not assuredly distinguish foreign from domestic actors.

This situation gives rise to concerns about the risk of undermining the practices and

institutions of a representative democracy. The question as to whether democratic rights are more effectively protected by strong measures against corrosive effects of hostile or dissident opinion or by allowing open deliberation to facilitate public reasoning about the contentious matters is clearly an important one. Moreover, in a democracy, it is also of practical importance how an answer to that question is decided.

In order to provide safeguards against unacceptable infringements of citizens' rights, one would expect, at the least, adequate democratic oversight over the intelligence services and appropriate accountability in their organisation. Yet given that 'disinformation' is itself such a slippery concept, identifying a clear and workable role for intelligence agencies in relation to a war against it could never be straightforward. Insofar as intelligence agencies are expected to advise governments on the basis of accurate factual claims, they cannot on the same basis warn against disinformation which actually consists of carefully selected factual claims: the required work of interpretation might be attempted, but at the risk of sacrificing accuracy. Running such a risk can threaten an agency's reputation. It is therefore understandable that this work has effectively been outsourced via the kind of organisational arrangements referred to in the previous section. This enables specialists in psychological operations, information operations and public diplomacy to develop particular 'counter-disinformation' programmes that have the backing of governments while, in terms of accountability, being kept at arms' length. Thus, some of this work is done quite openly, as evidenced by the existence of the Centres of Excellence mentioned, and the burgeoning array of think tanks and funded university research into all aspects of 'disinformation'. But some of the coordination is covert. For although the authorised messaging can be well-supported and effective, it is nevertheless vulnerable to challenge from dissident perspectives. Dissidents who simply highlight inconveniently true information may be perceived as a threat from the security perspective, and one which cannot be met by means of simply relaying sound intelligence. So, although the counter-intelligence imperative is to act against that dissent, the reputational risk of being seen to uphold untruth creates a contrary imperative. A solution is to have the necessary work done covertly, and with deniability.

But what appears as a solution from that security perspective is a problem from the perspective of a conception of democracy that takes the rights and freedoms of citizens to be fundamental to it. For enhancing the deniability of intelligence agencies' operations takes them still further from effective democratic oversight.

4. Covert management of dissent

This section illustrates how, in the implementation of the agencies' evident strategic objectives, adverse effects on the institutions of democracy and the rights of citizens can be real and serious. The *detection* of disinformation can be unreliable, for reasons that follow directly from the mentioned incoherence in the conceptualisation of it; and *disrupting* the activities of those unreliably accused of it can be unethical, anti-democratic and sometimes illegal.

In the contemporary context, although the detection and disruption of disinformation are acknowledged aims of the official intelligence agencies, the work involved is not necessarily done by them. Indeed, due to its self-contradictory features, as noted, they have an evident

incentive to outsource it. It happens that, as Dylan and Maguire point out, the intelligence services lean on organisations like Bellingcat to do work of kinds not traditionally done by their own agencies. If this new work simply involved a certain kind of expertise that is routinely required, there is no obvious reason why the resources of the state could not be applied directly to acquiring and deploying it; but in the context of an information war, an evident rationale is that it provides a deniable method of framing inconveniently true information – or even just inconvenient questioning (Adamo and Joner 2023) – as 'disinformation'.

It is interesting to note that the outsourcing of intelligence activities figured prominently in the efforts to detect and disrupt alleged disinformation concerning those very events of early 2018 that were publicly singled out by intelligence chiefs as significant cases of it. Certainly, the poisoning of the Skripals in Salisbury and the alleged chemical attack in Douma were both of notable political import, yet the official story in each case left a number of critical questions unanswered and appeared self-contradictory in important respects (McKeigue et al 2018; McKeigue et al 2020). We now know that citizens who highlighted these flaws at the time in social media were being monitored by a covert government-funded programme run by the Institute for Statecraft (IfS): this came to light with the release of some IoS documents that had apparently been hacked (Coburg 2019). The IfS is a shadowy organisation registered at an abandoned mill in Scotland, which, while falsely declared as a charity (Briggs 2019), was running a counter-disinformation operation from Temple Place in London under the eyes of MI6 (Elmaazi and Blumenthal 2018; Klarenberg 2019). As it happens, its tracking of 'pro-Kremlin troll accounts' included identifying as relevant a retweet of a tweet of mine. This is worth mentioning because the tweet itself commended the BBC's Eddie Mair for raising a critical question about the Salisbury incident:

> 'All credit to BBC's @eddiemair for asking whether Skripal "Novichok" poison was just "of a type developed by Russia" or actually made there. Answer seems to be nobody knows. Neither Porton Down nor FCO have said.'

Evidently, a British citizen relaying a comment by a well-known British BBC broadcaster was regarded by the troll trackers as a matter relevant to include in monitoring, paid for by the British Government, of 'foreign influence'. This demonstrates that what is categorised as presumptive 'Russian disinformation' does not necessarily originate from Russia. The question Mair asked had originally been raised by former British Ambassador Craig Murray, who was alert to the careful choice of words from his long experience working as a senior civil servant.

Nevertheless, the findings of this monitoring were presented to mainstream media outlets in the form of a narrative about the tracked users being bots, trolls or 'useful idiots' for the Kremlin which, according to the narrative, was generating multiple conspiracy theories so as to confuse the public and undermine trust in the government. Uncritical news outlets then cited these findings to warn the public about the 'Russian disinformation campaign'. The shaky basis of these attributions, however, was apparent to alert members of the public even at the time. In fact, certain critically attentive members of the public found themselves being the ones fingered as 'Russian bots'. They included the world-renowned concert pianist Valentina Lisitsa, the well-known vlogger Maram Susli, and Ian Shilling, a British citizen from Hastings, who was brought onto Sky News to address a bizarre accusation: "Are you a Bot?" (MacLeod 2021) This farcical situation highlighted both the lack

of methodological competence in the counter-disinformation research and the uncritical subservience of the media.

If the detection of disinformation has been predictably unreliable, also of concern are some of the tactics used to *disrupt* its alleged promotion. For instance, in the period immediately following that monitoring of social media, journalists identified in the Integrity Initiative documents published high profile attacks on academics who had publicly raised questions about the Skripals and Douma incidents. As one of those academics, I was astonished at the time, since in my own case, nothing more than my quoting of a tweet had been taken to merit front page attention in The Times, then amplified across other news outlets (Hayward 2018). The only possible news value I could discern in this lay in the deterrent message it conveyed to any others who might be tempted to voice public dissent. Yet the hostile attention towards the group continued in sections of the press (Hayward 2022a; Robinson 2022), including at the hand of an individual named Chris York who authored no less than twelve attacks on the group for HuffPost (Johnstone 2020). As whistleblowers came forward from within the OPCW to cast more decisive doubt on the official Douma story, the BBC joined in the attack (Maté 2020). Interestingly, key interviewees relied on by the BBC were individuals named in leaked documents submitted to FCO by its contractors in the field of strategic communications (Klarenberg 2021), notably, Alistair Harris, director of the company ARK, who was credited with 'playing the media like the fiddle' by Norton (2020). Then, during the intense information campaign around the Russian invasion of Ukraine in 2022, The Times (OII 2022) and the BBC (Klarenberg and Miller 2022b) were again at the forefront of mainstream attacks on dissenting opinion. The BBC journalist centrally concerned was subsequently revealed to have been copied into emails about a plan aimed at discrediting 'rogue academics' who were advocating hearing more than the one side of the story that intelligence-linked groups were pressing (Klarenberg and Miller 2022a). The emails show this plot was coordinated by the journalist Paul Mason, the interviewee who was given the final word on the BBC broadcast (Hayward 2022d).

The influence of covert security agendas over the free circulation of public information is not limited to disruption of inconvenient questioning, however. Something that came to light in the leaked documentation about Integrity Initiative was that some of its personnel had close association with operations that were not only monitoring others' information but also planting false stories. Kit Klarenberg (2018) shows that covert operations known about by intelligence agencies were involved in producing the dossier containing the now discredited 'Russiagate' allegations used in an evident attempt to prevent the 2016 election of President Trump. In this context it is interesting to note the British security state issued the press with a D(SMA) notice – i.e. "do not report" advice – against revealing that Sergei Skripal's MI6 handler had been Pablo Miller. Miller worked for the private intelligence company of his former MI6 colleague Christopher Steele who was responsible for the imaginative dossier at the centre of the Russiagate affair (Coburg 2018b). If Skripal had been involved in the dossier's production but his discretion had come into doubt, that could have been a motive for his poisoning, according to what former senior civil servants and whistleblowers Craig Murray and Clive Ponting surmise on the basis of their first-hand experience of how the British government and intelligence services work (Murray 2018; Ponting 2018). This is simply educated guesswork, of course. What we do know is that there is not certain knowledge in the public domain of what really did happen.

Political interference was also a concern in the UK, where the Integrity Initiative was found to have engaged in activities to undermine the candidacy of Jeremy Corbyn for prime minister (Curtis 2018). Although this could not be officially condoned by the government, it was done with their funding (Coburg 2018b). In fact, it was part of a broader intelligence-coordinated smear campaign against the Labour leader, with the purpose, according to the evidence presented by Matt Kennard (2019), of ensuring that he did not attain power within the British state. The position of the intelligence services on this matter had in fact been made explicit by the former Head of MI6: on the eve of the 2015 general election, Sir Richard Dearlove published a vehement article in *The Daily Telegraph* declaring that Jeremy Corbyn was 'unfit for the office' because he represented 'a clear and present danger to the country' and would not even pass the security services' vetting procedures, let alone be trusted to lead the country – so his election 'would put the intelligence services in a very difficult position.' (Dearlove 2017) The military, too, were said to take this view, according to The Times, which in 2015 reported that a serving general had warned 'there would be a direct challenge from the army and mass resignations if Corbyn became prime minister' (Shipman et al 2015). This view was very well publicised, with at least 34 major media stories depicting Jeremy Corbyn as a danger to British security (Kennard 2019), and with service chiefs reportedly threatening that Corbyn would receive only "restricted access" to intelligence if he persisted in policy views they disagreed with (Shipman et al 2015).

This issue brings into stark relief the question of who exactly the intelligence agencies serve or answer to. In principle, they serve the nation and answer to its elected representatives; in practice, they appear as conduits of an effective power to define the national interest that neither the electorate nor even parliament have any control over. Who they answer to in reality is not easy to determine. For notwithstanding the public relations efforts of intelligence chiefs to associate their services with ideas of transparency and democratic accountability, they have been found rather desultory in reporting to the UK Parliament's Intelligence and Security Committee which is charged with their oversight. Moreover, its 2021-22 report further found that a whole raft of additional intelligence activities aimed at influencing public opinion have been devolved to new government policy units which are not even included in the oversight arrangements (ISC 2022).

Lack of accountability applies also in regard to the British Army's Information Warfare Team which is a group within the 77th Brigade that is responsible for psychological and information operations (British Army website). According to the Secretary of State for Defence, 'the 77th Brigade's role is to challenge disinformation, not opinion', (Ben Wallace in Hansard, 2023) but no clarification is published about how it defines or operationalises that elusive distinction. Wallace says the unit is on the lookout 'for media manipulation of misinformation or lies from abroad', and yet no mention is made of how it addresses the challenge of attributing nationality to posts on the worldwide web. In fact, a whistleblower from the unit exposes the disingenuity of the official position:

> 'To skirt the legal difficulties of a military unit monitoring domestic dissent, the view was that unless a profile explicitly stated their real name and nationality they could be a foreign agent and were fair game. But it is quite obvious that our activities resulted in the monitoring of the UK population' (Anonymous (ex-77th Brigade officer) 2023).

According to the minister, the brigade's role 'is not to monitor or counter opinion', and yet the whistleblower testifies that this is exactly what it was doing – monitoring posts which

'did not contain information that was untrue or co-ordinated'. The whistleblower says 'the banner of disinformation was a guise under which the British military was being deployed to monitor and flag our own concerned citizens. … It was about domestic perception, not national security.' The 77th Brigade, according to investigations by Iain Cobain, 'uses social media platforms such as Twitter, Instagram and Facebook, as well as podcasts, data analysis and audience research to conduct what the head of the UK military, General Nick Carter, describes as "information warfare".' (Cobain 2019)

As well as monitoring social media users, the security services have also exercised significant influence over the social media platforms themselves. For instance, Twitter's top editorial adviser on the Middle East Gordon MacMillan was at the same time serving as a captain in the 77th Brigade; and the 'global threat intelligence lead' at Facebook, Ben Nimmo, is a former NATO press officer who had meanwhile been responsible for the monitoring of social media accounts referring to the Skripals and Douma incidents discussed above (Macleod 2021). More generally, there appears to be a revolving door and close working relations between the Western intelligence community and the social media companies. The extent of intelligence infiltration has more recently been illustrated with the release of the Twitter Files, which revealed a 'hidden partnership between state intelligence services, Silicon Valley, and traditional media, to manipulate the national conversation in the US - as well as much of the rest of the world' restricting what could be said on social media platforms – with the purpose 'not to prevent a crime or enforce laws, or even for the public good, but to tightly control political discourse to marginalise serious criticism of the establishment.' (Cook 2023) Under pressure from intelligence agencies, social networks were apparently drawing up secret blacklists so as to limit the reach of certain accounts or to stop certain topics trending. Even eminent experts were targeted if they challenged key establishment narratives (Magness and Waught 2022).

A particularly significant disclosure from the Twitter Files was that social media and state security agencies played a role in suppressing a story published in the New York Times, weeks before the 2020 presidential election, about Hunter Biden's laptop. The laptop was alleged to contain evidence of problematic ties between the Biden family and foreign officials in Ukraine (Cavallier 2022). The story was immediately declared to be Russian disinformation: this was the headline in a Politico article which implied the claim had the support of 50 former intelligence officials, including five CIA chiefs, who had signed a letter casting doubt on the authenticity of the story (Nathasha Bertrand 2020). And although that letter chose its words carefully, it was cited by Biden and his supporters as establishing that the story was 'disinformation from the Russians'. However a careful reading of the letter shows that the publicised interpretation involved misrepresentation of what was in reality a speculative suggestion, based on no evidence at all (see e.g. Kessler 2023). Meanwhile, ample evidence has been produced to show that the story was a genuine one. In fact, the FBI had known this even before the story became public. Yet it appears 'they manipulated the media, including social networks, into assuming that any story harming Biden before the election was Russian disinformation.' (Cook 2023) Pressure was exerted by the intelligence community on social media platforms like Twitter and Facebook to block the story so it would not widely circulate in the run-up to the election.

This episode can be contrasted with the approach of the intelligence community and the media with regard to the allegations made against Trump in the so-called Russiagate scandal.

During the 2016 presidential election, Russia was said to have colluded with candidate Trump and assisted him by weaponising social media to sow discord and manipulate the US electorate. To account for Putin's alleged leverage over Trump, material was cited from that imaginative dossier compiled by former MI6 officer and FBI informant Christopher Steele (Haynes 2019). This was accepted as genuine with little attempt to verify it in the media, and yet, as critical voices warned at the time (Maté 2023) and was later confirmed by the Mueller Inquiry (ABA 2019), it was a fabrication. Meanwhile, supposed evidence of the alleged manipulative social media activity was being produced by the Hamilton 68 Dashboard, whose claims to have uncovered a Russian influence campaign were routinely cited in the media and think tank publications. The methodology of Hamilton 68 was somewhat opaque, but its deployment and results were very comparable to those of the Integrity Initiative. Indeed, some of the same personnel were involved, and notably Ben Nimmo, who has been influential throughout this sector. His career as a 'counter-disinformation expert', already prior to becoming head of Global Threat Intelligence at Facebook, spanned positions as NATO Press Officer, advisor to Bellingcat, researcher for Integrity Initiative, director of Grafika, and founding member of DFRLab, which has partnered the Alliance for Securing Democracy (ASD), the organisation responsible for the 'Hamilton 68 Dashboard'. These organisations, and other similar ones, have been 'shown to have spread false charges of foreign disinformation' according to Margot Cleveland, and Twitter itself is said to have discerned that the entire methodology was flawed (Cleveland 2023a). Certainly, it does not stand up to critical scrutiny: serious criticisms of the Hamilton 68 methodology had early on been set out in written evidence to the UK Parliament by M C McGrath (2018); its opacity and circularity were also criticised by Olivier Jutel (2019). But the flawed methodology is itself just a symptom of the more fundamental problem.

The fundamental problem is that because the 'disinformation' to be countered is messaging that suits the purposes of an adversary rather than those of the agency's client or principal, it is sometimes just inconveniently true information. Since inconveniently true information cannot successfully be countered by simply engaging in the forthright dissemination of reliable intelligence, agents determined to counter it must resort to strategies that closely resemble those attributed to alleged purveyors of disinformation. Indeed, all the strategies analytically identified by counter-disinformation experts as available to adversaries can equally be deployed by their own side.

In an information war, truth is not necessarily the primary weapon. Nor is truth inevitably the outcome. More typically, truth is the first casualty.

But information wars can also be fought in contexts where there are real human casualties too. The intelligence services and the practices of deception that go into creating disinformation and counter disinformation are of military origin. The goal of participants in warfare, including information warfare, is dominance, not truth. Take the recent sabotage of the Nord Stream 2 pipeline as an illustration: after initial attempts in the media to blame Russia were dropped, the countries with a declared interest in disrupting its exportation of gas blocked a proposed UN-led inquiry into the matter (UN 2023). Or take the earlier cited example of the crime in Douma, where some 43 people died with apparent symptoms of a nerve agent. In this case, OPCW inspectors are striving to fulfil their responsibilities under the internationally agreed Chemical Weapons Convention by seeking to establish the truth of what happened. Yet they are being blocked by OPCW's US-approved management, with the

public support of US and allies at the United Nations, and by maintenance of a misleading one-sided narrative in the mainstream media (Hayward 2019b).

There is no evident public interest justification for blocking full inquiry into the truth of such events. The only discernible rationale is to cover up serious crimes. In the Nord Stream case, the crime was destruction of vital infrastructure. In the Douma case, where investigation of 43 murders was hindered, if allegations of Syrian government responsibility were shown to be unfounded, that would make the retaliatory bombing action by US, UK and France on 14 April 2018 unjustified, and thus a war crime. The covering up of serious crime cannot generally be considered to be in the public interest.

The regrettable truth, however, is that history is replete with instances of the intelligence agencies' privilege of secrecy being abused to cover official complicity in – and sometimes even instigation of – egregious crimes. This privilege is guarded jealously, as is starkly signalled by the treatment being meted out to the founder of Wikileaks, Julian Assange (Maurizi 2022; Melzer 2022). There may be little that any of us can individually do about this, but what academics can aim to do – as a collective with a vocation of scholarship in service of the search for reliable knowledge and understanding – is what I have elsewhere argued (Hayward 2019c) we should regard as a professional obligation to do, namely: be alert to how we may be deceived; be sure not to reproduce deceptive claims; and be prepared to stand with those who challenge deception, especially when they are attacked for doing so.

Conclusion

This article has outlined reasons for caution about forming unrealistic expectations of openness and frankness in public communications by members of the intelligence services; it has further shown reasons to be wary of spin when intelligence is made public; and it has emphasised especial concern about the involvement of intelligence agencies in counter disinformation operations. For however much their public statements may extol the virtues of transparency, democracy and a free press, their practices can do a great deal to undermine those very things. Their core purpose is to serve the security interests of the state, and this would include, if the state is a democratic one, protecting the institutions of democracy. But an appropriate understanding of what threatens democratic institutions and what undermines them cannot be left to security agencies to decide. The normative framework within which intelligence agencies legitimately operate has to be set by democratically elected representatives of the citizens. That framework has to be underwritten at the level of the constitution, and the legislature has to ensure that there are robust arrangements for effective oversight of the intelligence services.

In situations where oversight is not as robust or effective as in an ideal democracy it would be, and where the intelligence services may effectively be under political or corporate influence, then it is arguable that there is a civic right and even a duty – derivable from the basic rationale of a democratic constitution – to seek to hold them to account, just as politicians and corporate actors properly would also be. Certainly, the more that intelligence agencies involve themselves in information warfare in social media, supporting authoritarian strategies of cognitive infiltration and behavioural influence, the more compelling is the need for citizens to defend their rights of free expression and association.

Realistically, of course, holding to account agencies that have the power of state and corporate partners behind them, and whose privilege of secrecy is protected by the strongest of laws, would be in many ways an unequal struggle. But in one important respect the strength is on democratic citizens' side, and it is one where academics can potentially provide vital support: when 'counter-disinformation' operations mounted on behalf of states and their corporate partners deploy a conception of 'disinformation' that is inherently incoherent, and insofar as their communications involve ignoring factual information, manipulating evidence or defying logic, this can be revealed by those minded to reveal it. For the investigative norms and principles inherent in scholarship provide a firm basis on which to stand in support of open and honest inquiry.

---

[1] In Hayward (forthcoming) I show that the term 'disinformation' can refer to different problems, depending whether the user adopts an epistemic, behavioural or security framing. Policy-makers may accordingly be influenced by contradictory advice so that measures taken to correct one problem can exacerbate another. Insofar as intelligence agencies prioritise the security framing, their view of 'disinformation' is liable to be incoherent when judged by epistemic criteria.

Bibliography

- ABA (American Bar Association). 2019. 'Mueller finds no collusion with Russia, leaves obstruction question open', 25 March: https://www.americanbar.org/news/abanews/aba-news-archives/2019/03/mueller-concludes-investigation/
- Adamo, Thomas and Joner, Josiah. 2023. 'Stanford's Dark Hand in Twitter Censorship', The Stanford Review, 24 March: https://stanfordreview.org/stanfords-dark-hand-in-twitter-censorship/
- Anonymous (ex-77th Brigade officer). 2023. 'This snooping was wrong, it hangs over my proud Army career like a black cloud', in 'Army spied on lockdown critics', by Glen Owen, MailOnline, 28 January: https://www.dailymail.co.uk/news/article-11687675/Army-spied-lockdown-critics-Sceptics-including-Peter-Hitchens-suspected-watched.html
- Anonymous (MI6 Ethics Counsellor). 2022. 'Inherently despicable? Why spying agencies must prove they have a moral compass', TLS, 13 May: Anonymous (MI6 Ethics Counsellor) 2022
- Baker, Berry. 2020. 'UK Chief of Defence Staff participates in daily coronavirus briefing', Army Technology, 23 April: https://www.army-technology.com/news/uk-chief-of-defence-staff-participates-in-daily-coronavirus-briefing/
- Bertrand, Natasha. 2020. 'Hunter Biden story is Russian disinfo, dozens of former intel officials say', Politico, 19 October: https://www.politico.com/news/2020/10/19/hunter-biden-story-russian-disinfo-430276
- Briggs, Billy. 2019. 'Scottish charity watchdog damns group that attacked integrity of politicians', The Ferret, 5 November: https://theferret.scot/charity-statecraft-integrity-corbyn/
- Carter, Nick. 2018. 'Dynamic security threats and the British Army', speech to The Royal United Services Institute, 22 January: https://www.gov.uk/government/speeches/dynamic-security-threats-and-the-british-army-chief-of-the-general-staff-general-sir-nicholas-carter-kcb-cbe-dso-adc-gen
- Cavallier, Andrea. 2022. 'US diplomat in Kiev sent classified email in 2016 warning that Hunter Biden's business dealings in Ukraine 'undercut the anti-corruption message' his VP father was advancing', MailOnline 4 February: https://www.dailymail.co.uk/news/article-10475335/Former-diplomat-Kiev-warned-State-Department-Hunter-Bidens-business-dealing-Ukraine.html
- Chotiner, Isaac. 2022. 'John Mearsheimer on Putin's Ambitions After Nine Months of War', The New Yorker, 17 November: https://www.newyorker.com/news/q-and-a/john-mearsheimer-on-putins-ambitions-after-nine-months-of-war
- Cleveland, Margot. 2023a. 'Meet The Partisans Who Wove The Censorship Complex's Vast And Tangled Web', The Federalist, 28 February: https://thefederalist.com/2023/02/28/meet-the-partisans-who-wove-the-censorship-complexs-vast-and-tangled-web/
- Cleveland, Margot. 2023b. '"Twitter Files" Show More Groups Used Hamilton 68's Bogus Methodology To Sell The Russia Hoax', The Federalist, 6 March: https://thefederalist.com/2023/03/06/twitter-files-show-more-groups-used-hamilton-68s-bogus-methodology-to-sell-the-russia-hoax/
- Cobain, Ian. 2019. 'Twitter executive for Middle East is British Army 'psyops' soldier', Middle East Eye, 30 September: https://www.middleeasteye.net/news/twitter-executive-also-part-time-officer-uk-army-psychological-warfare-unit
- Coburg, Tom. 2018. 'Despite government censorship, a far bigger story behind the Skripal poisoning isemerging',Canary,1June:https://www.thecanary.co/global/world-analysis/2018/06/01/despite-government-censorship-a-far-bigger-story-behind-the-skripal-poisoning-is-emerging/
- Coburg, Tom. 2018b. 'Emily Thornberry turns up the heat on Tory minister in row over Jeremy Corbyn smears', Canary: https://www.thecanary.co/uk/analysis/2018/12/14/emily-thornberry-

turns-up-the-heat-on-tory-minister-in-row-over-jeremy-corbyn-smears/

- Coburg, Tom. 2019. 'A government-funded destabilisation network is forced to disable its own website', Canary, 28 January: https://www.thecanary.co/uk/analysis/2019/01/28/a-government-funded-destabilisation-network-is-forced-to-disable-its-own-website/
- Committee on Foreign Relations Committee. 2018. Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security. US Government Publishing Office: https://www.govinfo.gov/content/pkg/CPRT-115SPRT28110/pdf/CPRT-115SPRT28110.pdf
- Cook, Jonathan. 2023. 'How social networks became a 'subsidiary' of the FBI and CIA', Middle East Eye, 20 February: https://www.middleeasteye.net/big-story/twitter-files-social-networks-subsidiary-fbi-cia-how
- Cooper, Charlie. 2023. 'Who blew up Nord Stream?' Politico, 8 March: https://www.politico.eu/article/vladimir-putin-kremlin-russia-who-blew-up-nord-stream-2/
- Corera, Gordon. 2022. 'Ukraine: Inside the spies' attempts to stop the war', BBC News, 9 April: https://www.bbc.co.uk/news/world-europe-61044063
- Curtis, Mark. 2018. 'Twitter and the smearing of Corbyn and Assange: A research note on the "Integrity Initiative"', Mark Curtis blog, 28 December: http://markcurtis.info/2018/12/28/twitter-and-the-smearing-of-corbyn-and-assange-a-research-note-on-the-integrity-initiative/
- Dearlove, Richard. 2017. 'Jeremy Corbyn is a danger to this nation. At MI6, which I once led, he wouldn't clear the security vetting', The Telegraph, 17 June: https://www.telegraph.co.uk/news/2017/06/07/jeremy-corbyn-danger-nation-mi6-led-wouldnt-clear-security-vetting/
- Dilanian, Ken et al. 2022. 'In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid', NBC News, 6 April: https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014
- Dylan, Huw and Thomas J. Maguire. 2022. 'Secret Intelligence and Public Diplomacy in the Ukraine War', Survival, 64(4): 33-74. DOI: 10.1080/00396338.2022.2103257
- Elmaazi, Mohamed and Max Blumenthal. 2018. 'Inside the temple of covert propaganda: The Integrity Initiative and the UK's scandalous information war', Grayzone, 17 December: https://thegrayzone.com/2018/12/17/inside-the-temple-of-covert-propaganda-the-integrity-initiative-and-the-uks-scandalous-information-war/
- Expose Network. 2018. Upskilling to Upscale: Unleashing the Capacity of Civil Society to Counter Disinformation, confidential report to UK FCO. Available at: https://wikispooks.com/wiki/Document:Upskilling_to_Upscale:_Unleashing_the_Capacity_of_Civil_Society_to_Counter_Disinformation
- Fabre, Cécile. 2022. Spying Through a Glass Darkly: the ethics of espionage and counter-intelligence. Oxford University Press.
- Fleming, Jeremy. 2022. 'The head of GCHQ says Vladimir Putin is losing the information war in Ukraine', interview in The Economist, 18 August: https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine
- Hansard. 2023. 'Oral Answers to Questions Volume 729: debated on Monday 13 March 2023', UK Government: https://hansard.parliament.uk/Commons/2023-03-13/debates/59F6F12A-7C38-4DD2-BAB0-30208E8D3F7B/OralAnswersToQuestions
- Haynes, Deborah. 2019. '"Trump hater" ex-MI6 officer who compiled Russia dossier was a friend of Ivanka', SkyNews, 10 December: https://news.sky.com/story/trump-hater-ex-mi6-officer-who-helped-compile-russia-dossier-was-a-friend-of-ivanka-11882732
- Hayward, Tim. 2018. 'Attacked by the Times', Wordpress blog, 14 April: https://timhayward.wordpress.com/2018/04/14/attacked-by-the-times/

- Hayward, Tim. 2019a. Global Justice and Finance. Oxford University Press.
- Hayward, Tim. 2019b. 'Media coverage of OPCW whistleblower revelations', Wordpress blog, 24 October: https://timhayward.wordpress.com/2019/10/24/media-coverage-of-opcw-whistleblower-revelations/
- Hayward, Tim. 2019c. 'Three Duties of Epistemic Diligence', Journal of Social Philosophy, 50(4): 536-561. https://onlinelibrary.wiley.com/doi/10.1111/josp.12319
- Hayward, Tim. 2022a. 'WGSPM: timeline of hostile media coverage', Wordpress page: https://timhayward.wordpress.com/syria/working-group-in-the-press/wgspm-timeline-of-hostile-media-coverage/
- Hayward, Tim. 2022b. 'Questioning the official story about official stories: a role for citizen investigations', Propaganda in Focus, 11 December: https://propagandainfocus.com/questioning-the-official-story-about-official-stories-a-role-for-citizen-investigations/
- Hayward, Tim. 2022c. 'A UK Crackdown on Academic Freedom?' Wordpress blog: https://timhayward.wordpress.com/2022/03/18/a-uk-crackdown-on-academic-freedom/
- Hayward, Tim. 2022d. 'Whose Disinformation is it Anyway? BBC Vs Critical Academics', Propaganda in Focus: https://propagandainfocus.com/whose-disinformation-is-it-anyway-bbc-vs-critical-academics/
- Hayward, Tim. Unpublished. 'The Problem of Disinformation' (copy available on request from author)
- Helmus, Todd C. and Kepe. 2021. A Compendium of Recommendations for Countering Russian and Other State-Sponsored Propaganda. Research report for Rand Corporation.
- Hinšt, Daniel. 2021. 'Disinformation as Geopolitical Risk for Transatlantic Institutions,' International Studies, Libertas International University, 21(2): 89-111.
- ISC (Intelligence and Security Committee of Parliament). 2022. Annual Report 2021-22. UK Parliament: https://isc.independent.gov.uk/wp-content/uploads/2022/12/ISC-Annual-Report-2021–2022.pdf
- Jankowicz, Nina. 2019. Avoiding the Band-Aid Effect in Institutional Responses to Disinformation and Hybrid Threats. Policy paper for the German Marshall Fund: https://www.gmfus.org/news/avoiding-band-aid-effect-institutional-responses-disinformation-and-hybrid-threats
- Johnstone, Caitlin. 2020. 'Nobody Sets Out To Become A War Propagandist. It Just Sort Of Happens', Consortium News, 31 January: https://consortiumnews.com/2020/01/31/nobody-sets-out-to-become-a-war-propagandist-it-just-sort-of-happens/
- Jutel, Olivier. 2019. 'Civility, Subversion and Technocratic Class Consciousness: Reconstituting Truth in the Journalistic Field', in R. Overell and B. Nicholls (eds) Post-Truth and the Mediation of Reality, Palgrave Macmillan: 177-202
- Kennard, Matt. 2019. 'How the UK Military and Intelligence Establishment is Working to Stop Jeremy Corbyn Becoming Prime Minister', Declassified UK, 4 December: https://declassifieduk.org/how-the-uk-military-and-intelligence-establishment-is-working-to-stop-jeremy-corbyn-becoming-prime-minister/
- Kessler, Glenn. 2023. 'The Hunter Biden laptop and claims of "Russian disinfo"', The Washington Post, 13 February: https://www.washingtonpost.com/politics/2023/02/13/hunter-biden-laptop-claims-russian-disinfo/
- Klarenberg, Kit. 2018. 'Close Associate: The Integrity Initiative's Intimate Connections to "RussiaGate"', Sputnik, 18 January: https://web.archive.org/web/20190118201120/https://sputniknews.com/europe/201901181071610324-russiagate-integrity-initiative-wood/
- Klarenberg, Kit. 2019. 'Integrity Initiative: Psyops Institute Defanged, But British Spies' Disinfo War Still Rages', Medium.com, 30 December: https://medium.com/@KitKlarenberg/integrity-initiative-

psyops-institute-defanged-but-british-spies-disinfo-war-still-rages-a15bfe433c94

- Klarenberg, Kit. 2021. 'Questions about BBC producer's ties to UK intelligence follow "Mayday" White Helmets whitewash', Grayzone, 7 April: https://thegrayzone.com/2021/04/07/bbc-white-helmets-mayday-uk-intelligence/
- Klarenberg, Kit and David Miller. 2022a. 'British security state collaborator Paul Mason's war on 'rogue academics' exposed', Grayzone, 21 June: https://thegrayzone.com/2022/06/21/british-security-state-collaborator-paul-masons-war-on-rogue-academics-exposed/
- Klarenberg, Kit and David Miller. 2022b. 'BBC assault on antiwar academics was apparent product of UK intel plot', Grayzone, 21 August: https://thegrayzone.com/2022/08/21/bbc-antiwar-academics-uk-intel/
- MacLeod, Alan. 2021. 'Facebook hires NATO press officer Ben Nimmo as intelligence chief', Mint Press News, 9 February: https://www.mintpressnews.com/censorship-way-facebook-hires-nato-press-officer-intelligence-chief/275154/
- Magness, Phillip W. and David Waugh. 2022. 'Twitter Files Confirm Censorship of the Great Barrington Declaration', Independent Institute, 10 December: https://www.independent.org/news/article.asp?id=14366
- Maté, Aaron. 2020. 'Questions for BBC on new White Helmets podcast series attacking OPCW whistleblowers', Grayzone, 30 November: https://thegrayzone.com/2020/11/30/questions-bbc-podcast-opcw-whistleblowers/
- Maté, Aaron. 2023. Cold War, Hot War: How Russiagate Created Chaos from Washington to Ukraine. OR Books.
- Maurizi, Stefania. 2022. Secret Power: Wikileaks and its enemies. London: Pluto Press.
- McCallum, Ken. 2022. 'Annual Threat Update', MI5, 16 November: https://www.mi5.gov.uk/news/director-general-ken-mccallum-gives-annual-threat-update
- McGrath, M. C. 2018. Written evidence submitted to UK Parliament: https://committees.parliament.uk/writtenevidence/88837/pdf/
- McKeigue, Paul, David Miller and Piers Robinson. 2018. 'Briefing Note: Update on the Salisbury Poisonings', Working Group on Syria, Propaganda and Media: https://syriapropagandamedia.org/working-papers/briefing-note-update-on-the-salisbury-poisonings
- McKeigue, Paul, David Miller and Piers Robinson. 2020. 'Update on the OPCW's investigation of the Douma incident', Working Group on Syria, Propaganda and Media: https://syriapropagandamedia.org/update-on-the-opcws-investigation-of-the-douma-incident
- McLoughlin, Liam, Stephen Ward and Daniel W. B. Lomas. 2020. '"Hello, world": GCHQ, Twitter and social media engagement, Intelligence and National Security', 35(2): 233-251, DOI: 10.1080/02684527.2020.1713434
- Melzer, Nils. 2022. The Trial of Julian Assange: A Story of Persecution. Verso Books.
- Moore, Richard. 2016. Tweet: https://twitter.com/ChiefMI6/status/704062288681111552?s=20&t=w2wKQnEx2aLN2hUu0-a8Vg
- Moore, Richard. 2018. 'You're not entitled to your own facts', Foreign, Commonwealth & Development Office, 3 May: https://blogs.fcdo.gov.uk/richardmoore/2018/05/03/youre-not-entitled-to-your-own-facts/
- Moore, Richard. 2020. 'Human Intelligence in the Digital Age', Secret Intelligence Service MI6: https://www.sis.gov.uk/richard-moore-first-public-speech.html
- Moore, Richard. 2021. Interview: 'We ask "C": how do intelligence services need to change in the 21st century?' The Economist, 9 December: https://www.economist.com/podcasts/2021/12/09/we-ask-c-how-do-intelligence-services-need-to-change-in-the-21st-century

- Murphy, Brian. 2022. 'The US Needs a Center to Counter Foreign Malign Influence at Home', Defense One, 20 March: https://www.defenseone.com/ideas/2022/03/us-needs-center-counter-foreign-malign-influence-home/363366/
- Murray, Craig. 2018. 'Probable Western Responsibility for Skripal Poisoning', Craig Murray Blog, 28 April: https://www.craigmurray.org.uk/archives/2018/04/probable-western-responsibility-for-skripal-poisoning/
- Norton, Ben. 2020. 'Leaked docs expose massive Syria propaganda operation waged by Western govt contractors and media', Grayzone, 23 September: https://thegrayzone.com/2020/09/23/syria-leaks-uk-contractors-opposition-media/
- OII (Oxford Internet Institute). 2022. Press Release: 'University of Edinburgh academic Tim Hayward accused of spreading propaganda': https://demtech.oii.ox.ac.uk/press-university-of-edinburgh-academic-tim-hayward-accused-of-spreading-propaganda/
- Polyakova, Alina and Daniel Fried. 2019. 'Democratic Defense Against Disinformation 2.0', Atlantic Council, 13 June: https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/
- Ponting, Clive. 2018. Comment on Craig Murray Blog, 22 April: https://www.craigmurray.org.uk/archives/2018/04/senior-civil-servants-still-deeply-sceptical-of-russian-responsibility-for-skripal-poisoning/comment-page-5/#comment-742324
- Robinson, Piers. 2022. 'Democracies and War Propaganda in the 21st Century', Working Group on Syria, Propaganda and Media: https://syriapropagandamedia.org/working-papers-2/democracies-and-war-propaganda-in-the-21st-century
- Ryan, Missy et al. 2022. 'Outmatched in military might, Ukraine has excelled in the information war', The Washington Post, 16 March: https://www.washingtonpost.com/national-security/2022/03/16/ukraine-zelensky-information-war/
- Shipman, Tim, Sean Rayment, Richard Kerbaj and James Lyons. 2015. 'Corbyn hit by mutiny on airstrikes; Half of shadow cabinet back Syria actionSecurity services to deny Corbyn information on live operations', The Times, 20 September: https://www.thetimes.co.uk/article/corbyn-hit-by-mutiny-on-airstrikes-wgrvzpt30ld
- Siegel, Jacob. 2023. 'A Guide to Understanding the Hoax of the Century: Thirteen ways of looking at disinformation', The Tablet, 29 March: https://www.tabletmag.com/sections/news/articles/guide-understanding-hoax-century-thirteen-ways-looking-disinformation
- UN (United Nations). 2023.'Security Council Rejects Draft Resolution Establishing Commission to Investigate Sabotage of Nord Stream Pipeline', SC/15243, 27 March: https://press.un.org/en/2023/sc15243.doc.htm