DOI:
10.1080/00396338.2022.2103257

Document Version
Peer reviewed version

The Ukraine War: A Public Crucible for Secret Intelligence

Huw Dylan and Thomas J. Maguire

Abstract

Intelligence is generally collected and utilised in secret to inform internal audiences. But during the build-up to Russia's invasion of Ukraine, and during the early stages of the war, Britain and the US deployed intelligence in public extensively to influence external audiences. They used national assets, both to warn of Russia's hostile intent and in an attempt to deter Russia from invading. This article argues that while this was a significant evolutionary step in how governments use intelligence assets, it was built upon a longer historical legacy. It examines why states chose to use intelligence for influencing external audiences, what they aim to achieve by doing so, the uses and dangers of publicising secret information, and how the use of intelligence during the Ukraine crisis fits into broader historical trends. It concludes that while use of intelligence in public is to be welcomed it is not a policy without risk.

Authors

Dr Huw Dylan, is a Senior Lecturer in Intelligence and International Security at the Department of War Studies, King's College London.

Dr. Thomas J. Maguire is an Assistant Professor of Intelligence and Security in the Institute of Security and Global Affairs, Leiden University, and Visiting Fellow with the King's Intelligence and Security Group in the Department of War Studies, King's College London.

Word count

Full: 9006

Text minus endnotes: 7184

The Ukraine War: A Public Crucible for Secret Intelligence

The shock of Russia's invasion of Ukraine on 20 February was palpable, but few could have claimed to have been truly surprised. Leading NATO powers had been publicly and privately warning of such an event for several months, even going so far as to suggest the likely date of invasion. Government spokespersons explained that it was unlikely to occur sooner because Russian President Vladimir Putin would have been reluctant to unleash his forces whilst the Beijing Winter Olympics were ongoing, thereby detracting attention from his close Chinese ally Xi Jinping's exercise in soft power.[1] Indeed, citing a 'Western intelligence report', journalists were subsequently briefed confidentially that the Chinese government had allegedly requested no invasion until the end of the Games.[2] Nevertheless, within and without Ukraine's borders, many found it difficult to comprehend that large scale conventional warfare could return to Europe in 2022 and chose to downplay the threat.[3] Many others, no doubt, remembered the warnings of 'intelligence' on Iraqi weapons of mass destruction in 2002 and 2003 and assumed that this was another example of ambiguous Western intelligence being spun and broadcast for political ends.

But, no. The warnings were accurate. Intelligence analysts frequently struggle to discern intentions from capabilities. But on the borders of Ukraine there was little ambiguity. Why would field hospitals, bridging units, spare ammunition and sundry other combat enablers be mobilised on such a scale for a bluff?[4] And Vladimir Putin's view of Ukraine, and his willingness to use violence towards his neighbour have been clear for years. Having assessed the likelihood of invasion correctly, NATO member intelligence

communities are now monitoring the progress of Russian forces with relative ease, given the difficulty of hiding massed armour movements from various aviation, space, and social media platforms. Yet estimating Putin's intentions, as was the case with his Cold War predecessors in the Kremlin, remains far more challenging.[5] So far, so familiar for observers of strategic intelligence.

However, the Russo-Ukrainian War has been accompanied by an intriguing development in terms of intelligence, the increasingly frequent use of intelligence in the public domain by policymakers, particularly in Washington and London. Not only was there a running commentary on Russia's growing threat to Ukraine from November 2021, featuring processed imagery intelligence (IMINT) of its military build-up along Ukraine's border and strategic assessments of Russian plans to invade.[6] But there were also frequent allusions to Russian efforts to covertly subvert the government in Kyiv, to false flag operations seeking to provide Moscow with a legitimate pretext for military action, to disinformation in support of these operations, and to Russian post-invasion plans to target prospective Ukrainian dissidents and install pliant leaders.[7]

Whilst frequent references have been made to American use of intelligence in the UN General Assembly during the Cuban Missile Crisis in 1962 and in the build-up to the 2003 Iraq War, this public use of intelligence has provoked a number of commentators – from journalists to former security practitioners – to remark on its originality.[8] Certainly, the scope, vigour, and frequency of intelligence dissemination to external audiences to support policy – reaching its peak between mid-January and mid-February – the very public nature of this, and the pre-emptive manner of using intelligence this way to deter

or undermine an adversary or ally's potential future actions have been remarkably novel in the modern history of international statecraft.

Yet few things are new under the sun are new. This has been an evolutionary rather than revolutionary development. What we have witnessed forms part of long-standing patterns. We tend to understand the primary purpose of intelligence as something secret, produced to inform *internal* consumers within governments for decision and operational advantage. Less well understood, however, is an established track record of states also deploying intelligence to influence *external* audiences. Indeed, states have at times collected and processed intelligence specifically for this purpose. London and Washington's intelligence-led revelations and claims about Russian actions and intentions are not even novel within their recent relations with Moscow. Compared to fairly limited public exposures and attributions of Russian unacknowledged actions in Crimea and Eastern Ukraine in 2014, these revelations form part of an ongoing campaign – starting with the US Intelligence Community's January 2017 public attribution of Russian interference in the 2016 US elections[9] – to use intelligence to more readily call out unacknowledged Russian (as well as Chinese, Iranian, and North Korean) intelligence collection, political influence, and coercive activities.[10] While such public attribution has been a political and diplomatic decision by elected national leaders, it has been informed by intelligence assessment.

Public intelligence and intelligence as influence

To understand what is taking place during the Russo-Ukrainian War, we need to unpack the interlinked concepts of 'intelligence as influence' and 'using intelligence in public'. First, when evaluating what intelligence is being disseminated, we need to differentiate between 'raw' intelligence (such as a satellite image, intercepted communications audio, or social media post), 'finished' intelligence (such as a report assessing such raw sources), and 'intelligence-led' communications (such as statements of findings based on underlying intelligence assessments). This is not simply an exercise in ensuring we are all talking about the same thing. The granularity of intelligence disseminated has implications for the potential gains and costs of doing so. Illuminating this point, for instance, is the case of the US and Iran. The US has publicised sanitised satellite images of Iranian nuclear power plants in controlled circumstances, but an unplanned release of a more high-spec image by then President Donald Trump raised concerns, and much hand wringing, about revealing advanced capabilities.[11]

Ahead of Russia's invasion of Ukraine, with the exception of verifiable satellite IMINT and confidential briefings of intelligence to trusted journalists, most 'intelligence releases' by London and Washington have fallen into the final category of high-level, highly sanitised intelligence-led communications. These have been deployed in accessible formats at briefing lecterns and online, including on social media through the likes of UK Defence Intelligence's daily 'intelligence update' on Russian military progress, with the intent of being widely disseminated and viewed.[12] In the UK's case, these have been frequently but not always adorned with language such as 'we judge it be highly likely'[13], guided by a centralised intelligence assessment 'probability yardstick' to regulate the communication of confidence and certainty.[14] It used to be unusual to have

such formal assessment language so widely reported in public. Over the past five years, it has become increasingly common place.

Next, we need to differentiate between, first, intelligence that state disseminators consider to be an accurate and reliable snapshot or assessment; second, intelligence they have purposefully collected, collated, and/or spun with the primary goal of influencing external audiences; and, third, intelligence they have purposefully fabricated to support an act of disinformation to confuse or deceive audiences. In all three categories, the disseminating body is trading off the power of 'intelligence' as something that is perceived to provide unique insights. During the ongoing crisis, all three have been in play: the first two from London and Washington through their confidential briefings and social media updates; the latter from Moscow, with their false-flag operations and fraudulent claims of evidence that a neo-Nazi Ukrainian regime has been committing a genocide against Russian-speakers and has designs on nuclear weapons.[15]

The Kremlin's comfort with trafficking fabricated intelligence reflects a well-established track record. At the height of the Cold War, as part of their so-called active measures, the KGB and its Soviet bloc allies frequently disseminated forged intelligence to sympathetic leaders in the Global South that claimed to expose the nefarious activities of Western services like the CIA in their countries.[16] More recently, the Russian state disseminated fabricated intelligence following the downing of Malaysian Airlines flight MH17 over Ukraine with the aim of diverting the blame for that outrage from itself.[17] This has continued during the current conflict, with the Kremlin claiming to have documents from captured Ukrainian public health laboratories exposing (erroneously)

US Pentagon-funded 'secret biological experiments' with plague, cholera, and anthrax.[18] Their actual role since 2005 has been to support disease control and prevention, including during the COVID-19 pandemic. But this fits into decades-old Russian uses of fabricated intelligence for disinformation portraying the US government as a bioweapons proliferator since the Korean War, disinformation that itself has been called out by NATO and EU members as a pretext for Russia deploying its own chemical weapons against Ukrainian targets.[19]

Additionally, we need to understand the methods states employ to use intelligence for influence. Broadly speaking, there are three main types, all of which have been at play during the current crisis. Firstly, public dissemination of intelligence to target audiences in an attributed manner, i.e., where the government source is clear, with senior policymakers, civil servants, or security practitioners directly divulging intelligence. Not only has this been a prominent feature of the Ukraine crisis, but it also has recent historical precedents in not only the aforementioned Anglo-American campaign to expose covert adversarial activities but also several other cases. The UK government, for example, published the assessment of its Joint Intelligence Committee (JIC) regarding the use of chemical weapons in Syria's civil war in 2013, something the US government also did following the chemical weapons attack in Douma, Syria, in April 2018.[20] Similarly, in February 2021 the US government published a sanitised version of its intelligence community's judgement concerning the culpability of the Saudi state in the murder of dissident journalist Jamal Khashoggi in Istanbul in 2018.[21]

Second, states privately disseminate intelligence to more focused target audiences – state and non-state partners and proxies – as part of wider clandestine intelligence-sharing channels and networks. The US government did this, for example, during the Cuban Missile Crisis, sharing intelligence with allies on growing Soviet nuclear capabilities in Cuba in order to gain public support for its naval 'quarantine' of the island.[22] These targets can also include adversaries or belligerent parties in a dispute or conflict. Former Acting Director and Deputy Director, CIA, John McLaughlin, was occasionally sent to Moscow to relay messages based on classified intelligence, protecting sources and methods whilst letting them 'know that you knew'.[23] In November 2021, CIA Director William Burns followed in McLaughlin's footsteps, privately meeting with President Putin to convey both the gravity of the US's concerns but also its intelligence-based understanding of Russian movements.[24]

Third, states also privately 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, and/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. Dover and Goodman's *Spinning Intelligence* highlights the symbiotic relationship between intelligence communities and the media in this regard, each gaining something from the relationship.[25] Controlled or sympathetic media assets, for example, have been valuable for intelligence agencies 'surfacing' not only narratives but also authentic, spun, and fabricated intelligence, whether to encourage the idea that the US military secretly manufactured the HIV/AIDS

virus, to expose sensitive and embarrassing personal communications of election candidates through so-called 'hack and leak' operations, or during the current Russo-Ukraine War to support the Kremlin's false flag disinformation.[26] The permeability of the membrane between the secret and the open world offers many opportunities for politicians to use intelligence creatively in their statecraft.

Tinker, Tailor, Soldier, Incriminator

As well as the how, we need to consider the why, the motive. There are four main reasons why states use intelligence for influence, publicly or privately. The first, 'support gains', uses intelligence to justify one's own actions, either before or after they occur. This practice has a long history. In 1927, reacting to criticism of a police raid on the Soviet trade mission in London – the notorious ARCOS raid – that had found little evidence to justify the action, British Prime Minister Stanley Baldwin went before Parliament. The motive for the raid, he announced, and for his government's intention to take the major step of breaking diplomatic relations with the Soviet Union, was Soviet espionage and subversion in the UK. While the raid had not been fruitful, Baldwin and his ministers quoted selected decrypted Soviet telegrams as evidence of these activities, later published in a public White Paper, as their only means of proving their charge.[27]

More recently, to gain support for the American-led invasion of Iraq in 2003, London and especially Washington made such justificatory use of intelligence pre-emptively rather than post-hoc. Documents and dossiers detailing British and American

intelligence communities' judgements about Iraqi leader Saddam Hussein's alleged weapons of mass destruction (WMD) programme and connections to the Al Qaeda perpetrators of 9/11 were released to much fanfare. Secretary of State Colin Powell presented this intelligence to the United Nations Security Council with Director of Central Intelligence George Tenet sat behind him. Both elements sought to show domestic and international audiences the intelligence analysis supposedly underpinning the policymaking process.[28] In both cases, the perceived power of intelligence was put to work to persuade.

The second motive, 'action gains', sees governments deploy intelligence to sway or persuade the decision-making, actions, or even worldview of partners and proxies – be they state or non-state – to their benefit and to an adversary's cost. Cooperating with allies through the likes of intelligence-sharing is not merely an act of solidarity or support but also a channel for influencing everything from strategic priorities to operational targeting of adversarial embassies, terrorist groups, or dissidents. As noted above, this has typically been done in private to focus on the target of persuasion and control for adversarial adaptation costs when more public exposure is not desired. Over a century ago, during the famous Zimmerman Telegram case, Prime Minister David Lloyd George's British government did just this to help persuade President Woodrow Wilson's American government to enter the war in 1917. At the heart of this gambit was the private sharing with US representatives of an incriminating decrypted communication between German Foreign Minister Arthur Zimmerman and Germany's embassy in Mexico City, proposing support for Mexican territorial claims in the US in exchange for Mexican entry into the war. Britain took careful measures to control for adaptation costs in order to enable

Wilson's government to later publish the telegram as part of an exposure of German hostility and campaign to persuade the American public on the need to enter the war.[29]

There have been numerous cases of intelligence deployed for such action gains since. To persuade more allies like Prime Minister Jean Chrétien's Canadian government and President Jacques Chirac's French government to adopt more forceful positions at the UN and even join the invasion of Iraq, George Bush's administration lobbied them – unsuccessfully – using the intelligence analysis it claimed supported their case.[30] At times during the post-9/11 conflict in Afghanistan, the US government and CIA sought to carefully use intelligence to pressure Pakistan's Inter-Services Intelligence to cease their covert support for the Afghan Taliban.[31] But as the Cuban Missile Crisis and the use of intelligence during the current Russo-Ukrainian crisis highlight, sometimes states seek to influence their allies through a mix of public and private intelligence dissemination. This has been the case with Israel's use of intelligence to lobby key stakeholders – in particular President Donald Trump's former administration – against the signing, adherence to, and renewal of the Iran nuclear deal.[32] The Trump administration itself used similar tactics to pressure the UK government and other European allies away from adopting Chinese telecommunications company Huawei's equipment in their next-generation 5G networks.[33] And the British government pursued such public-private intelligence dissemination following Russia's attempted covert assassination of intelligence defector Sergei Skripal on British soil in 2018 to persuade partners to impose costs on Moscow by expelling 153 Russian intelligence officers.[34]

The third motive, 'resilience gains', involves governments disseminating intelligence to forewarn, build awareness, and enhance the resilience of state, private, civil society, and public audiences in the face of a developing, often clandestine, threat. This practice has a long history and operates at various levels. Governments' regularly updated threat-orientated travel advice and public indicators of risk calculus like the 'terrorist threat level' produced by the UK's Joint Terrorism Analysis Centre represent simpler, intelligence-led communications of this.[35] More complex are the proliferating links between national intelligence agencies and the private sector for sharing intelligence on cyber threats. The vulnerability of critical national infrastructure – much of which is increasingly in private, not public hands – make it imperative that corporations and their cybersecurity contractors are made aware of attacks, exploits, and sundry other threats that state and non-state actors deploy targeting online networks. External-facing bodies like the US FBI's InfraGard programme, the UK's National Cyber Security Centre (NCSC), and the clones the latter has helped to spawn in Western allies are, essentially, vectors for filtering intelligence from the secret world of agencies like the Government Communications Headquarters (GCHQ) to build resilience in the more open worlds of business, civil society, and public data protection.[36]

The final and perhaps most common motive, 'incrimination gains', sees governments disseminate intelligence to expose, embarrass, or 'call out' an adversary, or occasionally an ally, for their past, present, or anticipated actions, intentions, or even beliefs. Intelligence has tended to be used in this manner when the political climate – issue-specific or strategic – with an adversary or ally is fraught. The desire to retake or retain the moral high ground is often key, meaning that even if intelligence is initially

distributed through private or unattributed channels, public audiences are the ultimate target of influence. This is especially so in cases where the state, entity, or individual targeted for exposure is acting in a manner contrary to international or domestic norms and laws, denying an act, benefitting from acting deniably or ambiguously, influencing audiences by propagating a false or misleading narrative, or operating clandestinely in a hypocritical manner contradicting their stated policy or beliefs. Each of these has been true of the Kremlin and its proxies before and during the invasion of Ukraine.

The most famous example of intelligence used to incriminate, cited regularly during the current crisis, is US Ambassador to the UN Adlai Stevenson's presentation of U-2 spy plane photographs of Soviet nuclear missiles in Cuba before the UN General Assembly in 1962. Approved by President John F. Kennedy, Stevenson sought to undermine Soviet denials and accusations of American disinformation and warmongering, publicly embarrassing his Soviet counterpart and Nikita Khrushchev's government with hard evidence to move allied, neutral, and global opinion toward supporting the US naval 'quarantine' of Cuba.[37]

Stevenson's presentation may have been ground-breaking, but it was by no means unique. After the Soviet air force shot down Korean Airlines flight KAL 007 on 1 September, 1983, the Kremlin not only denied its involvement but kept secret the recovered flight recorder for a decade to hinder the investigation. To expose Soviet duplicity and guilt during a period of high Cold War tensions, US Secretary of State George Shultz presented intercepted Soviet communications at a press conference immediately after the event and US Ambassador to the UN Jeane Kirkpatrick released

recordings of the Soviet pilots' conversations. Soviet efforts to fight back with intelligence to impose their own incrimination costs by releasing details of a US surveillance flight that had supposedly provoked the pilots' actions underscore the perceived persuasive power of intelligence.[38] The Biden administration's publication of the USIC judgements on Saudi state culpability in the murder of Jamal Khashoggi and the Anglo-American-led campaign to publicly attribute Russian, Chinese, North Korean, and Iranian covert activities since 2017 have all been motivated by incrimination gains. They have sought to underline to adversaries and problematic partners that they cannot necessarily act with impunity and their behaviour carries costs, now nor later.

The drivers behind using intelligence for influence during the current crisis underscores that these four motives do not exist in isolation from each other, as incrimination, action, and support gains have interacted. Imposing incrimination costs on Russia has been the primary driver, aiming to illuminate Moscow's efforts to operate in the shadows, covertly, without attribution in the so-called 'grey zone'. Doing so could deny Putin the luxury of past gains through quasi-deniable activities, of sowing confusion and paralysis in Ukraine and internationally, of a surprise attack to rapidly decapitate the Kyiv government through a *coup de main*, and of a credible and legitimate pretext for doing so to impose a 'normalised' new order.

If we go by the words of key stakeholders in this endeavour, achieving these incrimination gains through intelligence-led exposures – combined with shuttle diplomacy, threats of heavy economic sanctions, and security assistance to Ukraine – had the maximalist aim before 23 February of deterring Putin from covertly subverting

Volodymyr Zelenskiy's Kyiv government or overtly invading Ukraine. From Bill Burns' visit to Moscow in early November 2021 onwards, these were private and public signals to Putin that the outside world knew what he was doing, that – unlike the seizure of Crimea and Donbas in 2014 – achieving strategic surprise would not be possible, and that NATO and Ukraine were factoring his actions into their policies and plans. Before the UK Parliament on 25 January, for example, British Prime Minister Boris Johnson framed declassifying 'compelling intelligence' – stretching the nature of the intelligence-led communications – on Russian intent to install a puppet regime, covert cyber sabotage, false flag operations, and disinformation as part of 'credible deterrence'.[39] This fit into London and Washington's exposure campaign over the past five years. Exemplified by the Trump Administration's 2018 Cyber Deterrence Initiative, internationally coordinated intelligence-sharing, post-hoc public attributions of malign cyber activities, and dissemination of technical indicators have been intended to support deterrence – and thus, prevention – by raising incrimination costs for adversaries' future planning and building public and private sector resilience to their activities.[40] In this regard in Ukraine, however, British and American efforts failed to achieve strategic deterrence, though future historians may be able to determine from Russian sources if it had any operational deterrent or disruptive effect in pushing back or amending plans.

Nevertheless, this campaign may have had, and achieved, more minimalist aims. Four days before the invasion, President Joe Biden explained that by exposing Russia's plans, 'we are doing everything in our power to remove any reason Russia may give to justify invading Ukraine.'[41] Similarly, as the invasion commenced, British Secret Intelligence Service Chief Richard Moore highlighted the pre-emptive exposures his service had

supported as revealing that, 'This attack was long planned, unprovoked, cruel aggression. No amount of Russian disinformation will now disguise that fact from the international community.'[42] Exposing Russian intelligence agencies' use of media assets to propagate disinformation, the falsity of allegations of American mercenaries introducing chemical weapons into and Ukrainian armed provocations against the self-declared republics of Donetsk and Luhansk, and regime change plans from before these fabricated provocations occurred undercut Russia's tried and tested tactic of shaping the information environment in its favour to gain narrative superiority.

These counter-measures told audiences not to buy into Moscow's attempts to build a credible justification for invasion by pre-emptively undermining the use of international normative and legal frameworks like self-defence and responsibility to protect. Those willing to listen among fence-sitting Ukrainian, European, and global audiences could be in little doubt that Putin's credibility was weak, or that Moscow was saying one thing but doing another. Operating in the grey zone and generating confusion through their own manufactured intelligence 'exposures' became less frictionless than in the past for Russia's information warriors, a 'spotlight' method that experts have been calling on to help counteract these activities.[43] The ground for doing so has been laid over the past five years, with global malicious cyber behaviour no longer tolerated or allowed to pass without comment by London and Washington in the public domain.

Indicative of the perceived success of using intelligence in this manner for not only incrimination but also resilience gains, Brian Murphy, a former Acting Under Secretary for the Office of Intelligence and Analysis for the Department of Homeland Security, has

called for a new US inter-agency 'Centre to Counter Foreign Malign Influence' to extend this approach from countering influence operations abroad to within the domestic sphere too. It would use, he envisages, all-source intelligence to anticipate, identify, and defuse foreign state-backed disinformation. By disseminating selected intelligence to key governmental, civil society, and private sector stakeholders, it would 'make citizens aware of misconduct by hostile foreign actors… public resilience would be strengthened.' The parallels with the resilience mission of bodies like the UK's NCSC and FBI's InfraGard programme in the cybersecurity sector are no accident. Murphy cites them as inspiration, noting that just as the realisation that 'we were losing and losing badly to adversaries' broke the circular debate about sharing relevant and actionable cyber threat intelligence with stakeholders versus protecting sources and methods, the US and UK may have reached a similar watershed.[44] As Cold War predecessors of such intelligence-led counter-propaganda missions reveal, however, these activities are fraught with dangers in liberal democracies, from approving intelligence for dissemination to the legal, ethical, and political risks of state-led domestic influence campaigns.[45]

Additionally, publicising intelligence in this manner may have been intended to head off domestic and international criticisms of more resolute positions as provocative 'Western aggression', providing an explanatory context for why they were necessary to gain support. Moreover, in combination with private lobbying and intelligence-sharing, this may have sought action gains to move European allies to these more resolute positions and forestall the divided and confused response that Putin likely counted upon. The UK and US intelligence communities privately shared much more and more

granular intelligence – including raw reporting – on Russian actions, capabilities, and intentions as part of this resolve and consensus building. Media reporting quoting European officials with access to this intelligence confirms this.[46] The parallel public dissemination placed further pressure on allies who may have been hesitant to take firmer actions, like France and especially Germany, particularly when Russia indicated (falsely) that it was withdrawing troops from Ukraine's border, anticipating an easing of international pressure. This deception itself was also exposed through US and allied intelligence-led communications.[47]

In December and early January, for example, before US and UK public intelligence disseminations on Russian plans and actions became regular and more detailed, the coalition of new German Chancellor Olaf Scholz was talking about pursuing a reset and 'new start' with Moscow, focused on energy politics and framing the Nord Stream 2 gas pipeline from Russia as a 'private economy project'.[48] By mid-February, when the public exposures had become almost daily, Scholz had moved to warning of 'serious consequences' for a Russian invasion and dismissing Russian casus belli such as a genocide in Donbas as 'ridiculous'. He would, however, continue to resist a public threat of cancelling Nord Stream 2 or promise to change long-standing German policy of providing lethal security assistance until events – the Russian recognition of Ukraine's breakaway provinces and subsequent invasion – forced his hand.[49] The intelligence-led exposure campaign, thus, was by no means the only factor at play. Nevertheless, increasingly unable to hide behind private intelligence-sharing due to growing public lobbying in their legislatures, civil societies, and domestic and international media, the

corralling of international allies with intelligence represents a fascinating continuity of influence campaigns from the Cuban Missile Crisis to the Iraq War.

Adapting, Escalating, Politicising: The Risks of Oversharing

Acting on any intelligence, especially but not only secret intelligence, brings costs as well as gains. Many of these are well known and frequently discussed in intelligence scholarship, including the classic paradox of access and utility: the better a source's access, the more challenging it use it for fear of compromise. Using intelligence to influence external audiences entails exaggerated risks, especially so if done publicly in an attributable manner. Indeed, these risks may typically dissuade states from such actions, depending on the type of intelligence being used, the sensitivity of its subject matter, the more public or private dissemination method, and how sensitive the government is to matters like domestic audience trust costs. Some will be especially sensitive. In the UK, policymakers and intelligence officers alike still remember the reckoning they faced after using intelligence to support the Iraq war. Indeed, the Ukraine case may have rehabilitated British intelligence in the view of some sceptics. The Kremlin, of course, cares less about domestic reputational harm to its intelligence services.

The risks of disseminating intelligence to external audiences can be split into several categories. The first, 'adaptation costs', will be familiar to those, for example, who have observed the fallout from leaks like Edward Snowden's. The utility of certain sources is closely correlated with their secrecy. If secrecy is compromised, so is access. And in the

case of human intelligence, a source's well-being could be put in jeopardy. Aimen Dean, an extremely useful SIS agent inside al Qaeda, experienced this following a decision, allegedly from the office of the then US Vice President, Dick Cheney, to brief a journalist about him.[50] Developing and running such an asset was difficult and time-consuming. Adapting to his loss was significant endeavour.

This risk applies to all categories of intelligence. Following Stanley Baldwin's 1927 revelations before the British Parliament, Stalin's government, naturally, promptly changed their encryption codes to more secure one-time pads. This, combined with the expulsion of the Soviet Trade Delegation, significantly reduced Britain's Government Code and Cypher School ability to decrypt high-grade Soviet diplomatic – though not Red Army – communications for the next two decades. New recruits over the next decade were told the story of this loss of access as a warning of politicians' indiscretion.[51] Nearly sixty years later, in 1986, President Ronald Reagan justified a strike on Libya in retaliation for the state-sponsored bombing of a disco in East Berlin by referring to SIGINT intercepts of Muammar Gaddafi's government that allegedly exposed its culpability. To the dismay of NSA, this may have raised Iranian suspicions about American access to their communications too, achieved through compromised Swiss encryption machines Tehran shared in common with Tripoli through the NSA, CIA, and West German BND's Operation Rubicon.[52] Developing such access is difficult, losing it is easy, and adapting to its loss is complex. It is for this reason that many former British and American intelligence practitioners have reacted warily to their governments' gambit before and during the Ukraine War.[53]

These adaptation costs explain, in part, why states seeking to impose incrimination costs on adversaries often prefer open-source intelligence (OSINT) as the main stay of what they disseminate. In an era before easy third-party access to OSINT, for example, Britain's Cold War anti-Communist propaganda body, the Foreign Office Information Research Department (IRD), developed a global OSINT collection network for its analysts to process and editors to repurpose for propaganda to expose adversaries' actions, intentions, and ways of life through indirect, unattributable methods. The IRD had access to secret intelligence and was occasionally permitted to use it for operational purposes, but OSINT was generally much preferred to reduce more serious adaptation costs.[54]

That is not to say these costs do not exist. First, any knowledge of channels, either those that factor into governmental assessments, or those that the public may use to confirm them, can offer adversaries or mischief-makers a vector for deception operations. John McLaughlin noted an example of a country doing just this to the US with the support of declassified intelligence in raising the risks of how intelligence was used before Russia's invasion of Ukraine.[55] Second, adversaries may adapt when they realise what access and use is being made from open sources, as Russia sought to through operational security changes to frontline soldiers' access to mobile phones and social media after Bellingcat's revelations of Russian complicity in the shooting down of Malaysia Airlines Flight 17 in 2014 using these sources.[56] Third, publics observing national intelligence agencies publishing documents that appear to rely more or less entirely on open sources may react with confusion or scepticism, asking 'is this all there is?' This carries the risk of undercutting the authority of the voice of 'intelligence': if it cannot demonstrate any

advanced or special access that ought give its voice extra weight and credibility, why should it necessarily be taken any more seriously than a government press release?

Nevertheless, using OSINT undoubtedly poses fewer or lower risks than using secret sources. This was the IRD's view during the Cold War. Being more readily citeable and quotable, OSINT was considered key for such exposures to be deemed credible by intermediary and ultimate target audiences and, thus, more persuasive.[57] Using intelligence for incrimination gains publicly, in particular, introduces greater prospect of third-party challenge. This dynamic has changed little since the Cold War, although the information environment has, especially in terms of the volume of conflicting and confusing data openly available. To achieve desired impact today, thus, depends even more on institutional reputation and the credibility and verifiability of the information than doing so through more indirect, unattributable means.

It is becoming easier for governments to talk publicly about some topics, such as malign cyber activities, due to an improving ability to parallel source to open, verified voices. The increasing ability of non-state third-parties – from traditional journalists, to investigative organisations like Bellingcat, to cybersecurity companies, to civil society initiatives like the University of Toronto's Citizen Lab – to impose their own incrimination costs through exposures is well-documented and has been on show during this crisis. The trend for military deployments to be more publicly visible, for example, is linked to the proliferation of affordable commercial satellites – releasing images once seen only by intelligence agencies – and video footage from mobile phones and car dashcams uploaded to social media, poured over and publicised by sundry independent open-

source analysts in a manner that continues the long-standing erosion of state monopolies on information collection and flows.[58] But the ability of these third-parties to conduct more extensive open-source research and analysis to triangulate sources and test claims has more direct implications for using intelligence publicly: it can either strengthen those state actors seeking to expose adversaries by verifying their evidence; or it can undermine them by exposing fabricated material and false narratives that had been intended to incriminate.

Russian intelligence officers and propagandists have encountered this to their cost over the past two months. Their shoddy efforts to incriminate NATO members and Ukraine through forged intelligence supporting false-flag operations were quickly exposed by the expanding international community of open-source analysts who debunked the validity of Russian narratives.[59] London and Washington's previous warnings may have heightened alert to these duplicitous methods, warnings that have continued to expose Russian 'fake news farms' and covert propaganda fronts.[60] But little more state intelligence was needed to support these independent analysts once their verification checks spun into action. With the help of third-parties and affected stakeholders like internet service providers and social media companies, governments can more easily turn to verified OSINT – guided by secret intelligence – to expose adversaries' military, cyber, and information operations.

These considerations make the current Russia-Ukraine case that much more significant. In 2018, for example, the British government leant on Bellingcat's revelations for the detailed revelations of Moscow's attempted assassination of Sergei Skripal, revelations

that had more currency as a result.[61] That London and Washington have been willing to use secret intelligence – albeit in a highly sanitised manner – for their exposures rather than simply lean on widely available OSINT on Russian troop movements and capabilities highlights the gravity of the crisis in pushing them to go further. Yet they have frequently found themselves in a bind by doing so. Disseminating scrubbed intelligence-led communications, while eagerly reported on in international media, also prompted distrust and even derision when they were not supported by more granular – or, indeed, any – supporting intelligence. When State Department spokesperson Ned Price outlined a deep fake operation allegedly being weighed by the Russians as a pretext for invasion, for example, tough questions ensued. 'Where is the declassified information?' Matthew Lee of the Associated Press asked. 'I just delivered it', Price said. 'No, you made a series of allegations', Lee responded.[62] There are adaptation costs to going further, but also audience costs for not doing so. Establishing a precedent for openness risks increased demands for and expectations of access. This can be managed by building the credibility of one's intelligence community with external audiences, assisting governments in cases where they cannot be specific.

The adaptation cost of deploying intelligence in public is complemented by a host of others, which manifest differently with each case. A notable risk factor is to generate or incur escalation costs. Covert operations, proxy wars, subversion, and propaganda have been tried and tested tools of statecraft for decades. Throughout the Cold War, using them enabled the principal states to pursue national security interests whilst mitigating the risk of direct confrontation with each other. As Austin Carson has argued, doing so somewhat covertly and deniably also allowed these states to signal their intent,

priorities, and core interests to each other in a manner that did not introduce as much public pressure to respond. Similarly, Washington and Moscow often, but not always, maintained a norm of not exposing each other's covert operations, especially during periods of crisis. Harry Truman's government, for example, chose not to expose the intelligence they had revealing Soviet pilots were participating in the Korean War.[63] Removing the grey zone by protesting publicly risked limiting the options at these states' disposal to binary choices, building pressure to respond assertively, and closing the clandestine diplomatic safety valve of international affairs. This escalation risk remains a factor in need of consideration today. With his government's aggressive plans and capabilities exposed, could Putin have backed down from invading Ukraine as easily without losing face, assuming this remained a consideration?

There is also the risk of the self-negating prophecy. By using intelligence of an impending attack as part of a deterrence posture, states may negate the very thing they assess as likely, thus rendering their assessment apparently wrong. This occurred in the 1961 Iraq Kuwait crisis.[64] This could, for a public customer base without the complete picture, undermine the credibility of the intelligence assessment process and the organisations that produce them, and make future deployments less impactful. More problematic, it would offer adversaries a weapon to wield in future crises. During the build-up to the invasion, Russian officials frequently referred to the 'so called' intelligence publicised by the US and UK before the disastrous Iraq War as a means of undermining the credibility of ongoing intelligence revelations.[65] The visible capabilities in the Ukraine case may have been so clearly indicative of hostile intent that the risk of publicising the intelligence was acceptable, though there remained a risk of successful deterrence

leading to a later public enquiry regarding another perceived intelligence failure. Not all cases will be as clear cut. Politicians will doubtless be moved to push for more intelligence to be publicised in future crises, but intelligence agencies should carefully mind their credibility with the public as well as their utility to policy, they are, now, intrinsically linked.

Additionally, the risk of mixing intelligence too closely with politics is extremely difficult to manage. Intelligence is there to be used. Intelligence services provide just that, a service. They must be responsive, useful, and provide what their policy makers require, in response to priorities set by policy makers. But they must not subscribe to the service provider's mantra of the customer always being right. Indeed, it is likely that part of Russia's intelligence failings before and during its invasion was precisely because intelligence officers gave their customer precisely what he wanted to hear.[66] Maurice Oldfield, the former 'C', Chief of SIS, noted to Prime Minister James Callaghan in the 1970s that his job was 'to bring unwelcome news'.[67] But this is easier when the entire conversation is in secret; officers can stand their ground and be damned. But when intelligence is deployed publicly this is more difficult: the product is inherently political; it will lack the nuance of secret communications; it will be delivered to a customer base largely unfamiliar with the uses and limits of intelligence.

This is a perilous environment for intelligence agencies to navigate. First, in an extreme case, policymakers who deploy intelligence in public may lean on their officers to give direct, less ambiguous assessments, clearly communicating *a* threat, but perhaps not quite the nuance of *the* threat. As several observers have underlined having surveyed

the wreckage of Iraqi WMD, this is a risk that needs careful management. High-pressure, high-stake circumstances may heighten the risk of unwitting politicisation.[68] Second, by introducing public perception this raises the potential audience costs. Intelligence assessments operate in the realm of uncertainty, ambiguity, and probabilities, with reporting rarely a slam dunk. The public consumer, however, is consistently reminded of past intelligence failures, and, perhaps naturally, suspicious of politicians who wield 'intelligence' as the factor exposing an adversary and justifying serious policy choices. Iraqi WMD underscored the reputational risks of leaning too heavily on incomplete and overly-spun intelligence in public, something that has been repeatedly mentioned by a sceptical media reporting on the British and American governments' revelations during the Ukraine crisis. Narrowing the divide between the intelligence and policy worlds further in the minds of the public risks the perceived independence of intelligence communities in liberal democracies and, thereby, damaging trust. As the 2004 UK Butler Report concluded in reflecting on the public use of intelligence on Iraqi WMD, careful explanations of intelligence uses and limitations are needed, together with clearer and more effective dividing lines between assessment and advocacy.[69] This may not sit well with the policy requirements for impactful intelligence-led communications to incriminate, justify, and persuade.

Spies for transparency

Could the prolific public use of intelligence, on the model of the Ukraine War, be a sign of things to come? Could it be a new age of public intelligence diplomacy, with intelligence increasingly used for external influence as well as internal consumption in

sustained offensives, not merely surgical strikes? It is highly likely that having witnessed the utility of judicious use of intelligence in the build-up to the invasion, allowing Western governments to pre-emptively undermine Russia's narratives and claims, policymakers will aim to reap similar rewards in future crises. It is a development broadly to be welcomed, as long as adaptation costs are managed, the integrity of the analytical process respected, and the professional judgement of intelligence officers left uncompromised. Intelligence is a tool, an element of state power. Used judiciously, it has utility in the public sphere, just as it does every day in its more natural secret habitat. A matter as serious as deterring and managing war in a region within one's core national interests merits the deployment of the nation's capabilities. Yet having seen the potential riches of using intelligence this way, governments may now wish to lower the threshold for deployment as global inter-state competition continues to deepen. The policy demands placed on intelligence communities, and how they balance the risks and rewards, may be entering a new era in international politics.

[1] Julian Borger and Dan Sabbagh, 'US warns of 'distinct possibility' Russia will invade Ukraine within days', *Guardian*, 11 February, 2022, https://www.theguardian.com/world/2022/feb/11/biden-ukraine-us-russian-invasion-winter-olympics .

[2] Edward Wong and Julian E. Barnes, 'China asked Russia to delay Ukraine war until after Olympics' , *New York Times*, 2 March, 2022, https://www.nytimes.com/2022/03/02/us/politics/russia-ukraine-china.html .

[3] Andrew Roth, Dan Sabbagh, Lisa O'Carroll, 'Ukraine taking UK claim of Russian invasion plot seriously, says adviser', *Guardian*, 23 January, 2022, https://www.theguardian.com/world/2022/jan/23/ukraine-taking-uk-claim-of-russian-invasion-plot-seriously-says-adviser .

[4] Andrew Marrow and Aleksandar Vasovic, 'West warns military build-up near Ukraine growing, not shrinking', *Reuters*, https://www.reuters.com/world/europe/russian-pullout-meets-uk-scepticism-ukraine-defence-website-still-hacked-2022-02-16/ .

[5] Gordon Corera, 'Ukraine War: Western agents seek to get inside Putin's head', *BBC News*, 20 March 2022.

[6] Natasha Bertrand, Jim Sciutto, and Kylie Atwood, 'CIA Director dispatched to Moscow to warn Russia over troop buildup near Ukraine', *CNN*, 5 November, 2021, https://edition.cnn.com/2021/11/05/politics/bill-burns-moscow-ukraine/index.html; Shane Harris, Paul Sonne, 'Russia planning massive military offensive against Ukraine involving 175,000 troops, US intelligence warns', *Washington Post*, 3 December, 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html .

[7] See Julian Borger and Luke Harding, 'US claims Russia planning 'false-flag' operation to justify Ukraine invasion', *Guardian*, 14 January, 2022, https://www.theguardian.com/world/2022/jan/14/us-russia-false-flag-ukraine-attack-claim; Mark Landler, 'Britain pursues more muscular role in standoff with Russia on Ukraine', *New York Times,* 23 January, 2022, https://www.nytimes.com/2022/01/23/world/europe/uk-russia-ukraine.html; Ellen Nakashima, Shane Harris, Ashley Parker, John Hudson, Paul Sonne, 'US accuses Russia of planning to film false flag attack as pretext for Ukraine invasion', *Washington Post*, 3 February, 2022, https://www.washingtonpost.com/national-security/2022/02/03/russia-ukraine-staged-attack/; Dan Sabbagh, 'Russia's FSB agency tasked with engineering coups in Ukrainian cities UK believes', *Guardian*, 13 February, 2022, https://www.theguardian.com/world/2022/feb/13/russias-fsb-agency-engineering-coups-ukrainian-cities; SeanLengaas and Zachary Cohen, 'US accuses Moscow of working with Russian language media outlets to spread Ukraine disinformation', *CNN*, 15 February, 2022, https://edition.cnn.com/2022/02/15/politics/us-russia-ukraine-misinformation/index.html .

[8] Katie Bo Lillis, Natasha Bertrand, Kylie Atwood, 'How the Biden administration is aggressively releasing intelligence in an attempt to deter Russia', *CNN*, 11 February, 2022; https://edition.cnn.com/2022/02/11/politics/biden-administration-russia-intelligence/index.html; Dan Sabbagh, 'Ukraine crisis brings British intelligence out of the shadows', *Guardian*, 18 February, 2022, https://www.theguardian.com/world/2022/feb/18/ukraine-crisis-bring-british-intelligence-out-of-the-

shadow-warning-russian-invasion-information-war-with-kremlin; Douglas London, 'To reveal or not to reveal', *Foreign Affairs*, 15 February, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-02-15/reveal-or-not-reveal .

[9] US Intelligence Community Assessment, 'Assessing Russian Activities and Intentions in Recent U.S. Elections', 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[10] For a variety of UK statements relating to attribution see, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks; https://www.gov.uk/government/publications/letter-from-the-uk-national-security-adviser-to-the-nato-secretary-general; https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign; https://www.gov.uk/government/news/gulf-of-oman-attacks-uk-statement.

[11] Geoff Brumfiel, 'Trump tweets sensitive surveillance image of Iran', *NPR*, 30 August, 2019, https://www.npr.org/2019/08/30/755994591/president-trump-tweets-sensitive-surveillance-image-of-iran .

[12] Ministry of Defence Twitter account, 17 February, 2022, https://twitter.com/DefenceHQ/status/1494344646864031758?s=20&t=lEzYc3hzJLPWa2-zQxqsWg; https://twitter.com/DefenceHQ/status/1500885976146759686 .

[13] Dan Sabbagh, 'Ukraine crisis brings British intelligence out of the shadows', *Guardian*, 18 February, 2022, https://www.theguardian.com/world/2022/feb/18/ukraine-crisis-bring-british-intelligence-out-of-the-shadow-warning-russian-invasion-information-war-with-kremlin .

[14] For an example of a probability yardstick, see https://www.app.college.police.uk/app-content/intelligence-management/analysis/delivering-effective-analysis/ .

[15] Emma Farge, 'Russia says ;real danger' of Ukraine acquiring nuclear weapons required response', *Reuters*, 1 March, 2022, https://www.reuters.com/world/russias-lavrov-says-there-is-danger-ukraine-acquiring-nuclear-weapons-2022-03-01/; Stephanie van den Berg, 'Russian no whos at UN court hearing on Ukrainian genocide', 7 March, 2022, https://www.reuters.com/world/europe/ukraine-russia-face-off-world-court-over-genocide-claim-2022-03-06/.

[16] Christopher Andrew and Vasili Mitrokhin, *The KGB and the World: The Mitrokhin Archive II* (London: Allen Lane, 2005), pp. 435-42.

[17] Veli-Pekka Kivimäki, 'Russian state television shares fake images of MH17 being attacked', 14 November 2014, https://www.bellingcat.com/news/2014/11/14/russian-state-television-shares-fake-images-of-mh17-being-attacked/ .

[18] 'Ukraine hastily destroyed pentagon-funded biological program: Kremlin', *Defence World.net*, 6 March, 2022, https://www.defenseworld.net/news/31520#.YiiAPujMI2x; Robin Emmott, 'EU says Russia report of biolabs in Ukraine likely disinformation', *Reuters*, 9 March, 2022, https://www.reuters.com/world/eu-says-russia-reports-biolabs-ukraine-likely-disinformation-2022-03-09/ .

[19] 'China's false allegations of the use of biological weapons by the United States during the Korean war', *Cold War International History Programme*, March, 2016, https://www.wilsoncenter.org/publication/chinas-false-allegations-the-use-biological-weapons-the-united-states-during-the-korean; Milton Leitenberg, 'False allegations of biological-weapons use from Putin's Russia', *The Nonproliferation Review* (2021), DOI: 10.1080/10736700.2021.1964755; Joseph A. Gambardello, 'Social media posts misrepresent US-Ukraine threat reduction program', *Factcheck.org*, 2 March, 2022, https://www.factcheck.org/2022/03/social-media-posts-misrepresent-u-s-ukraine-threat-reduction-program/; Dan Sabbagh, Julian Borger, 'Britain and US fears Russia could be setting stage to use chemical weapons', *Guardian,* 9 March, 2022, https://www.theguardian.com/world/2022/mar/09/britain-fears-russia-could-be-setting-stage-to-use-chemical-weapons.

[20] Joint Intelligence Committee, 'Syria: reported chemical weapons use', 29 August, 2013, https://www.gov.uk/government/publications/syria-reported-chemical-weapons-use-joint-intelligence-committee-letter; The White House, 'United States assessment of the Assad regime's chemical weapons use', 13 April, 2018, https://dod.defense.gov/portals/1/features/2018/0418_syria/img/United-States-Assessment-of-the-Assad-Regime%E2%80%99s-Chemical-Weapons-Use.pdf.

[21] Office of the Director of National Intelligence, 'Assessing the Saudi government's role in the killing fo Jamal Khashoggi', 11 February, 2021,

https://www.dni.gov/files/ODNI/documents/assessments/Assessment-Saudi-Gov-Role-in-JK-Death-20210226v2.pdf .

[22] Center for the Study of Intelligence, 'The Cuban missile crisis of 1962: Presenting the photographic evidence abroad', https://irp.fas.org/imint/cubakent.htm .

[23] 'The US is Engaging in a Strategy to Share Intelligence on Russia More Broadly. Is it Worth the Risk?', *The Cipher Brief*, 16 February 2022, accessed at: https://www.thecipherbrief.com/the-us-is-engaging-in-a-strategy-to-share-intelligence-on-russia-more-broadly-is-it-worth-the-risk.

[24] Jim Scuitto and Natasha Bertrand, 'CIA Director had rare conversation with Putin while in Moscow last week', *CNN*, 8 November, 2021, https://edition.cnn.com/2021/11/08/politics/bill-burns-cia-putin-moscow/index.html .

[25] Rob Dover and Michael S. Goodman (eds), *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence* (London: Hurst, 2009).

[26] Thomas Boghardt, 'Soviet Bloc intelligence and its AIDS disinformation campaign', *Studies in Intelligence*, 53, 4 (2009), pp. 1-24; Douglas Selvage, 'Operation "Denver": The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985-1986', *Journal of Cold War Studies*, 21, 4 (Fall 2019), pp. 71-123; James Shires, 'The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics', *Texas National Security Review*, 3, 4 (Fall 2020), pp. 10-29; Nomaan Merchant, 'US accused financial website of spreading Russian propaganda', *ABC News*, 15 February, 2022, https://abcnews.go.com/Politics/wireStory/us-accuses-financial-website-spreading-russian-propaganda-82898788.

[27] Christopher Andrew, *The Defence of the Realm: The Authorized History of MI5* (London: Allen Lane, 2009), pp. 154-56.

[28] Richard J. Aldrich, 'Whitehall and the Iraq War: The UK's Four Intelligence Enquiries', *Irish Studies in International Affairs*, 16 (2005), pp. 73-88; Robert Jervis, 'Reports, politics, and intelligence failures: The case of Iraq', *Journal of Strategic Studies*, 29, 1 (2006), pp. 3-52.

[29] Thomas Boghardt, *The Zimmermann Telegram: Intelligence, Diplomacy, and America's Entry into World War I* (Annapolis, MD: Naval Institute Press, 2012); Daniel Larsen, *Plotting for Peace: American Peacemakers, British Codebreakers, and Britain at War, 1914-1917* (Oxford: Oxford University Press, 2021), pp. 280-306.

[30] Alan Barnes, 'How Canada's intelligence agencies helped keep the country out of the 2003 Iraq war', *Open Canada*, 18 November 2020: https://opencanada.org/how-canadas-intelligence-agencies-helped-keep-the-country-out-of-the-2003-iraq-war/; 'U.S. Allies Were Not Persuaded By U.S. Assertions on Iraq WMD', Institute for Science and International Security, 9 June 2003: https://isis-online.org/isis-reports/detail/u.s.-allies-were-not-persuaded-by-u.s.-assertions-on-iraq-wmd/9#back56.

[31] Steve Coll, *Directorate S: The C.I.A. and America's Secret Wars in Afghanistan and Pakistan, 2001–2016* (New York: Penguin, 2016); Stephen Tankel, *With Us and Against Us: How America's Partners Help and Hinder the War on Terror* (New York: Columbia University Press, 2018), chapter four.

[32] David M. Halbfinger, 'Israel Presses the Case Against Iran But Not For War', *New York Times*, 16 May, 2019, https://www.google.com/search?client=safari&rls=en&q=Israel+Presses+the+Case+Against+Iran+But+Not+For+War%E2%80%99&ie=UTF-8&oe=UTF-8.

[33] Ellen Nakashima and Brian Fung, 'U.S. allies differ on difficulty of containing Huawei security threat', *Washington Post*, 6 March 2019; Garrett M. Graff, 'The US Is Losing Its Fight Against Huawei', *Wired*, 29 January, 2020: https://www.wired.com/story/uk-huawei-5g-networks-us/.

[34] Julian Borger et al, 'Western allies expel scores of Russian diplomats over Skripal attack', *The Guardian*, 27 March 2018.

[35] The JTAC threat level is published on the Security Service website: https://www.mi5.gov.uk/news-categories/threat-level .

[36] See the NCSC's 'Cyber Threat' website: https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=cyber%20threat&sort=date%2Bdesc .

[37] The use of intelligence in secret and publicly during the Cuban Missile Crisis has been extensively discussed, for a useful summary see https://www.cfr.org/blog/twe-remembers-adlai-stevenson-dresses-down-soviet-ambassador-un-cuban-missile-crisis-day-ten , and for a more detailed discussion see the essays in James G. Blight, David A. Welch, *Intelligence and the Cuban Missile Crisis*, (Routledge, 1998).

[38] See Celestine Bohlen, 'Tape displays anguish on jet the Soviets downed', *New York Times*, 16 October, 1992, https://www.nytimes.com/1992/10/16/world/tape-displays-the-anguish-on-jet-the-soviets-downed.html and Peter Grier, 'The death of Korean Air Lines flight 007', 1 January, 2013, https://www.airforcemag.com/article/0113korean/ .

[39] Oral statement to Parliament, 'PM statement on Ukraine: 25 January 2022', House of Commons, 25 January 2022: https://www.gov.uk/government/speeches/pm-statement-on-ukraine-25-january-2022.

[40] US Government, 'National Cyber Strategy of the United States of America', September 2018, p. 21, accessible at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[41] Tweet, President Biden, *Twitter*, 19 February ,2022: https://twitter.com/POTUS/status/1494863649500168193.

[42] Tweet, Richard Moore, *Twitter*, 24 February, 2022: https://twitter.com/ChiefMI6/status/1496939916965695489.

[43] Jake Harrington and Riley McCabe, 'Detect and Understand: Modernizing Intelligence for the Gray Zone', CSIS Brief (Center for Strategic and International Studies, December 2021).

[44] Brian Murphy, 'The US Needs a Center to Counter Foreign Malign Influence at Home', *Defense One*, 20 March 2022, accessed at: https://www.defenseone.com/ideas/2022/03/us-needs-center-counter-foreign-malign-influence-home/363366/.

[45] Thomas J. Maguire, 'Counter-subversion in early Cold War Britain: the Official Committee on Communism (Home), the IRD and "state-private networks"', *Intelligence and National Security*, 30, 5 (2015), pp. 637-66

[46] Ellen Nakashima, Shane Harris, Alex Horton, Michael Birnbaum, 'US intelligence shows Russia's military pullback was a ruse, officials say', *Washington Post*, 17 February, 2022, https://www.washingtonpost.com/world/2022/02/17/ukraine-russia-putin-nato-munich/ .

[47] Ibid,

[48] Jamie Dettmer, 'Smaller European nations uneasy as Germany's Scholz plans to meet Putin', *VOA*, 3 January, 2022, https://www.voanews.com/a/smaller-european-nations-uneasy-as-germany-scholz-plans-to-meet-putin/6379981.html; Hans Von Der Burchard, David M Herszenhorn, 'Russian test for Scholz: Ukraine crisis exposes divisions in Berlin', *Politico*, 17 January, 2022, https://www.politico.eu/article/germany-russia-ukraine-crisis-olaf-scholz/.

[49] Jenny Hill, 'Olaf Scholz: Ukraine crisis a challenge for German leader', *BBC*, 14 February, 2022, https://www.bbc.com/news/world-europe-60344479; 'Scholz's dismissal of alleged genocide in Donbass 'unacceptable', Russia says', *Reuters*, 19 February, 2002,

https://www.reuters.com/world/europe/scholzs-dismissal-alleged-genocide-donbass-unacceptable-russia-says-2022-02-19/.

[50] Aimen Dean, Paul Cruickshank, Tim Lister, *Nine Lives: My Time As MI6's Top Spy Inside Al-Qaeda* (Oneworld Publications, 2018)

[51] Andrew, *Defence of the Realm*, pp. 154-56; John Ferris, 'Issues in British and American Signals Intelligence, 1919-1932', NSA Center for Cryptological History, Special Series, Vol. 11 (2015), pp. 31-32.

[52] See Jason Dymydiuk, 'RUBICON and revelation: the curious robustness of the 'secret' CIA-BND operation with Crypto AG', *Intelligence and National Security*, 35, 5 (2020), pp. 641-58.

[53] Max Colchester and Warren P. Strobel, 'U.S., Allies Fight Information War With Russia to Deter Ukraine Invasion', *Wall Street Journal*, 9 February 2022.

[54] Thomas J. Maguire, *The Intelligence-Propaganda Nexus: British and American Covert Action in Cold War Southeast Asia* (Oxford: Oxford University Press, forthcoming 2022).

[55] 'The US is Engaging in a Strategy to Share Intelligence…', *The Cipher Brief*, 16 February 2022.

[56] See, for example, 'Russia bans smartphones for soldiers over social media fears', *BBC News*, 20 February, 2019.

[57] Maguire, *The Intelligence-Propaganda Nexus*.

[58] 'Trainspotting, but with nukes: Open-source intelligence challenges state monopolies on information', *The Economist*, 7 August 2021; 'OSINT: A new era of transparent warfare beckons', *The Economist*, 18 February 2022; Christian Davenport, 'Commercial satellites test the rules of war in Russia-Ukraine conflict', *Washington Post*, 10 March 2022.

[59] Matthew Gault, 'The Internet Is Debunking Russian War Propaganda in Real Time', *Vice*, 22 February 2022, accessible at: https://www.vice.com/en/article/7kb75e/the-internet-is-debunking-russian-war-propaganda-in-real-time; Investigation Team, 'Documenting and Debunking Dubious Footage from Ukraine's Frontlines', *Bellingcat*, 23 February 2022, accessed at: https://www.bellingcat.com/news/2022/02/23/documenting-and-debunking-dubious-footage-from-ukraines-frontlines/.

[60] Jon Ungoed-Thomas, 'West hits Vladimir Putin's fake news factories with wave of sanctions', *The Observer*, 20 March 2022.

[61] Investigation Team, 'The GRU Globetrotters: Mission London', *Bellingcat*, 28 June 2019, accessed at: https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/.

[62] Chris Megerian, 'Looking for evidence? Trust us, Biden administration says', *AP News*, 5 February 2022, accessed at: https://apnews.com/article/coronavirus-pandemic-russia-ukraine-health-europe-national-security-5c4182d83dd8b7585ac49fdbb5f91c45.

[63] Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton University Press, 2018).

[64] The crisis and the JIC is discussed in Richard A. Mobley, 'Gauging the Iraqi threat to Kuwait in the 1960s', *Studies in Intelligence*, 45/5 (2001), https://apps.dtic.mil/sti/pdfs/ADA529668.pdf .

[65] Kyle Farrell, '"Remember Iraq!" Russian ambassador mocks UK in brutal weapons of mass destruction jibe', *Express*, 20 February, 2022, accessed at: https://www.express.co.uk/news/world/1568905/russia-news-trevor-phillips-ukraine-troops-sky-news-conflict-war-video-latest-vn.

[66] See David V. Gioe and Huw Dylan, 'Putin's KGB past didn't help him with intelligence on Ukraine', *Washington Post*, 17 March, 2022, https://www.washingtonpost.com/outlook/2022/03/17/putins-kgb-past-didnt-help-him-with-intelligence-ukraine/ .

[67] Kevin Theakston, *British Foreign Secretaries Since 1974*, (Routledge: London, 2004), p.26.

[68] These issues are widely discussed, see for instance, Eric Herring and Piers Robinson, 'Report X Marks the Spot: The British Government's Deceptive Dossier on Iraq and WMD', *Political Science Quarterly*, 129/4 (2014), https://doi.org/10.1002/polq.12252 .

[69] Report of a Committee of Privy Counsellors, 'Review of Intelligence on Weapons of Mass Destruction', HC 898 (London: Stationery Office, 2004), p. 87.