Routledge
Taylor & Francis Group

Survival
Global Politics and Strategy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tsur20

Secret Intelligence and Public Diplomacy in the Ukraine War

Huw Dylan & Thomas J. Maguire

To cite this article: Huw Dylan & Thomas J. Maguire (2022) Secret Intelligence and Public Diplomacy in the Ukraine War, Survival, 64:4, 33-74, DOI: 10.1080/00396338.2022.2103257

To link to this article: https://doi.org/10.1080/00396338.2022.2103257

Published online: 02 Aug 2022.

Secret Intelligence and Public Diplomacy in the Ukraine War

Huw Dylan and Thomas J. Maguire

Russia's February 2022 invasion of Ukraine was shocking, but few could claim 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 while the Beijing Winter Olympics were ongoing, thereby detracting attention from 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 undoubtedly 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 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

Huw Dylan is a Reader in Intelligence and International Security at the Department of War Studies, King's College London, and Associated Researcher at the Centre for Intelligence Studies, Norwegian Intelligence School. **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.

Survival | vol. 64 no. 4 | August–September 2022 | pp. 33–74 https://doi.org/10.1080/00396338.2022.2103257

units, spare ammunition and sundry other combat enablers be mobilised on such a scale for a bluff?[4] 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 remains far more challenging.[5] This is a familiar problem.

The Russo-Ukrainian war has, however, been accompanied by an intriguing development: 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 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]

While 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, the public use of intelligence regarding Ukraine 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 (reaching its peak between mid-January and mid-February 2022), the very public nature of this, and the pre-emptive approach of using intelligence to deter or undermine Russian actions have been remarkably novel in the modern history of international statecraft.

Yet few things are new under the sun. 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. 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's and Washington's intelligence-led claims about Russian actions and intentions are not unique even within their recent relations with Moscow. Compared to fairly limited public exposures and attributions of unacknowledged Russian 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, especially in cyberspace.[10] Indeed, the creation of the public-facing National Cyber Security Centre in the United Kingdom in October 2016 and the Cybersecurity and Infrastructure Security Agency in the United States in November 2018 (which have led public attributions of hostile covert activities in cyberspace), as well as Britain's Joint State Threats Assessment Team in June 2017, meant that some of the intelligence and policy infrastructure necessary for vetting and communicating intelligence on the Ukraine crisis was already in place with a track record of use in these two countries, if not in other NATO partners.

Public intelligence and intelligence as influence

To understand what is taking place in the Russo-Ukrainian war, we need to unpack the interlinked concepts of 'intelligence as influence' and 'using intelligence in public'. When evaluating what intelligence is being disseminated, we need to differentiate between 'raw' intelligence (such as satellite images, intercepted-communications recordings or social-media posts), 'finished' intelligence (such as a report assessing such raw sources) and 'intelligence-led communications' (such as statements of findings based on underlying intelligence assessments). Doing so is important not only to ensure that we are all talking about the same thing, but also because the specificity, or granularity, of the intelligence being disseminated – as well as whether this intelligence is fully or only partially disclosed – 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 caused much hand-wringing, about revealing advanced capabilities.[11]

Ahead of Russia's invasion of Ukraine, with the exception of verifiable satellite images and confidential briefings to trusted journalists, most 'intelligence releases' by London and Washington fell into the category of high-level, highly sanitised, intelligence-led communications. These were deployed in accessible formats from 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, updates were frequently but not always adorned with phrases such as 'we judge it to 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 see such formal assessment language so widely used in public. Over the past five years, however, it has become increasingly commonplace. In the weeks since Russia's 2022 invasion of Ukraine, not only the UK and the US, but also NATO partners and Ukraine itself, have disclosed raw and finished intelligence on Russian actions. Examples include low-level signals-intelligence intercepts of communications between Russian troops and commanders by Ukraine and Germany to highlight poor morale and war crimes in occupied territory; Slovakian surveillance video of a Russian intelligence officer meeting an agent of influence recorded in 2021 as part of a wave of European expulsions of Russian intelligence officers; and British assessments of Russian disinformation methods.[15]

The type of intelligence being disclosed can be categorised in another way. Intelligence that state disseminators consider to be accurate and reliable, and that is intended primarily for an internal audience, can be considered 'good faith' deployment. Intelligence that state disseminators have purposefully collected, collated and spun with the primary goal of influencing external audiences can be described as a 'strategic' deployment. Finally, intelligence that disseminators have purposefully fabricated to

support an act of disinformation intended to confuse or deceive audiences is 'deceptive' deployment. In all three categories, the disseminating body is seeking to exploit the power and authority of 'intelligence' as something that is perceived to provide unique insights. During the ongoing crisis, all three types have been in play: the first two from London and Washington through their confidential briefings and social-media updates; and the latter from Moscow, with its false-flag operations and fraudulent claims that a neo-Nazi Ukrainian regime has been committing genocide against Russian speakers and has designs on nuclear weapons.[16]

The Kremlin's comfort with trafficking fabricated intelligence and using false flags as pretexts for coercive acts 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 intelligence services such as the CIA in their countries.[17] More recently, Russia disseminated fabricated intelligence following the downing of Malaysia Airlines Flight 17 over Ukraine with the aim of diverting the blame for that outrage from itself.[18] The UK, the US and other NATO and allied intelligence communities have also documented and exposed widespread Russian use of false flags to conceal cyber intrusions during the past decade, from piggybacking on the servers of Iranian hacking groups to masquerading as criminal entities.[19] This has continued during the conflict in Ukraine, with the Kremlin claiming to have documents from captured Ukrainian public-health laboratories exposing Pentagon-funded 'secret biological experiments' with plague, cholera and anthrax.[20] The labs' actual role since 2005 has been to support disease control and prevention, including during the COVID-19 pandemic. The Russian claims are consistent with the country's decades-old practice, dating to the Korean War, of using fabricated intelligence to portray the US government as a bioweapons proliferator, disinformation that has been called out by NATO and European Union members as a pretext for Russia deploying its own chemical weapons against Ukrainian targets.[21]

Intelligence communities exposed widespread use of false flags

There are three main methods through which states use intelligence for influence, all of which have been at play during the current crisis. Firstly, intelligence is publicly disseminated to target audiences in an attributed manner, in that 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 has several recent historical precedents. The UK government, for example, published the assessment of its Joint Intelligence Committee 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 in April 2018.[22] Similarly, in February 2021 the US government published a sanitised version of its intelligence agencies' judgement concerning the culpability of the Saudi state in the murder of dissident journalist Jamal Khashoggi in Istanbul in 2018.[23]

States can also privately disseminate intelligence to more focused target audiences – state and non-state partners and proxies – as part of wider, clandestine intelligence-sharing networks. The US government did this, for example, during the Cuban Missile Crisis, sharing intelligence with allies on growing Soviet nuclear capabilities in Cuba to gain support for its naval 'quarantine' of the island.[24] Target audiences can also include adversaries or belligerent parties in a dispute or conflict. John McLaughlin, when serving as the acting director and deputy director of the CIA, was occasionally sent to Moscow to relay messages based on classified intelligence to let the Russians 'know that you knew' while protecting sources and methods.[25] In November 2021, CIA Director William Burns followed in McLaughlin's footsteps, privately meeting with Putin to convey both the gravity of Washington's concerns and its understanding of Russian movements and intentions, increasingly solidified from mid-2021 through joint UK–US intelligence-gathering and analysis from multiple sources.[26]

Thirdly, states can 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 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. Rob Dover and Michael Goodman's *Spinning Intelligence* highlights the symbiotic relationship between intelligence communities and the media in this regard, each gaining something from the relationship.[27] Controlled or sympathetic media assets, for example, have allowed intelligence agencies to 'surface' 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, as during the current Russo-Ukraine war, to spread false-flag disinformation.[28] The permeability of the membrane between the secret and open worlds offers many opportunities for politicians to use intelligence creatively.

Tinker, tailor, soldier, incriminator

As well as the how, we need to consider the why. There are five 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), British prime minister Stanley Baldwin announced before Parliament that the motive for the raid, and for his government's intention to break its 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.[29]

More recently, to gain support for the American-led invasion of Iraq in 2003, London and especially Washington made justificatory use of intelligence pre-emptively rather than post hoc. Documents detailing British and American intelligence communities' judgements about Iraqi leader Saddam Hussein's alleged weapons 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 George Tenet, the director of Central Intelligence, sat behind him. The purpose of these presentations was to persuade by revealing to domestic and international audiences the intelligence analysis supposedly underpinning the policymaking process.[30]

The second motive, *action gains*, sees governments deploy intelligence to sway or persuade the decision-making, actions or even world view 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 the 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 to avoid tipping off adversaries. Over a century ago, during the famous Zimmerman Telegram case, David Lloyd George's British government sought to persuade US president Woodrow Wilson to enter the war in 1917. At the heart of the British 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 enable Wilson's government to later publish the telegram without putting Germany on notice as part of an exposure of German hostility and a campaign to convince the American public of the need to enter the war.[31]

Governments deploy intelligence to sway partners

Since then there have been numerous cases of intelligence deployed for action gains. To persuade more allies, such as the governments of Canadian prime minister Jean Chrétien and French president Jacques Chirac, to adopt more forceful positions at the UN and even to join the invasion of Iraq, George W. Bush's administration lobbied them – unsuccessfully – using the intelligence analysis it claimed supported the American case.[32] At times during the post-9/11 conflict in Afghanistan, the US government and the CIA sought to carefully use intelligence to pressure Pakistan's Inter-Services

Intelligence to cease its covert support for the Afghan Taliban.[33] As the Cuban Missile Crisis and the use of intelligence during the current Russo-Ukrainian crisis demonstrate, however, states sometimes seek to influence their allies through a mixture of public and private intelligence. This has been the case with Israel's use of intelligence to lobby key stakeholders – in particular, the Trump White House – against the signing, adherence to and renewal of the Iran nuclear deal.[34] The Trump administration itself used similar tactics to pressure the UK government and other European allies not to adopt Chinese telecommunications company Huawei's equipment in their next-generation 5G networks.[35] The British government pursued public–private intelligence dissemination following Russia's attempted 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.[36]

The third motive, *resilience gains*, involves government dissemination of 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 is intended to both influence the behaviour and build the capacity of audiences to better protect themselves, highlighting the fuzzy line between action and resilience gains when these audiences are partners and proxies. This practice has a long history and operates at various levels. Governments regularly update threat-oriented travel advice and public indicators of risk. The 'terrorist threat level' produced by the UK's Joint Terrorism Analysis Centre represents an example of this kind of intelligence-led communication.[37]

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 rather than public hands – makes it imperative that corporations and their cyber-security contractors are made aware of attacks, exploits and sundry other threats by state and non-state actors targeting online networks. External-facing bodies such as the Cybersecurity and Infrastructure Security Agency and the FBI's InfraGard programme in the US, the UK's National Cyber Security Centre, and the clones the latter has helped to spawn in

NATO and other allies are, essentially, vectors for filtering intelligence from the secret world of agencies such as the Government Communications Headquarters (GCHQ) to build resilience in the more open worlds of business, civil society and public data protection. Their attributions and releases of technical intelligence can act as a model for other states, companies and civil-society organisations that are subject to similar threats.[38]

European partners agree on the importance of this approach for building resilience to Russia's 'hybrid' spectrum of coercive and subversive influence. At a 2021 seminar of the Estonian Internal Security Institute and the Intelligence College in Europe on the impact of hybrid threats on European security, for example, a key consideration was intelligence-informed education. A 'population who is aware and understands and recognizes threats', attendees concurred, 'is our strength and improves our resilience'.[39] This has been exemplified through the European Centre of Excellence for Countering Hybrid Threats (known as the Hybrid CoE), founded in Finland in October 2017, which draws on pre-existing NATO and EU structures to share intelligence and research between partners in a manner that has led to calls for something similar in the Indo-Pacific.[40]

Perhaps the most common motive, *incrimination gains*, sees governments disseminate intelligence to expose, embarrass or 'call out' an adversary, or occasionally an ally, for its past, present or anticipated actions, intentions or even beliefs. Intelligence has tended to be used in this manner when the political relationship – either 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 true in cases where the actor targeted for exposure is known to be acting in a manner contrary to international or domestic norms and laws; is denying an act; is benefitting from acting deniably or ambiguously; is influencing audiences by propagating a false or misleading narrative; or is operating clandestinely in a hypocritical manner that contradicts its stated policy or beliefs. Using intelligence to influence others under these circumstances, such as in cases of breaches of arms-proliferation agreements or leaders' authorisations of

human-rights atrocities during a war, is generally aimed at securing penalties and imposing costs to reduce support for the actor, deter future acts or achieve greater compliance.[41] A number of these considerations have been true of the Kremlin and its proxies before and during the invasion of Ukraine, providing incentives to the UK, the US and NATO partners to name and shame.

The most famous example of incriminating intelligence being used to alter behaviour, cited regularly during reporting on the Ukraine crisis, is Adlai Stevenson's presentation of U-2 spy-plane photographs of Soviet nuclear missiles in Cuba before the UN General Assembly in 1962. With the approval of president John F. Kennedy, Stevenson sought to undermine Soviet denials and accusations of American disinformation and warmongering, publicly embarrassing Nikita Khrushchev's government with hard evidence to move not just allied but global opinion towards supporting the US naval quarantine of Cuba.[42]

Stevenson's presentation may have been ground-breaking, but it was by no means unique. After the Soviet air force shot down Korean Air Lines Flight 007 on 1 September 1983, the Kremlin not only denied involvement but kept secret the recovered flight recorder for a decade to hinder the investigation. To expose Soviet 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 Jeane Kirkpatrick, the US ambassador to the UN, released recordings of the Soviet pilots' conversations. Soviet efforts 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.[43]

The Biden administration's publication of the intelligence judgements of Saudi culpability in the murder of Khashoggi and the Anglo-American-led campaign to publicly attribute Chinese, Iranian, North Korean and Russian covert activities since 2017 have all been similarly motivated.[44] 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, shaping the political and normative operational environment in which they take place, and building public- and private-sector resilience to their activities.[45] As scholars such as Jon Lindsay, Florian Egloff and Joe Devanny have argued, in practice using public attributions for deterrence and norm-shaping is not a straightforward proposition, especially concerning cyber intrusions.[46] For a range of reasons, Devanny and colleagues concluded that 'the public diplomacy of coordinated attribution statements cannot be expected to cut through conclusively or uniformly' in managing hostile-state cyber powers.[47] Nevertheless, a range of Western actors have sought to signal to adversaries and problematic partners through intelligence disclosures that they cannot necessarily act with impunity and that their behaviour carries costs.

Support, action, resilience and incrimination gains are generally internally driven motives within governments and state bureaucracies, albeit interacting with external events and actors. The fifth motive for disclosing intelligence to influence external audiences, *third-party pressure*, is more externally driven. It is also becoming an increasingly prevalent factor in government decision-making. As state monopolies on information flows continue to erode and state transparency increases, non-state third parties – from traditional journalists, to open-source intelligence (OSINT) investigators such as Bellingcat and the Centre for Information Resilience, to civil-society initiatives such as the University of Toronto's Citizen Lab, to cyber-security and technology firms – 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.[48] The trend for military deployments like Russia's in Ukraine 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, pored over and publicised by sundry independent, open-source analysts.[49] Similarly, Russian and pro-Russian humanitarian atrocities and disinformation networks have been independently exposed during the

conflict.[50] These global trends mean non-state third parties are gaining the ability to influence internal state decision-making.

Much like the escalation costs of disclosing intelligence discussed below, these actors' disclosures can constrain governments' policy and operational choices, and encourage their own disclosures, for two main reasons. Firstly, the perceived need to correct or provide greater precision to a highly contested, open information environment in a way that favours the state discloser may encourage governments to give up the advantages of secrecy. Fragmentary OSINT reporting may not be considered authoritative, or may be potentially confusing and open to manipulation through dis- or misinformation, a factor that has affected public responses to cyber incidents.[51]

Secondly, considerations of reputation management and the possibility of public humiliation if a third party reveals certain information can make the costs of greater transparency less than those of concealing intelligence, making it harder not to act. Referring to OSINT reporting that may have emerged, journalists and public-interest groups may demand to know what the government knows or believes, adding to internal policy pressure. The need to be first in revealing information and influencing narratives – and then to assertively respond in other ways – may be especially acute when the disclosing state itself has been the victim of intelligence collection or an influence operation. Devanny, Ciaran Martin and Tim Stevens argue that this is especially true in cyberspace, where collateral damage affecting the private sector, civil society and public life is more immediately known to third parties. Governments, therefore, have less control over decision-making and narratives.[52] Political calculations concerning the use and deployment of intelligence for influence may be altered in ways that will not be entirely clear until the internal correspondence of state bureaucracies and national leaders is declassified.

Seeking gains in Ukraine

The use of intelligence for influence during the Ukraine crisis demonstrates that none of these motives exist in isolation from the others, but rather can interact. Imposing incrimination costs on Russia has been the primary driver, aiming to illuminate Moscow's efforts to operate covertly

in the so-called 'grey zone'. Doing so could deny Putin the luxury of gains through quasi-deniable activities, of sowing confusion and paralysis in Ukraine and internationally, of a surprise attack to rapidly decapitate the Kyiv government, or of a credible and legitimate pretext for doing so to impose a 'normalised' new order.

Judging by the words of key stakeholders, 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 24 February of deterring Putin from covertly subverting President Volodymyr Zelensky's government in Kyiv or overtly invading Ukraine. From Burns's visit to Moscow in early November 2021 onwards, these were private and public intelligence-led 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. Speaking in Parliament on 25 January, for example, British Prime Minister Boris Johnson claimed that declassification of 'compelling intelligence' on Russia's intent to install a puppet regime in Ukraine and its covert cyber sabotage, false-flag operations and disinformation was intended to help achieve 'credible deterrence'.[53] This kind of spotlight made it more difficult for Russian information warriors to operate in the grey zone and generate confusion through their own manufactured intelligence 'exposures'.

Experts have been calling for such a spotlight to counteract Russian activities since Moscow's partially concealed invasion of Crimea and Donbas in 2014. Then, unlike in the current crisis, senior intelligence officials blocked the Obama administration from publicly disclosing what they knew about Russian sponsorship of and actions by unacknowledged 'little green men'. NATO was limited to publicly releasing commercial-satellite images of the build-up of Russian forces along the Ukrainian border, a precursor to the more extensive availability and use of such imagery this year. Western intelligence officials have pointed to similar decisions not to disclose intelligence surrounding Russia's invasion of Georgia in 2008 and intervention in Syria in 2015 as also informing their thinking. 'We have learned a lot, especially

since 2014, about how Russia uses the information space as part of its overall security and military apparatus', said Emily Horne, the spokeswoman for the US National Security Council, before Russia's 2022 invasion. 'And we have learned a lot about how to deny them some impact in that space.'[54] In Ukraine, however, British and American efforts failed to achieve strategic deterrence. Future historians may be able to determine from Russian sources if disclosures had any deterrent or disruptive effect on Russian plans.

It is possible that intelligence efforts before the invasion of Ukraine 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'.[55] Similarly, as the invasion began to unfold, British Secret Intelligence Service Chief Richard Moore noted that the pre-emptive exposures his service had supported had revealed that Russia's 'attack was long planned, unprovoked, cruel aggression. No amount of Russian disinformation will now disguise that fact from the international community.'[56] Exposing Russian intelligence agencies' use of media assets to propagate disinformation – such as false allegations of American mercenaries introducing chemical weapons into Donetsk and Luhansk, of Ukrainian armed provocations against these self-declared republics, and of 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. Continually pre-empting possible Russian courses of action kept NATO on the front foot and helped with credibility and narrative control in cases where Russia's actions followed these intelligence-led predictions.[57]

It is also notable that British and American intelligence-led exposures evolved, from strategic warnings from November through January relying mainly on OSINT and less sensitive imagery revealing Russian military capabilities and intentions, to more granular and regular disclosures in January and February of the Kremlin's efforts to create a credible pretext for invasion, likely drawing on more sensitive intelligence to hammer home the weaknesses of justifications built on quicksand. This may simply have reflected Russian planning timelines or the dates on which Russian

activities became more concrete and visible. Yet this shift may also have been driven by a change in Western officials' primary aim, from seeking to deter Russian aggression to seeking narrative superiority as the crisis escalated towards an invasion. The West's countermeasures were intended to undermine support for Moscow's claims that an invasion was not going to happen even as it was simultaneously trying to build a justification for an invasion. Those willing to listen among fence-sitting Ukrainian, European and global audiences could be in little doubt that Moscow was saying one thing but doing another.

Since the invasion, intelligence disclosures have continued apace, targeting not only Russia but also China. The US highlighted OSINT revealing Russian recruitment of Wagner Group mercenaries early in the conflict, since independently confirmed.[58] The UK, through a public speech at Australian National University by GCHQ director Jeremy Fleming and UK Defence Intelligence daily briefings, has revealed significant deterioration in Russian military morale, cohesion, and command and control; how Putin was allegedly misled regarding expected Ukrainian resistance by fearful advisers; and how he has subsequently become involved in battalion-level decision-making.[59] Concerning Beijing, the Biden administration and European partners have confidentially briefed trusted media contacts with intelligence on Chinese involvement in Russian planning before the invasion, shared with allies assessments indicating Chinese openness to providing Russia with security assistance, and publicised OSINT assessments of Chinese propaganda support for Russian disinformation.[60] Similarly, Ukraine – likely with British and American support – supplied intelligence assessments to British media alleging that China had supported Russia with massive cyber attacks on Ukrainian military and nuclear facilities immediately before the invasion.[61]

Such disclosures have served the aims of incriminating and embarrassing Russia and China while helping to head off domestic and international criticisms of more resolute support for Ukraine and sanctions against Russia as 'Western aggression'. Public and private exposures provided reasons to justify these countermeasures and, therefore, generated support. Criticisms of alleged intelligence and policy failures surrounding the American and British

withdrawal from Afghanistan in summer and autumn 2021 were probably also still in the minds of many Whitehall and White House policymakers.[62]

Moreover, in combination with private lobbying and intelligence-sharing, this campaign likely sought to move European and NATO allies to adopt more resolute positions and to forestall the divided and confused response that Putin was likely counting on. Weak alliance cohesion had characterised NATO responses to the Russian invasions of Crimea and Donbas in 2014, exacerbated by initially poor intelligence-sharing. Senior Obama administration officials were frustrated when US intelligence agencies would not allow the White House to tell NATO, let alone the public, what Washington knew about Russia's actions.[63] This time, the UK and US intelligence communities privately shared much more, and more granular, intelligence on Russian actions, capabilities and intentions. US Director of National Intelligence Avril Haines visited NATO headquarters to share assessments in November 2021, two weeks after Burns visited Moscow, marking the start of much more regular intelligence-sharing on Russia, with visits to and calls with European partners by Haines, Burns and other senior leaders in the run-up to the invasion.[64] Parallel public disclosures placed further pressure on allies that may have been hesitant to take firmer actions, such as France and Germany, particularly when Russia indicated (falsely) that it was withdrawing troops from Ukraine's border. This deception itself was exposed through US and allied intelligence-led communications.[65]

Public disclosures placed pressure on allies

In December and early January, before the US and UK began making regular, detailed, public statements on Russian plans and actions, the coalition government of newly elected German Chancellor Olaf Scholz seemed intent on pursuing a 'new start' with Moscow, focused on energy politics and framing the Nord Stream 2 gas pipeline from Russia as a 'private economy project'.[66] By mid-February, when public intelligence exposures had become almost daily, Scholz had begun 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

publicly threatening to cancel Nord Stream 2 or promising to change the long-standing German policy of not providing lethal security assistance until the Russian recognition of Ukraine's breakaway provinces and subsequent invasion forced his hand.[67]

It is also notable that the French and German intelligence and policy communities did not initiate their own exposures of Russian intentions and actions. This can be explained in part by both countries' less hostile strategic positioning towards Russia before the current crisis and the desire of both Scholz and French President Emmanuel Macron to retain political flexibility for their ultimately unsuccessful shuttle diplomacy with Putin.[68] French and German exposure campaigns would have constrained their policy choices. There were also operational factors at play. Neither state had the capability to collect intelligence at the scale or with the access of the Anglo-American joint effort, or an established process for conducting such an intelligence-led campaign against adversaries. More importantly, the French intelligence community, much as it was in the lead-up to the Iraq War, was sceptical of Anglo-Saxon assumptions and, given that the Anglo-American effort was indeed intended to influence French actions, suspicious of its motives. The fact that American and British sources could not be shared, and that French assessments assumed Russia was bluffing, did not help to overcome French incredulity at British and American claims. Almost until the eve of the invasion, therefore, French public messaging still indicated that an invasion was not coming, informed by France's own incorrect military intelligence and assessments by the Directorate-General for External Security. General Eric Vidaud, chief of France's Directorate of Military Intelligence, subsequently lost his job due to this failure.[69]

It is clear that Anglo-American intelligence-led exposures did not influence all key allies towards a completely uniform position. Nevertheless, NATO partners like France and Germany were increasingly unable to hide behind private British and American intelligence-sharing and diplomacy to retain their prior positions on Russia due to growing public lobbying in their legislatures, civil societies, and domestic and international media – lobbying that was spurred, in part, by public intelligence. In this way, the British and American effort to corral international allies with intelligence

was not revolutionary, but comparable to previous intelligence-led 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 the literature, including the classic paradox of access and utility: the better a source's access, the more challenging it becomes to use it for fear of being compromised. Using intelligence to influence external audiences entails exaggerated risks, especially if done publicly in an attributable manner, generating 'disclosure dilemmas' and trade-offs.[70] Indeed, these risks may typically dissuade states from taking such action, depending on the type and granularity of the intelligence being used, the sensitivity of its subject matter, the method of dissemination and the sensitivity of the government to matters such as domestic trust. Some will be especially sensitive. In London and Washington, policymakers and intelligence officers alike still remember the reckoning they faced after using intelligence publicly to support the Iraq War through exaggerated and inaccurate efforts to incriminate. The Ukraine crisis may have rehabilitated the perceived ability of both the British and American intelligence communities to justify foreign interventions in the eyes of some sceptics. The Kremlin cares less about domestic reputational harm to its intelligence services.

The risks of disseminating sensitive information to external audiences can be split into several categories. The first, *adaptation costs*, will be familiar to those who have, for example, observed the fallout from unauthorised leaks such as Edward Snowden's, with terrorist groups such as al-Qaeda and transnational organised-crime groups quickly upgrading their communications encryption.[71] Similarly, authorised disclosures, such as the release of satellite images of adversaries' concealed nuclear sites (as during the Cuban Missile Crisis), may encourage and enable them and other proliferators to better hide their activities to avoid future detection. The utility of certain intelligence sources is closely correlated with their secrecy. If secrecy is compromised, access may be too, empowering targets to adjust their security and counter-intelligence measures to harm the discloser.[72] In the case of human

intelligence, a source's well-being could also be jeopardised. Aimen Dean, an extremely useful British agent inside al-Qaeda, experienced this following a decision, allegedly from the office of then-vice president Dick Cheney, to brief a journalist about him. Developing and running such an asset was difficult and time-consuming. Adapting to his loss was a significant endeavour.[73]

This risk applies to all categories of intelligence. Following Stanley Baldwin's 1927 revelations before Parliament relating to the ARCOS raid, the Soviet government predictably changed its encryption codes. This, combined with the expulsion of the Soviet trade delegation, significantly reduced the ability of Britain's Government Code and Cypher School to decrypt high-grade Soviet diplomatic – though not Red Army – communications for the next two decades. New recruits to the British service were told the story of this loss of access as a warning of politicians' indiscretion.[74] Nearly 60 years later, in 1986, Ronald Reagan justified a US strike on Libya in retaliation for the state-sponsored bombing of a disco in West Berlin by referring to signals-intelligence intercepts of Muammar Gadhafi's government that allegedly exposed its culpability. To the dismay of the US National Security Agency, this may have raised Iran's suspicions about American access to Iranian communications, achieved through compromised Swiss encryption machines Tehran shared in common with Tripoli.[75] Developing such access is difficult, losing it is easy, and adapting to its loss is a complex undertaking. This is why many former British and American intelligence practitioners have reacted warily to their governments' behaviour before and during the Ukraine war.[76]

Developing access is difficult, losing it is easy

Adaptation costs also explain, in part, why states seeking to impose incrimination costs on adversaries often prefer to do so by disseminating intelligence privately or indirectly, or by relying on OSINT when doing so publicly. For example, at a time when third-party access to OSINT was much less widespread than today, Britain's Cold War anti-communist propaganda body, the Foreign Office's Information Research Department, developed a global OSINT-collection network from overseas state and non-state broadcasts, publications, print journalism and public events. This was collated for

analysts to process and editors to repurpose as ammunition for propaganda exposing adversaries' actions, intentions and ways of life through indirect, unattributable methods. The Information Research Department 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.[77]

Of course, knowledge of any channels – including open-source ones – used by an intelligence service to inform governmental assessments, or by third parties to verify them and shape public discourse, can offer adversaries or mischief-makers a vector for deception operations using disinformation and so-called 'chicken feed' (accurate but unimportant information). Warning of the risks of public intelligence use prior to Russia's invasion of Ukraine, McLaughlin noted that US publication of intelligence derived from clandestine sources had encouraged such behaviour by another (unnamed) adversary in the past.[78] It is even easier for adversaries to pollute publicly available information for this purpose. Moreover, adversaries may adapt when they realise what use is being made of open sources, as Russia sought to do through changes to front-line soldiers' access to mobile phones and social media after Bellingcat's revelations of Russian complicity in the shooting down of Malaysia Airlines Flight 17 using these sources.[79] Thirdly, removing sensitive information from disclosures risks reducing the desired gains by generating credibility problems. Documents published by national intelligence agencies that appear to rely more or less entirely on publicly available information may cause the public to react with confusion or scepticism, asking 'is this all there is?' This carries the risk of undercutting the authority of the intelligence and its distributors: if a disclosure cannot demonstrate any advanced or special access, why should it necessarily be taken any more seriously than an ordinary government press release?

Nevertheless, using OSINT undoubtedly poses fewer risks than using secret sources. This was the Information Research Department's view during the Cold War. Being more readily citeable, OSINT was considered key for exposures to be deemed credible by intermediary and target audiences.[80] Using intelligence publicly for incrimination gains, in particular, introduces the prospect of a third-party challenge. This dynamic has changed little

since the Cold War, although the information environment *has* changed, especially in terms of the volume of conflicting and confusing data openly available. Achieving the desired impact today – especially when using direct, public communications compared to more indirect, unattributed methods – therefore depends even more on institutional reputation and the credibility and verifiability of the information.

It is becoming easier for governments to talk publicly about some topics, such as malign cyber activities. Their improving ability to cite open, verified voices represents the flip side of non-state third parties' growing capability to independently disclose information. The ability of cyber-security firms and OSINT investigators to conduct more extensive research and analysis to triangulate sources and test claims can strengthen those state actors seeking to expose adversaries by verifying their evidence. But it can also undermine them by exposing fabricated material and false narratives that had been intended to incriminate.

Little state intelligence was needed to support independent analysts

Russian intelligence officers and propagandists have discovered 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 Russian narratives.[81] London's and Washington's previous warnings of 'fake-news farms' and covert propaganda fronts may have heightened alertness to Russia's duplicitous methods,[82] but little state intelligence was needed to support independent analysts once their verification checks spun into action. With the help of third parties and affected stakeholders such as 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.[83]

These considerations make the Russia–Ukraine case that much more significant. In 2018, for example, the British government leaned on Bellingcat's revelations in exposing Moscow's attempted assassination of

Skripal, revelations that had more currency as a result.[84] That London and Washington have been willing to use secret intelligence – albeit in a highly sanitised manner – for their exposures concerning Ukraine, rather than simply leaning on widely available OSINT on Russian troop movements and capabilities, highlights the gravity of the crisis. In both capitals, this has been done in a highly orchestrated manner to balance the expected gains and risks, with intelligence and policy leaders notably marching in lockstep.

In the UK, there has been an integrated intelligence-policy process built through the Joint Intelligence Organisation structure. Once the Joint Intelligence Committee, which tops this structure, produced a strategic assessment in late 2021 judging a Russian invasion to be 'highly likely', a process was launched, in parallel to a similar effort in Washington, to vet intelligence collected by GCHQ, the Secret Intelligence Service and their American partners 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'.[85]

Since early February 2022, intelligence for external influence, once declassified, has been managed by a new inter-departmental unit, the Government Information Cell. It was stood up 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. The cell draws on expertise from numerous government departments in analysis, communications, disinformation and behavioural science as it assesses intelligence on Russian propaganda, guides government messaging and disseminates output in Russian, Ukrainian, German, Arabic and Mandarin through social-media and private-sector partners. These include advertising agencies, contracted to disseminate messages to target audiences through more credible cultural intermediaries than official UK government platforms. It also shares intelligence on Russian disinformation with NATO, the EU, and Australian and New Zealand partners to encourage and inform their own actions.[86] The cell fulfils the call of Parliament's Intelligence

and Security Committee's scathing 2020 Russia report to assign a lead organisation to tackle Russian disinformation.[87] It has 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. Reflecting on the cell's use of intelligence, GCHQ director Fleming has commented that 'intelligence is only worth collecting if we use it, so I unreservedly welcome this development'.[88] Notably, the cell's mission to use intelligence and 'the truth, well told' to tackle hostile Russian propaganda and disinformation also closely parallels that of Britain's Cold War Information Research Department when formed in 1948. This parallel has not been lost on one of its champions, Foreign Secretary Liz Truss, an ally of whom explained that she 'thinks ditching our Cold War anti-propaganda capability was a mistake and has restored it with this new information unit'.[89]

In the US, Haines, Burns and National Security Advisor Jake Sullivan have led the initiative to use intelligence on Russia for external influence since autumn 2021. Their efforts were authorised by President Biden and have been planned and coordinated by the US National Security Council. Experts on declassification were brought in to weigh up the risks and establish what could be shared with both allies and the public. Burns, before joining the intelligence community, was a highly respected diplomat and intelligence consumer with deep experience of Russia – including as US ambassador to Moscow. This background, together with the relationships he has built with other stakeholders, has reportedly helped him to manage the dilemmas and bureaucratic politics that can accompany this kind of intelligence use. His close relationship with President Biden was exemplified by his dispatch to Moscow to communicate American intelligence on Russian planning to Putin, whom he also knew well.[90]

Yet for some CIA Cold Warriors with a pre-digital view of how intelligence 'should' be used, the US has gone too far. 'If [Putin] knows where his regime is compromised, he may be planting these threats for our side to pick up', noted Burton Gerber, a former Moscow chief of station and chief of

the CIA's Soviet Division, just before the Russian invasion. 'I think our side has said too much.'[91] Nevertheless, sources within today's CIA have pointed to internal contentment with the Biden administration's approach as proof of its confidence in Burns's stewardship, both in this particular instance and more generally.[92] Given that the British and American intelligence communities have been leading and their policy communities supporting, this has helped to overcome fears among intelligence practitioners in both countries about reckless politicians leading the charge.

Yet even with such well-oiled processes, British and American leaders have frequently found themselves in a bind by using sanitised intelligence publicly. Disseminating scrubbed communications derived from sensitive sources, while eagerly reported on in international media, has prompted distrust and even derision in cases where such communications were not supported by more granular – or indeed any – supporting evidence. For example, when State Department spokesperson Ned Price outlined a deep-fake operation allegedly being weighed by the Kremlin as a pretext for invasion, 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.[93] There are adaptation costs to going further, but also costs for not doing so. Establishing a precedent for openness risks increased demands for and expectations of access, which require management through building credibility with external audiences to gain trust without having to provide sensitive specifics.

Some CIA Cold Warriors think the US has gone too far

Exposing the intentions and actions of adversaries or allies can also incur *escalation costs* by imposing constraints on policy and operational decisions. Throughout the Cold War, covert influence operations enabled the principal states to pursue their interests while mitigating the risk of direct confrontation with each other. As Austin Carson has argued, doing this secretly also allowed them to signal their intent, priorities and core interests to each other in a manner that did not bind governments by raising the political pressures of public and elite expectations or domestic approval ratings.

Similarly, maintaining secrecy allows the parties to retain the plausible deniability of any counteraction and to reach clandestine agreements that might not be viewed favourably by domestic or international audiences. For these reasons, during the Cold War Washington and Moscow often, but not always, refrained from exposing each other's covert operations, especially during periods of crisis. Harry Truman's government, for example, chose not to expose the intelligence it obtained revealing that Soviet pilots were participating in the Korean War. Removing the grey zone by protesting publicly risks limiting the options at states' disposal and their flexibility of action by closing a clandestine diplomatic safety valve.[94] This kind of escalation risk is still present today. Once his government's plans and capabilities had been exposed, could Putin have backed down from invading Ukraine without losing face, assuming this remained a consideration?

This dynamic can likewise be observed in other elements of the conflict, further underlining the care that policymakers should take when moving intelligence out of the shadows. Accompanying controlled public disclosures and private sharing among governments have been unauthorised leaks and briefings – especially from US government insiders – to enterprising journalists. These have detailed sensitive support for Ukraine's armed forces with targeting intelligence.[95] Of particular concern were revelations in April and May that US intelligence helped Ukrainian forces target senior Russian officers, enabling the killing of several high-ranking generals, as well as the sinking of the *Moskva*, the erstwhile flagship of Russia's Black Sea Fleet.[96] Such leaks carried a clear escalatory potential as they dispelled the illusion that US and NATO involvement was limited to disseminating incriminatory intelligence about Russian intentions, capabilities and actions, and providing Ukraine with security assistance that restricted the transfer of offensive weaponry. Each additional revelation – uncontrolled or otherwise – is another straw on the camel's back.

As Carson shows in his book *Secret Wars*, in order to manage escalation risks, states have historically been willing to publicly downplay the nature of third-party adversary involvement in their conflicts, even when privately they may suspect or know otherwise.[97] But supplying targeting intelligence is provocative, and publicising it more so. Such disclosures can feed Russian

propaganda about NATO 'aggression', and restrict Putin's policy and operational choices in how he manages the expectations of Russia's public and elites. President Biden's reportedly livid response to the leaks clearly indicates an awareness among his senior leadership team of the escalatory dangers; he is said to have warned Haines, Burns and Secretary of Defense Lloyd J. Austin III that 'this kind of loose talk is reckless and has got to stop immediately – before we end up in an unintended war with Russia'.[98] Putin, given his conspiratorial mindset, is unlikely to view an unauthorised leak any differently from a controlled release. Provoking a leader who increasingly identifies the survival of his regime with his own personal survival seems particularly risky given his apparent interest in the idea of 'escalating to de-escalate'.[99]

The release of sensitive information may become 'normalised'

While unauthorised leaks in liberal democracies are more commonplace than their national leaders would prefer, the release of sensitive information may become 'normalised' as part of the prevailing national policy, potentially causing the boundaries between strategic, deliberate disclosures and unauthorised revelations to become blurred, both by external observers and internal officials. This may be particularly true when agencies or individuals, driven by bureaucratic politics, feel the need to claim credit for significant events in which they had a hand. This phenomenon has been observable during the Ukraine crisis but has historical precedents, such as in the steady stream of leaks from the US intelligence community concerning responsibility for the Stuxnet attack on Iran's nuclear programme.[100] If the strategic deployment of intelligence for influence is to become a more frequent element of international affairs, including at tense moments involving nuclear-armed actors, institutional processes to maintain potentially escalatory secrets and control intelligence-supported narratives will require careful thought and reinforcement.

Adaptation and escalation costs are not the only considerations. There is also a series of potential *audience costs*, including 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, when the UK deployed military forces to newly independent Kuwait to defend it against an Iraqi attack British intelligence believed to be imminent but that, following the deployment, never came.[101] In cases where a public audience lacks the complete picture, this could undermine the credibility of intelligence assessments and the organisations that produce them. Worse, it could offer adversaries a weapon to wield in future crises. During the build-up to the invasion of Ukraine, Russian officials frequently referred to the flawed intelligence publicised by the US and UK before the disastrous Iraq War as a means of undermining the credibility of ongoing intelligence revelations.[102] The visibility of Russia's actions in the run-up to its invasion may have been so clearly indicative of hostile intent that the risk of publicising the intelligence was acceptable, though the risk remained 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 be careful to protect their credibility with the public, as well as their utility to policy.

Additionally, the risk of mixing intelligence too closely with politics is a difficult one to manage. Intelligence is there to be used, and intelligence services provide just that, a service. They must be responsive to the requirements and priorities of policymakers. But they should not subscribe to the service provider's mantra of the customer always being right. Indeed, it is likely that one of the reasons for Russia's intelligence failings before and during its invasion was a tendency among intelligence officers to tell their chief customer precisely what he wanted to hear.[103] Speaking to British prime minister James Callaghan in the 1970s, Maurice Oldfield, then chief of the Secret Intelligence Service, noted that his job was to 'bring unwelcome news'.[104] This is easier to do when the entire conversation is in secret; officers can stand their ground and be damned. But when intelligence is deployed publicly it is inherently political, lacks the nuance of secret communications, and is consumed by a public that is largely unfamiliar with the uses and limits of intelligence.

This is a perilous environment for intelligence agencies to navigate. Their assessments grapple with uncertainty and ambiguity, and communicate

probabilities, with source reporting rarely definitive. Yet in extreme cases, policymakers who deploy intelligence in public may lean on their officers to give direct, unambiguous assessments that clearly communicate *a* threat without fully capturing *the* threat. As the case of Iraq's supposed weapons programme demonstrated, high-pressure, high-stakes circumstances may heighten the risk of unwitting politicisation, causing reputational damage as incomplete and overly spun intelligence is made public.[105] Citizen audiences remember intelligence failures and may be understandably suspicious of politicians who wield 'intelligence' as the justification for serious policy choices. Indeed, before Russia's invasion of Ukraine, the Iraq case was repeatedly mentioned by sceptical media reporting on the British and American intelligence revelations. 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, heightening suspicions and damaging trust. As the 2004 UK Butler Report concluded in reflecting on the public use of intelligence on Iraqi weapons of mass destruction, careful explanations of intelligence uses and limitations are needed, together with clearer and more effective dividing lines between assessment and advocacy – something that may not sit well with policymakers hoping to use intelligence to incriminate, justify and persuade.[106]

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 we be entering a new age of intelligence diplomacy, in which intelligence is increasingly used for external influence as well as internal consumption in sustained offensives, not merely surgical strikes? It is highly likely that, having witnessed how the judicious use of intelligence in the build-up to the invasion of Ukraine allowed Western governments to pre-emptively undermine Russia's narratives and claims, policymakers will wish to reap similar rewards in future crises. The UK government, for example, is investing in an OSINT and artificial-intelligence centre – the Centre for Emerging Technology and Security based at the Alan Turing Institute – to reinforce its ability to publicly counter hostile disinformation.[107]

Many former senior security practitioners in the US have also voiced their support for using intelligence in this way. Rolf Mowatt-Larssen, a former CIA deputy chief of station in Moscow and later chief of the Counterterrorism Center, has hailed a 'new paradigm for intelligence'.[108] US intelligence leaders who earned their stripes during and after the Cold War have been equally supportive of this method of contesting the information space, including former CIA directors Leon Panetta, Michael Hayden and John Brennan; former CIA deputy director of intelligence Michael Morrell; and former director of national intelligence James Clapper.[109] Brian Murphy, a former acting under secretary for the Office of Intelligence and Analysis at the Department of Homeland Security, has gone further, calling for a new US inter-agency 'Centre to Counter Foreign Malign Influence' that would counter influence operations not just abroad but at home too. Inspired by the resilience mission of bodies such as the UK's National Cyber Security Centre and the FBI's InfraGard programme in the cyber-security sector, it would disseminate all-source intelligence on foreign state-backed disinformation to key governmental, civil-society and private-sector stakeholders, making 'citizens aware of misconduct by hostile foreign actors'.[110] A report by the Atlantic Council has recommended a similar intensification of intelligence-led exposures of Russian influence activities as one of three measures to protect the integrity of the 2024 national elections.[111]

Veterans of the Cold War have reason to warn that 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.[112] Nevertheless, this is a development broadly to be welcomed, so long as adaptation costs are managed; the integrity of the analytical process is respected; the professional judgement of intelligence officers is uncompromised; and a critical eye is cast over government releases. Intelligence is an element of state power. Employed judiciously, it has its uses in the public sphere, just as it does in its more natural, secret habitat. A matter as serious as deterring and managing a war affecting a country's core national interests merits the deployment of the nation's capabilities. The threshold for such deployments may well be lowered as global inter-state competition continues to deepen.

Notes

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, U.S. Officials Say', *New York Times*, 2 March 2022, https://www.nytimes.com/2022/03/02/us/politics/russia-ukraine-china.html.

3 See Andrew Roth, Dan Sabbagh and 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 Alexander 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 See Gordon Corera, 'Ukraine War: Western Agents Seek to Get Inside Putin's Head', BBC News, 20 March 2022, https://www.bbc.co.uk/news/world-europe-60807134.

6 See 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; and Shane Harris and Paul Sonne, 'Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. 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 et al., 'U.S. 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; and Sean Lyngaas and Zachary Cohen, 'US Accuses Moscow Spies 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 See Katie Bo Lillis, Natasha Bertrand and 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; and 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 Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US 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 Foreign and Commonwealth Office, 'Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks', 19 December 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; Foreign and Commonwealth Office, 'Foreign Office Minister Condemns Russia for NotPetya Attacks', 15 February 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks; Cabinet Office, 'Letter from the UK National Security Adviser to the NATO Secretary General', 13 April 2018, https://www.gov.uk/government/publications/letter-from-the-uk-national-security-adviser-to-the-nato-secretary-general; Foreign and Commonwealth Office and National Cyber Security Centre, 'UK and Allies Reveal Global Scale of Chinese Cyber Campaign', 20 December 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign; and Foreign and Commonwealth Office, 'Gulf of Oman Attacks: UK Statement', 14 June 2019, https://www.gov.uk/government/news/gulf-of-oman-attacks-uk-statement.

11 See 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 See, for example, UK Ministry of Defence (@DefenceHQ), tweet, 17 February 2022, https://twitter.com/DefenceHQ/status/1494344646864031758; and UK Ministry of Defence (@DefenceHQ), tweet, 7 March 2022, https://twitter.com/DefenceHQ/status/1500885976146759686.

13 See Sabbagh, 'Ukraine Crisis Brings British Intelligence Out of the Shadows'.

14 For an example of a probability yardstick, see College of Policing, 'Delivering Effective Analysis', 30 January 2020, https://www.app.college.police.uk/app-content/

intelligence-management/analysis/delivering-effective-analysis/.

15 See Julian Borger, 'Vitaly Gerasimov: Second Russian General Killed, Ukraine Defence Ministry Claims', *Guardian*, 8 March 2022; Isaac Stanley-Becker and Vanessa Guinan-Bank, 'Germany Intercepts Russian Talk of Indiscriminate Killings in Ukraine', *Washington Post*, 7 April 2022; Andrew Higgins, 'He Was a Penniless Donor to the Far Right. He Was Also a Russian Spy', *New York Times*, 20 April 2022; and UK Foreign, Commonwealth and Development Office, 'UK Exposes Sick Russian Troll Factory Plaguing Social Media with Kremlin Propaganda', press release, 1 May 2022, https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda.

16 See 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/; and Stephanie van den Berg, 'Russian No Show at U.N. 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/.

17 See Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive II: The KGB and the World* (London: Allen Lane, 2005), pp. 435–42; and Calder Walton, 'False-flag Invasions Are a Russian Specialty', *Foreign Policy*, 4 February 2022, https://foreignpolicy.com/2022/02/04/false-flag-invasions-are-a-russian-specialty/.

18 See 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/.

19 See Andy Greenberg, 'A Brief History of Russian Hackers' Evolving False Flags', *Wired*, 21 October 2019, https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/; and Leigh Hartman, 'How Russia Conducts False Flag Operations', US Embassy in Georgia, 24 January 2022, https://ge.usembassy.gov/how-russia-conducts-false-flag-operations/.

20 See Linda Kay, 'Ukraine Hastily Destroyed Pentagon-funded Biological Program: Kremlin', *Defence World*, 6 March 2022, https://www.defenseworld.net/2022/03/06/ukraine-hastily-destroyed-pentagon-funded-biological-program-kremlin.html; and 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/.

21 See Milton Leitenberg, 'China's False Allegations of the Use of Biological Weapons by the United States During the Korean War', Wilson Center, Cold War International History Project Working Paper no. 78, 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', *Nonproliferation Review*, 12 October 2021, https://doi.org/10.1080/10736700.2021.1964755; Joseph A. Gambardello, 'Social Media Posts Misrepresent U.S.–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/; and Dan Sabbagh and 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.

22 UK 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; and 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.

23 Office of the Director of National Intelligence, 'Assessing the Saudi Government's Role in the Killing of Jamal Khashoggi', 11 February 2021, https://www.dni.gov/files/ODNI/documents/assessments/Assessment-Saudi-Gov-Role-in-JK-Death-20210226v2.pdf.

24 Center for the Study of Intelligence, 'The Cuban Missile Crisis of 1962: Presenting the Photographic Evidence Abroad' (first published in *Studies in Intelligence* in 1972), https://irp.fas.org/imint/cubakent.htm.

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

26 See 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; and Gordon Corera, 'Ukraine: Inside the Spies' Attempts to Stop the War', BBC News, 9 April 2022, https://www.bbc.co.uk/news/world-europe-61044063.

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

28 See Thomas Boghardt, 'Soviet Bloc Intelligence and Its AIDS Disinformation Campaign', *Studies in Intelligence*, vol. 53, no. 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*, vol. 21, no. 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, vol. 3, no. 4, Fall 2020, pp. 10–29; and Nomaan Merchant, 'US Accuses 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.

29 See Christopher Andrew, *The Defence of the Realm: The Authorized History of MI5* (London: Allen Lane, 2010), pp. 154–6.

30 Richard J. Aldrich, 'Whitehall and the Iraq War: The UK's Four Intelligence Enquiries', *Irish Studies in International Affairs*, vol. 16, 2005, pp. 73–88; and Robert Jervis, 'Reports, Politics, and Intelligence Failures: The Case of Iraq', *Journal of Strategic Studies*, vol. 29, no. 1, 2006, pp. 3–52.

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

32 See 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/; and Institute for Science and International Security, 'U.S. Allies Were Not Persuaded by U.S. Assertions on Iraq WMD', 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.

33 See Steve Coll, *Directorate S: The C.I.A. and America's Secret Wars in Afghanistan and Pakistan, 2001–2016* (New York: Penguin, 2018); and 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.

34 See David M. Halbfinger, 'Israel Presses the Case Against Iran, but Not for War', *New York Times*, 16 May 2019, https://www.nytimes.com/2019/05/16/world/middleeast/israel-iran-netanyahu-war.html.

35 See Ellen Nakashima and Brian Fung, 'U.S. Allies Differ on Difficulty of Containing Huawei Security Threat', *Washington Post*, 6 March 2019; and 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/.

36 See Julian Borger et al., 'Western Allies Expel Scores of Russian Diplomats over Skripal Attack', *Guardian*, 27 March 2018.

37 The Joint Terrorism Analysis Centre threat level is published on the UK Security Service website at https://www.mi5.gov.uk/threat-levels.

38 See the National Cyber Security Centre's 'Cyber Threat' website at https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=cyber%20threat&sort=date%2Bdesc.

39 Erkki Koort et al., 'Hybrid Threats and Their Impact on European Security: Seminar Summary', Intelligence College in Europe and Internal Security Institute, Estonian Academy of Security Sciences, June 2021, https://

www.intelligence-college-europe.org/webinar-hybrid-threats-and-their-impact-on-european-security/.

40 Lesley Seebeck et al., 'Countering the Hydra: A Proposal for an Indo-Pacific Hybrid Threat Centre', Australian Strategic Policy Institute, Policy Brief Report No. 60/2022, 7 June 2022, https://www.aspi.org.au/report/countering-hydra.

41 See Allison Carnegie and Austin Carson, *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation* (Cambridge: Cambridge University Press, 2020), pp. 7–8.

42 The use of intelligence both in secret and publicly during the Cuban Missile Crisis has been extensively discussed. For a useful summary, see James M. Lindsay, 'TWE Remembers: Adlai Stevenson Dresses Down the Soviet Ambassador to the UN (Cuban Missile Crisis, Day Ten)', Council on Foreign Relations, https://www.cfr.org/blog/twe-remembers-adlai-stevenson-dresses-down-soviet-ambassador-un-cuban-missile-crisis-day-ten. For a more detailed discussion, see the essays in James G. Blight and David A. Welch (eds), *Intelligence and the Cuban Missile Crisis* (Abingdon: Routledge, 1998).

43 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', *Air Force Magazine*, 1 January 2013, https://www.airforcemag.com/article/0113korean/.

44 See James Landale, 'Transparency – The Tool to Counter Russia', BBC News, 4 October 2018, https://www.bbc.co.uk/news/uk-45751173.

45 White House, 'National Cyber Strategy of the United States of America', September 2018, p. 21, available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

46 Jon R. Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack', *Journal of Cybersecurity*, vol. 1, no. 1, 2015, pp. 53–67; Florian J. Egloff, 'Public Attribution of Cyber Intrusions', *Journal of Cybersecurity*, vol. 6, no. 1, 2020, pp. 1–12; Florian J. Egloff and Max Smeets, 'Publicly Attributing Cyber Attacks: A Framework', *Journal of Strategic Studies*, 10 March 2021, https://doi.org/10.1080/01402390.2021.1895117; and Joe Devanny et al., 'Strategy in an Uncertain Domain: Threat and Response in Cyberspace', *Journal of Strategic Security*, vol. 15, no. 2, 2022, pp. 34–47.

47 Devanny et al., 'Strategy in an Uncertain Domain: Threat and Response in Cyberspace', from the abstract.

48 On these trends, see Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington DC: Georgetown University Press, 2014); and Michael F. Joseph and Michael Poznansky, 'Media Technology, Covert Action, and the Politics of Exposure', *Journal of Peace Research*, vol. 55, no. 3, 2018, pp. 320–35.

49 See '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; and Christian Davenport, 'Commercial Satellites Test the Rules of War in Russia–Ukraine Conflict', *Washington Post*, 10 March 2022.

50 See Pranshu Verma, 'The Rise of the Twitter Spies', *Washington Post*, 23 March 2022; and Benjamin Strick, 'Eyes on Russia: Documenting Conflict and Disinformation in the Kremlin's War on Ukraine', Centre for Information Resilience, 15 May 2022, https://www.info-res.org/post/eyes-on-russia-documenting-conflict-and-disinformation-in-the-kremlin-s-war-on-ukraine.

51 See Florian L. Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia', *Contemporary Security Policy*, vol. 41, no. 1, 2020, pp. 55–81; and Devanny et al., 'Strategy in an Uncertain Domain', pp. 34–47.

52 Joe Devanny, Ciaran Martin and Tim Stevens, 'On the Strategic Consequences of Digital Espionage', *Journal of Cyber Policy*, vol. 6, no. 3, 2021, pp. 429–50. See also Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (London: Hurst, 2018).

53 House of Commons, 'PM Statement on Ukraine: 25 January 2022', https://www.gov.uk/government/speeches/pm-statement-on-ukraine-25-january-2022.

54 Julian E. Barnes and Helene Cooper, 'U.S. Battles Putin by Disclosing His Next Possible Moves', *New York Times*, 12 February 2022. See also Jake Harrington and Riley McCabe, 'Detect and Understand: Modernizing Intelligence for the Gray Zone', CSIS Brief, Center for Strategic and International Studies, December 2021; Felicia Schwartz and Demetri Sevastopulo, '"A Real Stroke of Genius": US Leads Efforts to Publicise Ukraine Intelligence', *Financial Times*, 6 April 2022; and David M. Herszenhorn, 'Satellites Show Russian Forces Poised Near Ukraine', *New York Times*, 10 April 2014.

55 President Joe Biden (@POTUS), tweet, 19 February 2022, https://twitter.com/POTUS/status/1494863649500168193.

56 Richard Moore (@ChiefMI6), tweet, 24 February 2022, https://twitter.com/ChiefMI6/status/1496939918416916484.

57 See Vladimir Isachenkov, 'Russians Scoff at Western Fears of Ukraine Invasion', ABC News, 15 February 2022, https://abcnews.go.com/International/wireStory/russians-scoff-western-fears-ukraine-invasion-82895312.

58 See Gordon Lubold, Nancy A. Youssef and Alan Cullison, 'Russia Recruiting Syrians for Urban Combat in Ukraine, U.S. Officials Say', *Wall Street Journal*, 6 March 2022.

59 Andres Schipani, Nic Fildes and John Paul Rathbone, 'Putin "Massively Misjudged" Ukraine War, Says UK Spy Chief', *Financial Times*, 31 March 2022; Dan Sabbagh, 'Putin Involved in War "At Level of Colonel or Brigadier", Say Western Sources', *Guardian*, 16 May 2022; and UK Ministry of Defence (@DefenceHQ), tweet, 19 May 2022, https://twitter.com/DefenceHQ/status/1527163546781483008.

60 See Edward Wong and Julian E. Barnes, 'China Asked Russia to Delay

Ukraine War Until After Olympics, U.S. Officials Say', *New York Times*, 2 March 2022; Demetri Sevastopulo, 'US Tells Allies China Signalled Openness to Providing Russia with Military Support', *Financial Times*, 14 March 2022; and US Department of State, 'People's Republic of China Efforts to Amplify the Kremlin's Voice on Ukraine', 2 May 2022, https://www.state.gov/disarming-disinformation/prc-efforts-to-amplify-the-kremlins-voice-on-ukraine/.

61 See Maxim Tucker, 'China Accused of Hacking Ukraine Days Before Russian Invasion', *The Times*, 1 April 2022.

62 See Katrina Manson, 'Taliban Rout Exposes US Intelligence Failings on Afghanistan', *Financial Times*, 16 August 2021; Mark Mazzetti, Julian E. Barnes and Adam Goldman, 'Intelligence Warned of Afghan Military Collapse, Despite Biden's Assurances', *New York Times*, 17 August 2021; Kylie Maclellan and Paul Sandle, 'UK Intelligence Did Not Expect Afghan Capital to Fall This Year – Raab', Reuters, 1 September 2021, https://www.reuters.com/world/uk/uk-foreign-minister-says-intelligence-was-afghan-capital-would-not-fall-this-2021-09-01/; and Vivian Salama and Warren P. Strobel, 'Four U.S. Intelligence Agencies Produced Extensive Reports on Afghanistan, but All Failed to Predict Kabul's Rapid Collapse', *Wall Street Journal*, 28 October 2021.

63 See Barnes and Cooper, 'U.S. Battles Putin by Disclosing His Next Possible Moves'.

64 See *ibid*.; Ellen Nakashima et al., 'U.S. Intelligence Shows Russia's Military Pullback Was a Ruse, Officials Say', *Washington Post*, 17 February 2022; and Schwartz and Sevastopulo, '"A Real Stroke of Genius"'.

65 Nakashima et al., 'US Intelligence Shows Russia's Military Pullback Was a Ruse, Officials Say'.

66 See Hans Von Der Burchard and 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/; and 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.

67 See Jenny Hill, 'Olaf Scholz: Ukraine Crisis a Challenge for German Leader', BBC, 14 February 2022, https://www.bbc.com/news/world-europe-60344479; and 'Scholz's Dismissal of Alleged Genocide in Donbass "Unacceptable", Russia Says', Reuters, 19 February 2022, https://www.reuters.com/world/europe/scholzs-dismissal-alleged-genocide-donbass-unacceptable-russia-says-2022-02-19/.

68 See Rick Noack, Loveday Morris and Karla Adam, 'Can European Shuttle Diplomacy Avert War in Ukraine?', *Washington Post*, 12 February 2022.

69 See 'French Military Spy Chief Quits After Ukraine Failings, Sources Say', *Guardian*, 31 March 2022; Maïa De La Baume, 'France Spooked by Intelligence Failures', *Politico*, 6 April 2022, https://www.politico.eu/article/france-military-intelligence-failure-russia-invasion-ukraine/; and Corera,

'Ukraine: Inside the Spies' Attempts to Stop the War'.

70 See Carnegie and Carson, *Secrets in Global Governance*.

71 See Dina Temple-Raston, 'Big Data Firm Says It Can Link Snowden Data to Changed Terrorist Behavior', NPR, 1 August 2014, https://www.npr.org/sections/thetwo-way/2014/08/01/336958020/big-data-firm-says-it-can-link-snowden-data-to-changed-terrorist-behavior?t=1655222739094; and Robin Simcox, 'Surveillance After Snowden: Effective Espionage in an Age of Transparency', Henry Jackson Society, June 2015, https://henryjacksonsociety.org/wp-content/uploads/2015/06/Surveillance-After-Snowden-16.6.15.pdf.

72 See Carnegie and Carson, *Secrets in Global Governance*, pp. 8–9.

73 See Aimen Dean, Paul Cruickshank and Tim Lister, *Nine Lives: My Time as MI6's Top Spy Inside Al-Qaeda* (London: Oneworld Publications, 2018).

74 See Andrew, *The Defence of the Realm*, pp. 154–6; and John Ferris, 'Issues in British and American Signals Intelligence, 1919–1932', NSA Center for Cryptological History, Special Series, vol. 11, 2016, pp. 31–2.

75 See Jason Dymydiuk, 'RUBICON and Revelation: The Curious Robustness of the "Secret" CIA–BND Operation with Crypto AG', *Intelligence and National Security*, vol. 35, no. 5, 2020, pp. 641–58.

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

77 See Thomas J. Maguire, *The Intelligence–Propaganda Nexus: British and American Covert Action in Cold War Southeast Asia* (Oxford: Oxford University Press, forthcoming in 2023).

78 'The US Is Engaging in a Strategy to Share Intelligence on Russia More Broadly'.

79 See, for example, 'Russia Bans Smartphones for Soldiers over Social Media Fears', BBC News, 20 February 2019.

80 See Maguire, *The Intelligence–Propaganda Nexus*.

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

82 See Jon Ungoed-Thomas, 'West Hits Vladimir Putin's Fake News Factories with Wave of Sanctions', *Observer*, 20 March 2022.

83 See Moustafa Ayad, 'The Vladimirror Network: Pro-Putin Power-users on Facebook', Institute for Strategic Dialogue, 4 April 2022, https://www.isdglobal.org/isd-publications/the-vladimirror-network-pro-putin-power-users-on-facebook/; and Brandy Zadrozny, 'Russian Propaganda Efforts Aided by Pro-Kremlin Content Creators, Research Finds', NBC News, 8 June 2022, https://www.

nbcnews.com/tech/tech-news/russian-propaganda-efforts-aided-kremlin-content-creators-research-fin-rcna32343.

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

85 Corera, 'Ukraine: Inside the Spies' Attempts to Stop the War'.

86 See Edward Malnick, 'Crack UK Team Tackling Kremlin's "Fake News"', *Sunday Telegraph*, 20 March 2022, p. 9; and Annabelle Dickson, 'Britain's (Opaque) War on Russian Propaganda', *Politico*, 4 April 2022, https://www.politico.eu/article/the-uk-counter-disinformation-russia-kremlin-cdu-media/.

87 Intelligence and Security Committee of Parliament, 'Russia', HC 632, 21 July 2020, https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.

88 UK GCHQ, 'Director GCHQ's Speech on Global Security Amid War in Ukraine', 31 March 2022, https://www.gchq.gov.uk/speech/director-gchq-global-security-amid-russia-invasion-of-ukraine.

89 See Edward Malnick, 'Inside the Secret Government Unit Returning Fire on Vladimir Putin's "Weaponised Lies"', *Telegraph*, 19 March 2022, https://www.telegraph.co.uk/news/2022/03/19/inside-secret-government-unit-returning-fire-vladimir-putins/; and Simon Baugh, 'Responding to Russia's Invasion', 24 March 2022, https://gcs.civilservice.gov.uk/news/responding-to-russias-invasion/.

90 See Lexington, 'Bill Burns and the Bear', *The Economist*, 9 April 2022; Corera, 'Ukraine: Inside the Spies' Attempts to Stop the War'; and Schwartz and Sevastopulo, '"A Real Stroke of Genius"'.

91 Michael Weiss, 'A CIA Cold Warrior on the Intelligence War Over Ukraine', *New Lines Magazine*, 22 February 2022, https://newlinesmag.com/reportage/a-cia-cold-warrior-on-the-intelligence-war-over-ukraine/.

92 See Barnes and Cooper, 'U.S. Battles Putin by Disclosing His Next Possible Moves'; and Lexington, 'Bill Burns and the Bear'.

93 See Chris Megerian, 'Looking for Evidence? Trust Us, Biden Administration Says', AP News, 5 February 2022, https://apnews.com/article/coronavirus-pandemic-russia-ukraine-health-europe-national-security-5c4182d83dd8b7585ac49fdbb5f91c45.

94 See Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton University Press, 2018); Joseph and Poznansky, 'Media Technology, Covert Action, and the Politics of Exposure'; and James D. Fearon, 'Domestic Political Audiences and the Escalation of International Disputes', *American Political Science Review*, vol. 88, no. 3, 1994, pp. 577–92.

95 American intelligence-sharing with Ukraine has not been fully reciprocated, owing to Kyiv's concerns that providing detailed information about its operational plans or battlefield performance might reveal weaknesses to its partners that could slow security assistance, or benefit Moscow if leaked. See Julian E. Barnes, 'U.S. Lacks a Clear Picture of Ukraine's

War Strategy, Officials Say', *New York Times*, 8 June 2022.

96 See Thomas L. Friedman, 'The War Is Getting More Dangerous for America, and Biden Knows It', *New York Times*, 6 May 2022.

97 Carson, *Secret Wars*.

98 Friedman, 'The War Is Getting More Dangerous for America, and Biden Knows It'.

99 'Escalate to de-escalate' is widely discussed. See, for instance, Olga Oliker and Andrey Baklitskiy, 'The Nuclear Posture Review and Russian "De-Escalation": A Dangerous Solution to a Nonexistent Problem', *War on the Rocks*, 20 February 2018, https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solution-nonexistent-problem/; and Joshua Ball, 'Escalate to De-escalate: Russia's Nuclear Deterrence Strategy', *Global Security Review*, 7 March 2022, https://globalsecurityreview.com/nuclear-de-escalation-russias-deterrence-strategy/.

100 See 'Stuxnet Part of Obama's Broader Cyberattack Plan, Book Alleges', CBC News, 5 June 2012, https://www.cbc.ca/news/science/stuxnet-part-of-obama-s-broader-cyberattack-plan-book-alleges-1.1173143.

101 The crisis is discussed in Richard A. Mobley, 'Gauging the Iraqi Threat to Kuwait in the 1960s', *Studies in Intelligence*, vol. 45, no. 5, Fall–Winter 2001, https://apps.dtic.mil/sti/pdfs/ADA529668.pdf.

102 See, for example, Kyle Farrell, '"Remember Iraq!" Russian Ambassador Mocks UK in Brutal Weapons of Mass Destruction Jibe', *Express*, 20 February 2022, https://www.express.co.uk/news/world/1568905/russia-news-trevor-phillips-ukraine-troops-sky-news-conflict-war-video-latest-vn.

103 See 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/.

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

105 These issues have been 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*, vol. 129, no. 4, Winter 2014, https://doi.org/10.1002/polq.12252.

106 Report of a Committee of Privy Counsellors, 'Review of Intelligence on Weapons of Mass Destruction', UK House of Commons 898, 2004, p. 87.

107 See Gordon Corera, 'New UK Centre Will Help Fight Information War', BBC News, 7 June 2022; and Ardi Janjeva, Alexander Harris and Joe Byrne, 'The Future of Open Source Intelligence for UK National Security', RUSI Occasional Paper, 7 June 2022, https://rusi.org/explore-our-research/publications/occasional-papers/future-open-source-intelligence-uk-national-security.

108 Schwartz and Sevastopulo, '"A Real Stroke of Genius"'.

109 Michael V. Hayden Center for Intelligence, Policy, and International

Security, 'The Directors' View: Russia & Ukraine', webinar, March 2022, https://www.youtube.com/watch?v=8V-LQwXyayU.

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

111 Gavin Wilde and Justin Sherman, 'Targeting Ukraine Through Washington: Russian Election Interference, Ukraine, and the 2024 US Election', Atlantic Council, 14 March 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington/.

112 See Thomas J. Maguire, 'Counter-subversion in Early Cold War Britain: The Official Committee on Communism (Home), the Information Research Department and "State–Private Networks"', *Intelligence and National Security*, vol. 30, no. 5, 2015, pp. 637–66.