

Russia, Ukraine, and the Future Use of Strategic Intelligence

By Joshua C. Huminski

Before Russia's unprovoked February 2022 invasion of Ukraine, the United States and the United Kingdom undertook an aggressive public and private information campaign to attempt to achieve two concurrent objectives. The primary goal was to convince their allies of the threat of Russia's pending offensive (and to smooth the mobilization of support to Ukraine after the fact) and to a lesser degree a secondary goal was to attempt to deter Moscow from acting. Central to this campaign was the very visible and highly publicized use of intelligence. Indeed, as Dan Drezner wrote in the *Washington Post*, "The U.S. intelligence community sure has been chatty as of late about what it thinks Russia is doing."¹ The use of intelligence to support policy or diplomatic efforts and to achieve a strategic effect is, in and of itself, not novel. Intelligence is meant to inform policymakers and their decisions.

What was novel was the speed, frequency, and extent to which intelligence was disclosed to the broader public—intelligence which demonstrated significant human or digital penetrations into Russia's political and military hierarchies, and which was designed to achieve a specific effect. These disclosures also benefited from an unplanned development: the existence of an external third-party validator in the open-source intelligence community. This nascent and maturing field offered a means by which some information, though not all, could be validated in near real-time. Tactical-level activity verified by these communities helped to reinforce Washington's broader message that policymakers were advancing using sensitive intelligence capabilities.

This use of intelligence, the perceived success of the effort, and the utility of that information will likely lead to an increase in demands both by politicians and the public writ large. This raises new issues and reaffirms preexisting challenges that affect and influence the use of intelligence. In that sense, the Ukraine campaign reflects lessons from past successes while, more importantly, also reflecting the lessons from past failures and offering warnings of risks for the future. Many of these lessons are not new. The need to protect sources and methods; the risk that politicians will selectively use intelligence for political aims; the

Joshua Huminski is Director of the Mike Rogers Center for Intelligence and Global Affairs at the Center for the Study of the Presidency and Congress.

importance of tailoring messaging to competing and differing audiences; all of these are familiar themes encountered throughout the history of intelligence.

What is perhaps most novel about the use of intelligence in Ukraine, and likely going forward, is that this represents an effort by the United States to recapture the initiative in the information war, which it largely ceded to Russia by omission and commission. This effort brings with it additional policy challenges and new considerations.

Goals and Efficacy

It is important from the outset to establish the broad outlines of what the United States and the United Kingdom hoped to achieve with the use of intelligence and the audiences at whom it was directed—namely policymakers at home and amongst allies, the adversary (Russia), and the broader world.

At a strategic level, the West's efforts in the run-up to Russia's invasion of Ukraine had two primary goals. The first, and arguably most successful, was to convince skeptical policymakers in Western allies and even Ukraine of the imminent threat from Moscow. The selective and sustained release of information, often augmented by considerable open-source information (though perhaps not always by design or intention), sought to allay allies' doubts about the imminence of the threat. This contributed to the subsidiary goal of beginning the process of mobilizing a collective allied response after the invasion. In this aim, the effort was decidedly successful.

Throughout the winter of 2021 and the early months of 2022, the United States highlighted a steady drumbeat of indicators and warnings about Russian intentions and likely plans vis-à-vis Ukraine. In December 2021, an unnamed administration official warned, "The Russian plans call for a military offensive against Ukraine as soon as early 2022 with a scale of forces twice what we saw this past spring during Russia's snap exercise near Ukraine's borders." They added, "The plans

involve extensive movement of 100 battalion tactical groups with an estimated 175,000 personnel, along with armor, artillery and equipment."² This was a concerted effort to prepare the battlefields of public opinion and private policymaking with intelligence.

By disclosing sensitive intelligence—even at possible risk to sources and methods—the United States signaled to Russia that it knew its plans and intentions in advance, thereby possibly achieving a deterring effect. After laying its cards on the table about what the intelligence community knew, the Biden Administration communicated the likely consequences should Moscow choose to act on the plans. According to National Security Advisor Jake Sullivan, to try to deter Putin they "needed to send somebody to Moscow to sit with the Russians at a senior level and tell them: 'If you do this, these will be the consequences.'"³ President Biden, for his part, noted, "What I am doing is putting together what I believe to be, will be the most comprehensive and meaningful set of initiatives to make it very, very difficult for Mr. Putin to go ahead and do what people are worried he may do."⁴

How effective the efforts were in deterring Russia is an open question. It was effective in getting ahead of false flag operations—operations designed to appear as being carried out by another actor—and disclosing what provocations Moscow planned to initiate to serve as a *casus belli* for its military activity. It does appear that America's warnings of imminent provocations⁵ may have prevented Russia from acting on those plans.⁶ Carrying out such an attack after the fact would have been undercut by the advance warning. This does assume that Russia needed the provocation in the first place and/or that the West was the primary audience of the said provocative act.

The U.S. intelligence revelations did not change Putin's plans to expand his invasion of Ukraine. They did, however, change the information environment in which his war took place. By disclosing the intelligence before the invasion, the West

undermined Russia's ostensible *casus belli*, removed potential provocations as justifications for invasion, and forced the Kremlin to concoct ever-evolving narratives for both foreign and domestic audiences, the development of which took time and energy, and which ultimately achieved little for Russia, in the West's estimation.

While the ultimate efficacy of the overall intelligence effort is subject to debate—especially as it is difficult to prove a negative or a counterfactual outcome—certain trends could, arguably, be divined. America's effort to convince its allies that the threat from Russia was imminent appears to have at the very least laid the foundation for a swifter response to Moscow's aggression than may have otherwise been possible. It is clear from reporting from the *Washington Post* and others that the effort was far from smooth. At times the United States struggled to convince its allies (beyond the United Kingdom and the Baltic States), and even Ukraine,⁷ of the seriousness of the threat. This is perhaps unsurprising, given the differing assessments of the threat posed by Russia. Doubts about U.S. intelligence among allies also reflected comparable weaknesses in terms of their intelligence services' access and penetration of Russian security services.

Indeed, America's performance in the run-up to the Ukraine War was, in many ways, a contrast to the flawed use of intelligence prior to the invasion of Iraq in 2003. America's intelligence community is seen as having been unduly influenced by the zeal of some members of the Bush Administration to invade Iraq, who selectively used intelligence to make their case for invasion. The failure to find weapons of mass destruction in Iraq and the subsequent chaos that resulted in the wake of the removal of Saddam Hussein were seen as a stain on the credibility of American intelligence. In the case of Ukraine, Germany⁸ and France,⁹ in particular, were thus skeptical of American claims about Russian intentions, especially after

Washington declined to share all of the intelligence available regarding Moscow's aims.

In reality it would have been naïve to expect that the selective disclosure of American and allied intelligence would ultimately dissuade Russia from acting. It is unlikely that any amount of dissuasion—publicly or privately—could have halted Russia's movement to war. At best it perhaps stalled or interrupted elements of the Kremlin's plans, but it would be too much to expect that it would halt a looming invasion. If there were such expectations that selective intelligence revelations would deter war, they likely resulted from assuming too much about the West's ability, and too little about President Putin's intentions. Arguably, there was little that the United States or the West writ large could have done to dissuade Moscow from acting, short of outright capitulation by Kyiv.

As for the wider world, the effort to use intelligence to control the narrative of the Ukraine War proved markedly less successful, and remains a challenge to this day. While it is arguable whether there was high value in convincing the Global South of the imminence of the threat or the need to respond to Russia's invasion of Ukraine, messaging to China and India is of critical importance. Given the relatively strong relationships of both Delhi and Beijing with Moscow, their voices on the international stage matter—particularly as calls for a resolution to the crisis are now growing.

Intelligence in Policy and Diplomacy

The use of intelligence to inform policy in a messaging manner is not a novel development. The United States, and indeed all powers, have sought to use intelligence at every level of political and military conflict to dissuade adversaries, convince allies, or communicate with the public more broadly. Even the use of sensitive intelligence—obtained via exquisite means or through high-level sources—to support policy aims is itself not a novel development.

The United States declassified photos obtained by the U-2 aircraft during the Cuban Missile Crisis,¹⁰ for instance, and used these photos in Adlai Stevenson's speech before the United Nations. The United States and the United Kingdom also undertook extensive efforts to sanitize and release information through unofficial means during the Cold War—e.g., selectively providing intelligence to friendly outlets, think tanks, and unwitting activist groups. In the wake of the 1986 bombing of the La Belle discothèque in West Berlin, Washington used declassified signals intelligence intercepts to prove the case that Muammar al-Qaddafi's Libya was responsible.¹¹ More recently, and perhaps most controversially, the United States used human intelligence of dubious value in the run-up to the 2003 invasion of Iraq over Baghdad's weapons of mass destruction (WMD) program.¹²

Indeed, in the aftermath of the failed intelligence related to Iraq's WMD program, several reviews were undertaken to evaluate what went wrong, and how, and to make recommendations for the future. There is a careful balance to be struck between providing intelligence for assessment and the use of that intelligence in policymaking. It is often the case that the latter omits the caveats of the former, caveats that are vitally important to accurately portray the information in question. In the United Kingdom, the "Review of Intelligence on Weapons of Mass Destruction," also known as the Butler Report, found that:

*If intelligence is to be used more widely by governments in public debate in the future, those doing so must be careful to explain its uses and limitations. It will be essential, too, that clearer and more effective dividing lines between assessment and advocacy are established when doing so.*¹³

The Iraq Inquiry report, also known as the Chilcot Report, echoed this conclusion, finding that, "The statements prepared for, and used by, the

UK Government in public from late 2001 onwards conveyed more certainty than the [Joint Intelligence Committee] Assessments about Iraq's proscribed activities and the potential threat they posed."¹⁴ In many ways, as discussed below, the use of intelligence in Ukraine reflected these lessons.

Risks to Sources and Methods

Perhaps the most significant issue resulting from the West's use of intelligence in this most recent crisis is the tension between protecting sources and methods and the utility of collected intelligence. This is not a new challenge. There is a fine balance between the intelligence officer's mission of ensuring the protection of their agent, or the cyber intelligence protection of a unique exploit or vulnerability, and the need to inform policymakers, who then seek to shape the political and diplomatic environment. Whenever intelligence is sanitized and released, there is the risk of heightening adversary awareness of capabilities and the resulting loss of that asset or exploit.

There are, and always will be, concerns about risks to sources and methods—it is the cardinal rule of intelligence collection: protecting agents and capabilities. Yet, in the words of one former senior intelligence officer,¹⁵ it can be followed to a fault. There is a risk that the zeal to protect sources and methods could restrict their attendant utility. Too much protection reduces their utility, too much use risks their exposure and loss. This can be avoided by the judicious and select release of information, but it remains a delicate balance between protection and usefulness.

Certainly, in the run-up to Ukraine, it appeared that the Biden Administration was willing to err on the side of utility over protection. The administration's disclosures about Russia's capabilities and intentions were impressive for their specificity. For example:

- "Intercepted communications obtained by the U.S. have revealed that some Russian officials have worried that a large-scale invasion of

Ukraine would be costlier and more difficult than Russian President Vladimir Putin and other Kremlin leaders realize, according to four people familiar with the intelligence.”¹⁶

- Speaking to the *New York Times*, a U.S. official noted that “the United States has acquired intelligence about a Russian plan to fabricate a pretext for an invasion of Ukraine using a faked video that would build on recent disinformation campaigns.”¹⁷
- “The U.S. intelligence community had penetrated multiple points of Russia’s political leadership, spying apparatus and military, from senior levels to the front lines, according to U.S. officials.”¹⁸

This intelligence could only have been acquired through high-level penetrations or compromised Russian communications networks. The very release of this information, sanitized as it was, could jeopardize the access of the agent in question or the vulnerability or exploit leveraged.¹⁹ While there is an argument to be made that Russia and others likely assume to some degree that they are subject to near-constant surveillance—attempted or successful—the specificity of the warning (if Moscow was paying attention) would likely have been disquieting. It is undoubtedly the case that Moscow has launched or will launch a robust counterintelligence effort to identify the source of the information used by the United States. If successful, that exploit or agent may be “burned” in intelligence parlance and no longer useful.

It is possible, though far less plausible, that the intelligence community wished to create the impression that it had insights into Russia’s decision-making process when, in fact, it did not, to sow doubt and confusion. While generating such intelligence is possible, doing so would have almost certainly been exposed by the Russians or allies and would have certainly eroded the credibility of the community at a time when that credibility was vital amongst allies.



U.S. Secretary of State Colin Powell holds a vial of anthrax during his presentation to the United Nations Security Council on February 5, 2003. UN Photo/Mark Garten.

In the case of Ukraine, it was clear that the urgency of the threat and the need to mobilize allied support trumped some, but not all, of the concerns about sources and methods. As reported by the *Washington Post*, and discussed above, the United States disclosed some intelligence related to what it knew about Russian intentions, but did not provide raw intelligence intercepts or reports to many of its

European allies. This caution is not surprising, as such information is restricted even amongst the Five Eyes.²⁰ While this was undoubtedly a prudent move, it fueled existing skepticism about the quality and veracity of American intelligence, and undoubtedly rekindled concerns from Berlin and Paris about the politicization of said intelligence (especially in light of their pre-existing skepticism of the threat from Russia and likely limited access of their own intelligence agencies to the Kremlin).

Open Source Validation

In the case of Russia's invasion of Ukraine, the United States and the United Kingdom did enjoy an advantage that did not exist to the current degree in previous crises: open-source intelligence. Throughout the run-up to Russia's expanded invasion of Ukraine, there was, and now remains, a robust body of open-source intelligence analysis.²¹ Derived through publicly available tools, commercial satellite imagery, and a dedicated cadre of social media sleuths, the open-source community served as an external validator or check for some of the claims made by the United States and the United Kingdom. Government claims about mobilization activities could, at least at a macro level, be verified against what commercial imagery revealed, and through collated analysis from groups like Bellingcat. Further validation of this information was found through social media channels like Telegram—troop movements could be tracked via the chattiness of Russian soldiers and the observations of the communities through which units moved. Perhaps most amusingly, the movements of Russian soldiers were tracked through their use of dating apps, according to reports.²²

Robust open-source intelligence served as a semi-transparent check on information released by governments. Bellingcat and others demonstrate their work, opening it up to public scrutiny in a way that the intelligence communities of the United States and the United Kingdom could not

and almost certainly would not. There are attendant risks, however, in relying on these well-meaning amateurs and semi-professional intelligence analysts. There is an uneven quality to the open source community—not every organization is Bellingcat, and there is not always wisdom in crowds. In theory, the free market nature of this community offers a check on the quality of the analysis. Outlets that are misleading, misguiding, or peddling inaccurate information will be outed and castigated if the system works as intended.

According to one former Central Intelligence Agency (CIA) operations officer, in the case of Ukraine, the United States had the most significant advantage in that truth was on its side, and this truth was validated by open-source analysis.²³ While open-source intelligence is certainly a novel development and reliant on technologies still in their relative infancy in many cases, there is a risk of self-fulfilling expectations. External checks such as Bellingcat and others were and are helpful in the present crisis, but only to a degree. In the future, these external checks will provide validation for the West's information in some cases, and in others it will contradict the information being offered by Western intelligence. In this sense the open-source community itself could well become part of the competitive information warfare terrain moving forward. While the West had the advantage of the truth, that will not necessarily always be the case. Counter-open source intelligence efforts could well emerge, either through direct state-sponsorship of institutions—an anti-Bellingcat of sorts—or penetration of existing organizations.

Moreover, while the open-source community has performed admirably in many cases, there are limits to what it can verify. The government will still retain exquisite means that will remain beyond the ability of open-source analysts to confirm or validate. Open-source intelligence will, in the future, be able to corroborate the presence of forces and the

movement of those forces, or even conduct small-scale intelligence investigations of their own—e.g., the identification of the GRU officers responsible for the Novichok poisoning in Salisbury, England.²⁴ It will not, however, be able to divine the intentions of those within the Kremlin (or in the future, perhaps within Zhongnanhai in Beijing). This will remain the unique selling point of the intelligence community.

There is also the question of what would happen if open-source intelligence contradicts official government sources of information. Russia's expanded invasion in February 2022 presented a perfect test-bed for when things go right, and when truth and interests aligned seamlessly. Such alignment will not always be the case. Governments will undoubtedly have information the open-source community will not be able to access. There will also be times when governments are interested in pursuing a policy and using intelligence selectively to support that policy, which may result in contradictions with the open-source community. Squaring this difference will be a challenge as it all feeds into the broader information ecosystem; e.g., a trusted open-source community disagrees with the government assessment, the media picks up on said disagreement, the media questions the government assessment, and so on.

The question of utility, then, inevitably follows. The open-source community has proven to be a particularly useful aid in the present crisis, but a useful aid only for the Western body politic. For Russia, China, India, and the Global South, the fact that Bellingcat and other open source outlets verified the West's intelligence matters far less, as does the intelligence itself.²⁵ In fact, on the global stage, open-source intelligence is likely competing in a much more contested information environment. There are already innumerable accusations that Bellingcat and others are merely arms of the CIA or Special Intelligence Service, allowing those predisposed to be skeptical of their claims to dismiss them as Western propaganda, no different than that which is

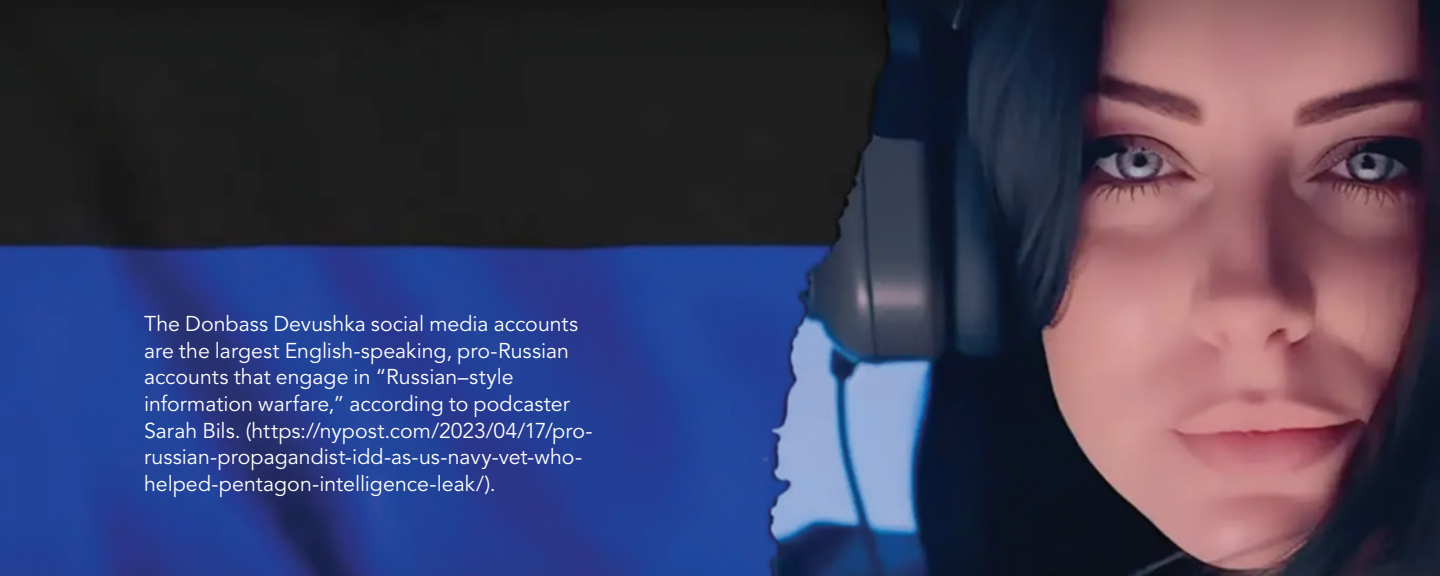
being produced by Moscow. Given the United States' and the United Kingdom's Cold War support for dissident movements, think tanks, and journalistic outlets, such claims are not without some historical grounding, however questionable they are today.

The Future of Intelligence as an Effect

There is a temptation to believe that the West's performance in the run-up to the Ukraine War will become the norm in the future—in other words, that the frequent disclosures of sanitized sensitive intelligence will become commonplace. While not wholly misguided, it's important to remember that the situation in Ukraine was unique. In the prelude to the largest war in Europe since the Second World War, Washington and its allies believed that all measures and steps were necessary. It was a crisis in which the United States was working to convince its allies of a clear and present danger and, to a lesser degree, to attempt to deter Russia from its course of action.

To expect the United States and its allies to attempt to communicate or signal through the use of strategic intelligence in a similar manner in every crisis would be misguided. Public dissemination of strategic intelligence can be a useful tool, but as University of Nottingham intelligence historian Rory Cormac noted, it is not a magic bullet. CIA Director William Burns also noted as much, saying, "I think we're going to have to be careful looking at other instances, whether it's in terms of cyber threats or other kinds of challenges that the United States and our allies will face in the future."²⁶

There is also a risk of confirmation bias in light of the Ukraine effort. The campaign to convince skeptical European allies was to a degree successful due in no small part to the accuracy of the information and the fact that the Biden Administration was and is seen as an honest broker or trusted source. Should the Intelligence Community get it wrong in the future, or should the intelligence be seen as used to support a



The Donbass Devushka social media accounts are the largest English-speaking, pro-Russian accounts that engage in “Russian-style information warfare,” according to podcaster Sarah Bils. (<https://nypost.com/2023/04/17/pro-russian-propagandist-idd-as-us-navy-vet-who-helped-pentagon-intelligence-leak/>).

DONBASS DEVUSHKA

political purpose, as was the case in 2002 and 2003 vis a vis Iraq, that goodwill will rapidly erode. Intelligence is not perfect—in the words of one former operations officer, it is never confirmed, it is only corroborated, building an incomplete picture and filling in the missing bits with analysis.

While public dissemination of intelligence may not become the “new normal,” it is also unlikely to be a one-off development. Its efficacy in this crisis may well presage a change in the attitude of the intelligence community. The pendulum may have swung away from the hoarding of intelligence and risk aversion. Instead, the United States and the West may subsequently use intelligence more often and more frequently in a public manner.

There is also a risk that policymakers and the public more broadly come to expect this to be the “new normal,” nonetheless. Representatives of the United Kingdom’s Ministry of Defence (MoD) noted that they had not expected their Twitter threads on the Ukraine conflict to become as popular or as widely sought after as they eventually became.²⁷ The MoD team quickly became a victim of its own success, with journalists, ministers, and the public alike clamoring for the latest releases. This forced the team to quickly staff up to

support the effort, one that was intended only to be a temporary activity (indeed, it continues as of this essay’s drafting to post content nearly every day). This creates a risky dynamic—not every crisis will be the equivalent of Ukraine and receive similar attention—and resolving that dynamic will require careful and astute policymaking.

Another risk is blending the public use of intelligence with public affairs activities. The former requires nuance and context, while the latter requires pith and often snark, which eliminates the care necessary in intelligence products. Striking the right balance between the two will present both a challenge and a risk. Managing the expectations of both the public and politicians will also be critical. Simply because there is a snarky Twitter thread on the crisis du jour does not mean that the issue is not serious or that the government lacks insight into what is happening.

Striking the right balance between intelligence used by policymakers for advocacy, versus intelligence provided by the community for assessment, will require continuous due diligence and attention. The Butler Report highlighted this tension in the government’s case to the British public concerning Iraq’s WMD program:

The Government wanted an unclassified document on which it could draw in its advocacy of its policy. The JIC sought to offer a dispassionate assessment of intelligence and other material on Iraqi nuclear, biological, chemical and ballistic missile programmes.... But this will have put a strain on them in seeking to maintain their normal standards of neutral and objective assessment.²⁸

Will the United States and the West find themselves in a similar crisis scenario necessitating a similar campaign to publicly reveal strategic intelligence in the future? Almost certainly. In the run-up to a potential Chinese invasion of Taiwan, the United States would almost certainly selectively disclose intelligence to allies in the region, and to the public more broadly. Such a disclosure could follow a similar pattern to the run-up to Ukraine—an aggressive campaign of private communication with regional allies and Beijing, backed by sanitized high-level intelligence to convince policymakers of the imminence of the threat (and the West’s awareness thereof), supported by a public campaign of signaling and communication. Once again, the goal would not primarily be deterrence alone. It is unlikely in that instance that Beijing could be deterred from its decided course of action. Rather, such disclosures would seek to convince regional and Western allies of the threat in a bid to mobilize their support.

The Politics of Intelligence as an Effect

The Biden Administration’s conduct in the run-up to the expanded invasion of Ukraine was an example of the professional and measured use of sensitive intelligence to achieve the desired effect. The administration, to its credit, is fairly *au fait* with the practice, consumption, and use of intelligence, and its associated sensitivities.

In the future, this may not always be the case. It is possible that future administrations will not

be as well-versed and knowledgeable about the use of intelligence and the process by which it is produced, or as circumspect in its use. Increased tensions between the intelligence community and elected officials and political appointees are not beyond the realm of possibility. Recent history has demonstrated significant tensions between the White House and the more apolitical intelligence community.²⁹ It is incumbent upon the analysts and officers to inform policymakers of the limitations of intelligence. This was a key finding of the Senate Select Committee on Intelligence’s “Report on the U.S. Intelligence Community’s Prewar Intelligence Assessments on Iraq.” The committee found that “The Intelligence Community did not accurately or adequately explain to policymakers the uncertainties behind the judgments in the 2002 National Intelligence Estimate.”³⁰ Whether or not policy makers read the National Intelligence Estimate is another matter.

The success—perceived or real—of the United States’ and United Kingdom’s intelligence efforts in Ukraine may well have set expectations of both availability and utility far higher than results justify. This could create a cycle of increased pressure for more publicly usable intelligence in both crisis and non-crisis scenarios—pressures that the intelligence communities in Washington and London may feel compelled to meet. The metaphorical genie is out of the bottle as the public and politicians alike may well demand increased intelligence to support or justify state actions.

Indeed, by way of example, how does one turn off the social media taps from the United Kingdom’s Ministry of Defence “Intelligence Update”? Concerning internal bureaucratic politics, the success of this effort could well be seen as a way to advance bureaucratic interests and gain increased political exposure and potential resources. It could become the “shiny new object” within the government toolkit. That path could easily lead to

the increased politicization of intelligence, which is anathema to intelligence agencies.

The tension between policymakers and intelligence professionals is not new or unique—it is inherent to the push-pull of politics and intelligence. This is not a strategic challenge, but more of a tactical problem set. As found in the Butler Report:

*We also recognise that there is a real dilemma between giving the public an authoritative account of the intelligence picture and protecting the objectivity of the JIC from the pressures imposed by providing information for public debate. It is difficult to resolve these requirements. [emphasis added]*³¹

Successfully managing intelligence in the future will require additional considerations to reflect this new environment. This becomes increasingly relevant in the domain of information warfare. To this end, for example, one former senior Ministry of Defence representative suggested that the governments of the United States and the United Kingdom, respectively, should establish clear guidelines on the use of intelligence in the public space, particularly in an information warfare context.³² Once again, this is not a novel development, but rather a response to the evolution of both the pace of events and the broader information ecosystem.

The efficacy of the Biden Administration's efforts to convince allies of the threat from Russia was due in no small part to the discipline of the messaging effort. Both publicly and privately, tailored messages were delivered to specific audiences. In the case of Ukraine, this campaign would not have been nearly as successful had it been uncoordinated, the messaging unclear, and elements of the administration working at cross-purposes. Indeed, throughout the summer there appeared at times breaks in this messaging discipline. For instance, the disclosure in May of this year from

unidentified American officials that Washington helped Ukraine target and kill Russian generals³³ was quickly rolled back.³⁴

Leaks or selective disclosures outside of the central narrative, or even well-meaning private initiatives, could undermine the overall effort. This highlights the imperative of controlling the use of intelligence to avoid disclosures that are unintentionally escalatory or inflammatory—again, not a novel development, but one that has taken on new urgency given the speed at which information travels. President Volodymyr Zelenskyy, prior to the February invasion, was at times critical of the information narrative, urging the West not to create a panic.³⁵ While perhaps understandable, it does highlight the challenges of competing information narratives and the risks of unintended consequences.

In the main, there is the risk that intelligence is stretched beyond its intended meaning and is selectively used to support government policy. Avoiding this requires a set of savvy intelligence consumers who understand the limitations and capabilities of the product they receive. Equally, it requires a community of intelligence professionals able to push back when political considerations appear to be driving intelligence and analytical products toward a specific end.

Intelligence in Information Warfare

The United States' use of intelligence in the run-up to Russia's invasion of Ukraine is, arguably, part of an attempt by Washington to regain the information narrative against Moscow's disinformation campaign. Russia's use of the information space as a domain of warfare is well understood and stands in contrast with the United States' understanding of that space.

As has been well documented, Russia wields a firehose of disinformation, falsehoods, propaganda, and "what about-ism."³⁶ It saturates the information space with conflicting narratives seeking to

confuse, disrupt, and convince adversaries, allies, and domestic audiences alike.

By contrast, Cormac notes that there is a consistent Western modernist assumption that the truth will speak for itself.³⁷ Yet, the West's "truth" is but one narrative in an increasingly tumultuous information space in which adversaries constantly attempt to undermine the very concept of objective truth. The challenge for the United States and the United Kingdom is finding a way for the truth to cut through the noise, and for their intended signal to reach the targeted audience for maximum effect. Because disinformation has far more avenues to spread while trusted sources are fewer in number and prominence, the speed of disinformation is far outpacing the speed of truth.

Russia's 2014 annexation of Crimea via "little green men" and later involvement in Eastern Ukraine were conducted with sufficient obfuscation and subterfuge to muddle the West's response. While there was significant reporting on the ground that the forces were Russian or Russian-backed, political obfuscation and an unwillingness to act ceded the information battlefield to Moscow. The United States' aggressive campaign in the run-up to the expanded invasion in February 2022 should then be seen as a corrective to this failure, and a sign of a growing recognition of the importance of the information space and the need to better integrate intelligence into the toolkit of national power.

There is a balance to be struck between intelligence to inform policymakers and intelligence for the information war. While they can be mutually reinforcing, tensions between the two are likely to exist. The information warfare calculus will require careful calibration, particularly as it pertains to intelligence. This goes to the heart of the use of intelligence in an era of information warfare—what is the desired effect (or effects) and what is the best way of achieving them? What is gained and what is lost in sanitizing and disclosing intelligence? Will a

source or exploit be exposed and, if so, at what cost? Will it be a short-term tactical gain at the expense of a long-term strategic benefit?

Such a calculus will inform policymakers and intelligence professionals in deciding what kind of intelligence is best suited for their objectives. Questions will naturally follow as to whether the information is appropriate for disclosure given the risks to sources and methods—a risk calculus that likely has changed in the wake of Ukraine. Does the immediacy of the crisis imply that greater risks to sources and methods are warranted? Or does the risk to long-term access outweigh the need for tactical intelligence successes? The messenger matters as much as the message. Statements from the White House or Department of State carry weight with traditional outlets, but feeding information to nontraditional partners or mediums may be more effective with different audiences.

In this new era of information warfare, the complexity of maintaining messaging discipline while communicating to differing audiences—policymakers at home and amongst allies, the adversary (Russia), and the broader world—will only grow. Discrepancies or differences in narratives will be easily discovered—what is said to a Russian audience could easily be compared with what is told to a European ally or even the American electorate. Social media has made this challenge infinitely more difficult—a quick Google search or scraping of Twitter's API will allow easy analysis.

There is also the temptation to engage in straightforward deception through official channels, which carries great risk. Once again, this is not new. During the Second World War nearly every outlet available to the allies was fed similar information as part of Operation Fortitude to deceive Nazi Germany into believing the invasion was coming across the English Channel at a different point, and not to Normandy. Prior to D-Day, the Allies engaged in complex and multi-layered deception operations

to convince Berlin that an invasion was targeting Greece and Sardinia, not Sicily.

The Cold War is also replete with examples of selective leaks to friendly journalists and the feeding of supported think tanks with official but off-the-record information to ensure the production of content supportive of the government's narratives. While not outright propaganda, it certainly supported the government's aims of undermining the Soviet Union. Of course, there is a difference between an official disclosure of accurate information for a desired political outcome and outright propaganda. There are legal restrictions, such as the Smith-Mundt Act of 1948 and Executive Order 12333, that are meant to control the production of propaganda and are intended to prohibit information designed for foreign audiences from reaching the American public. Maintaining these prohibitions and boundaries is arguably as important now in the era of social media as at any point prior.

The success of the efforts by the United States and Great Britain to use sensitive intelligence to seize the narrative before the most recent invasion of Ukraine was founded on the accuracy of the information presented, often validated by external open-source information. This is a marked recovery from the crisis of trust that resulted from the botched intelligence surrounding Iraq's WMD program. It is not beyond the realm of possibility that, by omission or commission, a government could seek to advance narratives that are false or contain seeds of falsehood but carry the imprimatur of "intelligence."

The reputational damage caused if such falsehoods are subsequently revealed, however, would be significant. That the UK's Defence Intelligence Twitter account has been so successful is due in no small part to its accuracy and the fact that it carries the weight of the official Ministry of Defence seal. The information is factual, not speculative, and generally limited to the realm of that which is known or verifiable. Were Defence Intelligence to

push unverified speculation—as it was seen to be doing by highlighting news stories alongside its own analysis—or to attempt to embark on a deception campaign, that trust would rapidly erode.

This is not to say that the government should not engage in deceptive activities. Arguably in the future deception and obfuscation will become even more important on the information battlefield. Rather, it is the mechanisms and vehicles that carry that information, and the labels that it carries, that will require greater due diligence. The *Washington Post* will want to know that the information that carries the label of "intelligence" is as factual as possible, and not being spun to suit a specific administration's requirements or political narrative. Again, this is not a new challenge, but one that is likely to be exacerbated in this new information era.

Planning, Measurement, and Information Warfare

The future successful use of intelligence as part of an information warfare narrative requires prior planning and internal interrogation. In the run-up to Ukraine, intelligence was largely used in a crisis response manner. Russia's invasion was looming; the United States sought to rally its allies, convince Ukraine of the urgency of the threat, and dissuade Moscow from acting. As discussed above, this effort was only partially successful.

Reflecting on the campaign in Ukraine and considering future scenarios, there is an opportunity to better plan how intelligence will be used. The key question underpinning any information effort must focus on the desired effect—what are policymakers trying to achieve? What are the desired effects or blend of effects? With the benefit of hindsight regarding Ukraine, was it a realistic goal to try to deter Putin or coerce Russia into not invading? Was a more realistic goal to sow dissent or mistrust within Putin's inner circle by the selective release of information, or to convince him that there is a mole



Russian military convoy marches towards the contact lines – Sputnik (<https://npasyria.com/en/73303/>).

within the Kremlin? More broadly, was the goal to expose Russian propaganda to the world at large? Was the desired effect introducing an element of chaos and distraction within Kremlin's counsels? A more modest goal, and one that was arguably achieved, might have been to simply make the operational environment for the Kremlin far more difficult than it would have otherwise been.

Having decided on the desired effects, what information or intelligence is available to support

this effort or this narrative? What or who is the best medium for conveying this information? How can all elements of the government be leveraged to achieve the desired effect? Finally, how will the efficacy of the information operation be judged?

This raises critical questions as to the intended audience, and whether it is even possible to achieve the desired effect given their preconceptions. In the case of France and Germany, for instance, there was considerable skepticism about American

intelligence. This was the result of past failures of American policymakers in handling intelligence (e.g., Iraq), and built-in skepticism about the possibility of a major land war on the European continent. Skepticism may also have resulted from the limitations and failures of their own intelligence agencies to anticipate events. Parochial economic and political interests of residents in Paris and Berlin may also have played a role.

These questions are not fundamentally new. The United Kingdom's robust efforts in the Second World War and both Washington and London's campaigns throughout the Cold War were all informed by these very questions. What is new is the effort by the West to recapture the information narrative in an era characterized by chaotic social media, growing open-source intelligence, and disinformation that travels at the speed of light.

Conclusion

The United States' use of intelligence in the run-up to Russia's expanded invasion of Ukraine marked an evolution of statecraft. Washington learned from past failures and sought to recapture an information space that had largely been ceded to an aggressive Moscow.

The nature of the crisis—the first major state-on-state conflict in Europe since the Second World War—demanded a unique response. The United States thus sought to leverage intelligence in a manner to convince allies of the imminent threat and, to a lesser degree, dissuade Moscow from acting, while signaling that it had deep insights into the Kremlin's plans. More than anything else, the United States had the benefit of the truth on its side—Washington was seen as a trusted information broker by most, particularly in the face of a belligerent and perceived pathological liar in Russia. Furthermore, the truth of the intelligence was validated by a far more established third-party open-source community than in previous incidents.

In many ways, the lessons to be drawn from this crisis are not unique. Future decisions on the use of intelligence to support military and diplomatic efforts will depend on a familiar calculus: Will the disclosure of information put sources and methods at risk? Will the gain outweigh the loss? Who is the best medium for the message? Most important, what is the desired effect?

What is unique is a rapidly evolving information domain, one in which information flows far faster and decisions must be made quicker. While the audiences may remain the same—domestic, adversary, and international—their habits of information consumption will demand far greater savviness in information operations than in the past. Washington may have achieved a nominal success in seizing the narrative in the Ukraine conflict, but it also potentially unleashed greater demands for its intelligence products than it is willing to provide. Not every crisis will be of the scale or scope of interstate war, nor will every crisis benefit so clearly from some intelligence informed truth-telling.

The Ukraine conflict strongly suggests that the use of intelligence in modern information warfare needs deeper consideration and analysis. We have seen selective intelligence releases by policymakers designed to achieve a signaling effect, for instance—not the least of which is related to the possibility of the use of nuclear weapons.³⁸ The West has also used intelligence to signal to its ostensible partner, Ukraine, its displeasure over the assassination of Darya Dugina, the daughter of a Russian ultra-nationalist polemicist.³⁹

The Ukraine conflict may also prove somewhat unique. In a future crisis scenario, for instance, the attending pressures and rapid build-up toward an impending war may also work against an administration's efforts to similarly craft or control the narrative, a situation one could easily imagine in the scenario of a rapid Chinese invasion of Taiwan. The reality to always keep in mind in all modern warfare

is that the delta between the speed of disinformation and the speed of information will always favor the former over the latter.

The intelligence community will continue to be *sine par* in terms of exquisite collection and analysis. Suggestions that it will simply offload its intelligence collection requirements to the open-source community are spurious. It will undoubtedly increasingly leverage this community where appropriate (as well as increase its own in-house open-source capabilities), but as noted above, the OSINT community's abilities are and will remain limited and will not always be suitable for a policymaking agenda. As General Sir Jim Hockenfull, Commander of the United Kingdom's Strategic Command, recently said, the linkage of open-source and secret intelligence will prove invaluable in the future:

Whilst open source doesn't provide the lid of the jigsaw box, it gives an almost infinite number of jigsaw pieces. The challenge now is that you can make an almost infinite number of pictures as a consequence of the available pieces. It also introduces a challenge in terms of discretion around the information, and we must filter with a view to being able to refine. This is where the combination of open source intelligence and secret sources of intelligence becomes invaluable in being able to see whether we can define greater understanding as a consequence.⁴⁰

The Ukraine conflict also suggests that the lessons of America's post-Iraq intelligence reviews, as well as those conducted in the United Kingdom, are just as applicable and relevant today as when they were first drafted. There remains a fine balance between intelligence produced to inform policymakers and the use of intelligence to achieve desired effects. Maintaining this balance between assessment, analysis, and advocacy requires officials

who understand and respect the difference. The temptations to blur the distinctions by omission or commission are very real, and the consequences are potentially disastrous.

While there exist processes and protocols for the declassification of information and its dissemination within the government and to the public, these processes are not designed for the demands of information warfare. The ad hoc process undertaken by the Biden Administration in regards to Ukraine, while effective, needs a procedural framework and template for future administrations to follow. That will be especially true in crisis situations where the politicians in power are not as savvy in the use of classified information and the distinctions between different kinds of intelligence. Equally, future administrations must be prepared for the possibility that the intelligence community might get it wrong.

The Ukraine War has shown that competing in the modern information domain requires leveraging all tools of national power. Intelligence, hitherto used primarily to inform policymakers, will be an increasingly key asset in that arsenal when judiciously and appropriately used. The role of intelligence will become even more important as the West seeks to recapture the initiative in the information war.

America's intelligence community and the policymakers it supports demonstrated the potential utility of this information in the 2022 Ukraine conflict and the information war against Russia. Changes in modern warfare will necessitate adjustments in the way the intelligence community views intelligence—not just as a product to be provided to policymakers, but a ready-made tool to achieve strategic effects in a crisis scenario. Drawing the right lessons from its use in the Ukraine War—cognizant of that which has changed and that which has not—will ensure that Washington is better placed to wage the information wars of the future. **PRISM**

Notes

¹ Dan Drezner, “Why is the U.S. intelligence community so chatty about Russia?” *Washington Post*, February 8, 2022, available at <<https://www.washingtonpost.com/outlook/2022/02/08/why-is-us-intelligence-community-so-chatty-about-russia/>>.

² Shane Harris and Paul Sonne, “Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns,” *Washington Post*, December 3, 2021, available at <https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecd7a2ad_story.html>.

³ Shane Harris et al., “Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion,” *Washington Post*, August 16, 2021, available at <<https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/>>.

⁴ Harris and Sonne, December 3, 2021.

⁵ Amy Mackinnon, Jack Detsch, and Robbie Gramer, “Russia Planning Provocation in Ukraine as Pretext for War,” *Foreign Policy*, January 14, 2022, available at <<https://foreignpolicy.com/2022/01/14/russia-provocation-war-pretext-false-flag-ukraine-east-ern-us-intelligence>>.

⁶ Katherine Lawlor and Kateryna Stepanenko, “Warning Update: Russia May Conduct A Chemical or Radiological False-Flag Attack As a Pretext for Greater Aggression Against Ukraine,” Institute for the Study of War, March 9, 2022, available at <<https://www.understandingwar.org/backgrounder/warning-update-russia-may-conduct-chemical-or-radiological-false-flag-attack-pretext>>.

⁷ David Stern and Robyn Dixon, “Ukraine’s Zelensky’s message is don’t panic. That’s making the West antsy,” *Washington Post*, February 7, 2022, available at <<https://www.washingtonpost.com/world/2022/01/30/ukraine-zelensky-russia-biden/>>.

⁸ Holly Ellyatt, “Germany urged to ‘wake up’ over Ukraine-Russia crisis, before it’s too late,” *CNBC*, February 7, 2022, available at <<https://www.cnbccom/2022/02/07/germany-forced-to-defend-itself-over-ukraine-crisis.html>>.

⁹ Maia de la Baume, “France spooked by intelligence failures,” *Politico.EU*, April 6, 2022, available at <<https://www.politico.eu/article/france-military-intelligence-failure-ukraine-invasion-ukraine>>.

¹⁰ https://nsarchive2.gwu.edu/nsa/cuba_mis_cri/photos.htm.

¹¹ Norman Kempster, “Cables Cited as Proof of Libyan Terror Role: 2 Messages to Kadafi Headquarters Predicted, Confirmed W. Berlin Bombing, Reagan Says,” *Los Angeles Times*, April 15, 1985, available at <<https://www.latimes.com/archives/la-xpm-1986-04-15-mn-4815-story.html>>.

¹² Report on the U.S. Intelligence Community’s Prewar Intelligence Assessments on Iraq (Washington, D.C.: Select Committee on Intelligence, United States Senate, 2004), available at <https://irp.fas.org/congress/2004_rpt/ssci_concl.pdf>.

¹³ *Review of Intelligence on Weapons of Mass Destruction* (London, England: Report of a Committee of Privy Counsellors, July 2004), 87, available at <<https://irp.fas.org/world/uk/butler071404.pdf>>, The Butler Report.

¹⁴ *The Report of the Iraq Inquiry* (London, England: Report of a Committee of Privy Counsellors, July 2016), 115, available at <<https://webarchive.nationalarchives.gov.uk/ukgwa/20171123122743/http://www.iraqinquiry.org.uk/the-report/>>.

¹⁵ Interview with the author.

¹⁶ Natasha Bertrand, Jim Sciutto, and Katie Bo Lillis, “US intel indicates Russian officers have had doubts about full scale Ukraine invasion,” *CNN*, February 7, 2022, available at <<https://www.latimes.com/archives/la-xpm-1986-04-15-mn-4815-story.html>>.

¹⁷ Julian Barnes, “U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion,” *New York Times*, February 3, 2022, available at <<https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html>>.

¹⁸ Harris et al. August 16, 2022.

¹⁹ Central intelligence Agency. 2022. “Director Burns’ Remarks at the Billington CyberSecurity Summit,” September 8, 2022, <<https://www.cia.gov/stories/story/director-burns-remarks-at-the-billington-cybersecurity-summit/>>.

²⁰ The Five Eyes is an intelligence-sharing alliance consisting of Australia, Canada, New Zealand, the United Kingdom, and the United States.

²¹ Pranshu Verma, “The Rise of the Twitter Spies,” *Washington Post*, March 23, 2022, available at <<https://www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/>>.

²² Ian Birrell, “Ukraine’s online Mata Hari: Russian troops are being duped by woman, 18, using dating app to lure them into giving away their location in Ukraine by flirting with them,” *Daily Mail*, March 23, 2022, available at <<https://www.dailymail.co.uk/news/article-11289159/Invaders-duped-dating-app-teen-lures-Russian-soldiers-giving-away-location.html>>.

²³ Interview with the author.

²⁴ Bellingcat Investigation Team, 2018, “Skrripal Suspect Boshirov Identified as GRU Colonel Anatoliy Chepiga,” *Bellingcat*, September 26, 2018, <https://www.bellingcat.com/news/uk-and-europe/2018/09/26/skrripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga/>.

²⁵ Sarang Shidore, 2022, “Global South Again Shows Ambivalence on the Ukraine War,” *Responsible Statecraft*, October 13, 2022, <https://responsiblestatecraft.org/2022/10/13/global-south-again-shows-ambivalence-on-the-ukraine-war/>.

²⁶ Lauren Williams, 2022, “Sharing Secrets Has Been ‘Effective’ against Russia, but the Tactic Has Limits, CIA Chief Says,” *Defense One*, September 8, 2022, <https://www.defenseone.com/defense-systems/2022/09/sharing-secrets-has-been-effective-against-russia-tactic-has-limits-cia-chief-says/376882/>.

²⁷ Interview with the author.

²⁸ The Butler Report, 113.

²⁹ Karen DeYoung, “Tension between CIA and Trump White House persists over personnel and policy,” *Washington Post*, March 15, 2022, available at https://www.washingtonpost.com/world/national-security/tension-between-cia-and-trump-white-house-persists-over-personnel-and-policy/2017/03/15/0694bf76-09b5-11e7-b77c-0047d15a24e0_story.html.

³⁰ *Report on the U.S. Intelligence Community’s Prewar Intelligence Assessments on Iraq* (Washington, D.C., Select Committee on Intelligence, United States Senate, 2004), 16, available at https://irp.fas.org/congress/2004_rpt/ssci_concl.pdf.

³¹ The Butler Report, 114.

³² Interview with the author.

³³ Matt Seyler, “U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Say,” *New York Times*, May 4, 2022, available at <https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html>.

³⁴ Matt Seyler, “Officials push back on report US intel helping Ukraine target Russian generals,” *ABC News*, May 5, 2022, available at <https://abcnews.go.com/Politics/officials-push-back-report-us-intel-helping-ukraine/story?id=84518393>.

³⁵ Karen DeYoung, “Ukraine crisis: Don’t create panic, Zelensky tells West,” *BBC News*, January 28, 2022, available at <https://www.bbc.com/news/world-europe-60174684>.

³⁶ Christopher Paul and Miriam Matthews, *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND Corporation, 2016), available at <https://www.rand.org/pubs/perspectives/PE198.html>.

³⁷ Interview with the author.

³⁸ Helene Cooper, Julian E. Barnes, and Eric Schmitt, “Russian Military Leaders Discussed Use of Nuclear Weapons, U.S. Officials Say,” *The New York Times*, November 2, 2022, sec. U.S., <https://www.nytimes.com/2022/11/02/us/politics/russia-ukraine-nuclear-weapons.html>.

³⁹ Julian E. Barnes, Adam Goldman, Adam Entous, and Michael Schwirtz, “U.S. Believes Ukrainians Were behind an Assassination in Russia,” *The New York Times*, October 5, 2022, sec. U.S., <https://www.nytimes.com/2022/10/05/us/politics/ukraine-russia-dugina-assassination.html>.

⁴⁰ Ministry of Defence, “How Open-Source Intelligence Has Shaped the Russia-Ukraine War,” *GOV.UK*, December 9, 2022, <https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war>.