SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Public intelligence as a strategic tool: The role of real-time intelligence disclosure in the Ukraine War

Alfred Marleku

alfred.marleku@ubt-uni.net

https://orcid/org/0000-0003-0018-042X

Faculty of Political Science and Security Studies, University for Business and Technology, Kalabria 10000, Prishtina, Kosovo

Abstract

This paper aims to analyse the role of public intelligence as a strategic tool in modern conflicts, focusing on its use during the Russo-Ukrainian war. It employs a qualitative research design, combining comparative case analysis and document analysis to examine the role of public intelligence as a strategic tool in the Ukraine War. The primary data sources include declassified intelligence reports, official government statements, media coverage, and academic literature on intelligence disclosure and strategic communication. The findings of this study indicate that public intelligence disclosure in the Ukraine War has been highly effective in countering Russian disinformation and strengthening diplomatic cohesion among Western allies. Unlike previous conflicts, intelligence transparency played a crucial role in shaping global narratives and mobilising international support. However, its deterrence value remains uncertain, as intelligence disclosures did not prevent Russia's full-scale invasion. The findings of this paper highlight how intelligence dissemination has shifted from classified circles to a public tool of strategic statecraft. The Ukraine War marked a departure from traditional intelligence practices, as the United States and the United Kingdom used real-time declassification to counter Russian disinformation, unify allies, and shape global opinion. This shift underscores both opportunities and limitations, as intelligence transparency did not deter Russia's invasion. Public intelligence disclosures proved effective in neutralising misinformation and influencing diplomatic responses. Intelligence disclosure also had diplomatic ramifications. While it helped rally allies, initial scepticism from Germany and France revealed lingering distrust due to past intelligence failures.

Keywords:

foreign policy, Russia-Ukraine War, public intelligence, strategic disclosure, intelligence transparency

Article info
Received: 11 February 2025
Revised: 2 May 2025
Accepted: 26 May 2025
Available online: 30 June 2025

Citation: Marleku, A. (2025) 'Public intelligence as a strategic tool: The role of real-time intelligence disclosure in the Ukraine War', *Security and Defence Quarterly*, 50(2). doi: 10.35467/sdq/205566.

Introduction

The role of intelligence in shaping foreign policy has evolved significantly in the modern era, transitioning from a primarily covert function to a tool for public diplomacy and strategic influence. The Russian invasion of Ukraine in 2022 marked a pivotal moment in this transformation, as Western states—most notably the United States and the United Kingdom—adopted an unprecedented approach: declassifying and disseminating intelligence to the public in real-time. Unlike past conflicts where intelligence remained confined to policymakers and security communities, the Ukraine War demonstrated how intelligence disclosures could serve as a deterrence mechanism, counter-narrative and instrument of diplomatic pressure (Dylan and Maguire, 2022). Such strategic disclosure aligns with Rovner's (2015) analysis of intelligence politicisation, emphasising how intelligence dissemination is strategically managed to influence both policy outcomes and public perceptions. This practice, which some have labelled "public intelligence" (Dylan and Maguire, 2022; Huminski, 2023; Schwartz and Sevastopulo, 2022; Scott and Jackson, 2004; Zegart, 2022), has redefined the traditional boundaries of intelligence use, raising critical questions about its implications for international relations and security studies.

Intelligence is conventionally understood as the systematic collection, analysis, and dissemination of information to support national security objectives (Collins, 2019; Scott and Jackson, 2004). However, the Ukraine case presents a unique manifestation of public intelligence, defined as the deliberate release of declassified intelligence to influence public opinion, deter adversaries, and shape diplomatic discourse (Gustafson *et al.*, 2024; Schwartz and Sevastopulo, 2022; Shaaban Abdalla *et al.*, 2022). This approach departs from the traditional secrecy of intelligence operations. It aligns with the broader concept of strategic intelligence (Huminski, 2023), which involves using intelligence to shape long-term policy goals and international behaviour (Meijer and Brooks, 2021). Unlike past instances, such as the 2002–2003 Iraq War, where intelligence was selectively disclosed to justify military intervention (Zarefsky, 2007), the Ukraine War exemplifies a new paradigm wherein intelligence disclosures are used proactively to counter disinformation and pre-empt adversarial narratives (Schwartz and Sevastopulo, 2022).

Despite the growing recognition of public intelligence as a foreign policy tool, significant gaps remain in the academic literature. This paper strengthens the literature by integrating both historical and contemporary contributions, including overlooked aspects of democratic resilience and the role of societal actors in intelligence communication. While research has extensively examined intelligence failures (Kessler, 2019), disinformation tactics (Khaldarova and Pantti, 2019), and the role of intelligence in war (Sutherland, 2020), there is limited scholarly analysis on the real-time use of public intelligence in modern conflicts. Existing studies primarily focus on intelligence-sharing within alliances (Harris and Sonne, 2021) or its role in shaping diplomatic strategies (Carnegie and Carson, 2020). However, there is a need for a comprehensive assessment of how states strategically employ intelligence for public consumption and the extent to which this practice influences adversarial behaviour, allied cohesion, and global public opinion (Dylan and Maguire, 2022).

This study aims to address the above research gap by analysing the use of public intelligence as a strategic tool in the Ukraine War and evaluating its effectiveness in deterring aggression, countering disinformation, and shaping foreign policy discourse. It adopts a comparative interpretive approach by examining not only the Ukraine case but also the 2003 Iraq War and Israel's conflict with Hamas, highlighting variations in how public disclosure functions as a deterrence tool, an instrument of persuasion, anda narrative control

mechanism. This qualitative, theory-informed synthesis contributes conceptually by identifying the conditions under which public intelligence proves effective or counterproductive in shaping international responses. Through this analysis, the study offers a nuanced understanding of how intelligence disclosure strategies have evolved and the risks associated with their implementation. It assesses whether the Ukraine model represents a new norm in geopolitical conflict or remains an exception dictated by unique circumstances.

Declassified intelligence and strategic diplomacy

The intersection of intelligence and foreign policy has been historically characterised by secrecy, discretion, and highly classified decision-making processes. However, the Russo-Ukrainian war has highlighted a paradigm shift, with the United States and the United Kingdom leveraging public intelligence to shape narratives, counter misinformation, and apply diplomatic pressure. The existing research has demonstrated that intelligence disclosure can effectively counter disinformation and enhance strategic communication in modern conflicts. The declassification of intelligence before Russia invaded Ukraine serves as a unique example of intelligence being employed for real-time strategic communication, significantly influencing public discourse (Schwartz and Sevastopulo, 2022). Unlike conventional intelligence-sharing, which is restricted to policymakers, intelligence-led communication is disseminated through both traditional and social media platforms, shaping global public opinion and altering diplomatic alignments (Dylan and Maguire, 2022; Gustafson *et al.*, 2024; Huminski, 2023; Shaaban Abdalla *et al.,* 2022). This shift has expanded the function of intelligence beyond traditional military applications, positioning it as an instrument of public diplomacy (Pinkus, 2014).

Studies on intelligence dissemination reveal that the pre-emptive release of intelligence reports during the Ukraine conflict prevented Russian disinformation from taking hold as effectively as in previous conflicts. The study by the Royal United Services Institute (RUSI) on the "Ukraine model" of intelligence disclosure underscores the unprecedented nature of this approach and highlights that the model was effective in countering Russian disinformation, thereby altering diplomatic responses and foreign policy strategies significantly (Duffield, 2023). This aligns with the findings from intelligence analysts who have argued that misinformation can be neutralised when confronted with timely and transparent counterintelligence (Jonsson, 2024). Furthermore, research suggests that the effectiveness of intelligence disclosures is influenced by the adversary's ability to adapt to strategic transparency, as seen in the ongoing Russo-Ukrainian conflict, where intelligence disclosures disrupted Russian military strategies and limited their operational flexibility (Huminski, 2023). Additionally, intelligence warnings and their impact on the Ukraine War have been analysed, showing that while intelligence disclosures did not prevent the invasion, they successfully undermined Russian justifications and strengthened Western support for Ukraine (Holmgren, 2024).

The effectiveness of intelligence disclosure in diplomacy is also widely debated in academic literature. Scholars have noted that the use of declassified intelligence to pressure allies into aligning with strategic objectives was evident during the prelude to the Ukraine War, when the United States and the United Kingdom used intelligence briefings to shift European perspectives on the inevitability of war (Michaels, 2024; Von Der Burchard and Herszenhorn, 2022). By publicising intelligence assessments, the United States and the United Kingdom sought to compel reluctant allies to acknowledge the inevitability of a Russian invasion and take pre-emptive actions (Dettmer, 2022; Schwartz and Sevastopulo, 2022). The use of intelligence disclosure as a diplomatic tool was further highlighted in a study on intelligence operations in Germany, which examined how external experts had

warned about the invasion but struggled to shift political and strategic priorities in time (Michaels, 2024). Historical comparisons have been made with the Bush administration's approach in leveraging intelligence to justify the Iraq War: intelligence was selectively declassified to secure international support, leading to long-term scepticism of intelligence-sharing among European allies (Barnes, 2020; Collins, 2019). This demonstrates that while intelligence disclosure can be an effective tool for coalition-building, its credibility depends on the accuracy of the information and the historical trust between intelligence-sharing partners.

Despite its effectiveness in shaping international narratives, intelligence disclosure carries inherent risks. Studies on intelligence failures highlight that selective declassification can undermine long-term credibility, with the case of Iraq serving as a cautionary tale demonstrating how intelligence manipulation can erode trust in state institutions (Carnegie and Carson, 2020; Hedley, 2005; Jensen, 2012). This scepticism was further compounded by the inconsistencies in intelligence assessments regarding Russian troop movements, which some European policymakers initially dismissed as exaggerated (De La Baume, 2022). Furthermore, research on Swedish intelligence has shown that intelligence failures are often a product of deeply ingrained institutional assumptions, as seen in Sweden's misjudgement of Russia's military intentions before the invasion (Jonsson, 2024). Researchers have also raised concern regarding the possibility of intelligence disclosure strategies having unintended diplomatic consequences, as states with different national security cultures may be reluctant to engage in public intelligence-sharing (Phythian, 2013; Buluc, Radu and Bogzeanu, 2025), as seen in the German and French responses to the Ukraine issue (Michaels, 2024). Intelligence disclosures also run the risk of providing adversaries with operational insights, making the "Ukraine model" a case-specific strategy that may not be applicable to all conflicts (Duffield, 2023). Additionally, studies have suggested that the long-term impact of intelligence disclosure on trust between intelligence agencies and policymakers remains unclear, as the repeated use of intelligence for public persuasion may diminish its strategic value over time (Shaaban Abdalla *et al.*, 2022).

The use of public intelligence in the Ukraine War has significant implications for intelligence studies and international relations theory. Some scholars argue that it marks the emergence of a "new paradigm" in intelligence operations, where real-time intelligence-sharing becomes a core element of strategic statecraft (Schwartz and Sevastopulo, 2022). Others caution that this model remains an exception, rather than the rule, emphasising the importance of contextual and geopolitical factors in determining the viability of intelligence disclosure strategies (Maguire, 2015). The challenges of applying this model beyond the Ukrainian context are evident in the case of Israel's war against Hamas, where intelligence disclosure was significantly less frequent, illustrating that public intelligence-sharing is not universally effective in all conflicts (Duffield, 2023).

As technological advancements continue to shape the information landscape, the role of intelligence in international conflicts will likely evolve, with open-source intelligence (OSINT) and Artificial Intelligence (AI)-driven analysis becoming increasingly central to intelligence operations (Janssen, 2012). Moreover, advances in data analytics and machine learning are facilitating the ability of intelligence agencies to process and disseminate information more rapidly, potentially increasing the effectiveness of intelligence-led strategic communication. However, the ethical and legal dimensions of these practices remain contested, particularly concerning data privacy and the manipulation of intelligence for political objectives (Shaaban Abdalla *et al.*, 2022). These issues highlight the need for continuous examination of how intelligence disclosure interacts with broader security and diplomatic frameworks.

The Russo-Ukrainian war underscores the growing role of intelligence as a public-facing tool of statecraft. The strategic declassification of intelligence by the United States and the United Kingdom not only countered Russian disinformation but also influenced diplomatic responses and shaped international perceptions of the conflict. While intelligence disclosure has proven effective in this context, its broader applicability remains controversial. Future research should explore the long-term implications of this approach, particularly in conflicts where intelligence manipulation is more ambiguous. Additionally, scholars should examine whether intelligence disclosure can be sustained without diminishing its strategic efficacy. Ultimately, the case of Ukraine signals a shift in the intelligence landscape, one that necessitates a re-evaluation of traditional intelligence paradigms within international relations, emphasising the need for transparency, credibility, and adaptability in modern intelligence practices.

Intelligence warnings and strategic disclosures

The initial indications of Russian troop activities, first detected through military exercises, were closely monitored by Western intelligence services throughout 2021 (Brown, 2022; Corera, 2022; Harris and Sonne, 2021). By late 2021, intelligence analysts observed a sustained Russian military build-up along Ukraine's borders, prompting heightened concerns among European nations and the United States. The scale and strategic nature of this deployment suggested a level of preparation that far exceeded standard military exercises, leading analysts to warn of potential offensive operations (Duffield, 2023). In April 2022, Russia announced a withdrawal of its forces, yet intelligence assessments revealed that the troop presence remained substantial, reinforcing suspicions of an impending invasion (Jonsson, 2024). Secretary of State Antony Blinken, speaking at NATO headquarters, emphasised the gravity of the situation: "We are witnessing the most substantial concentration of Russian forces along Ukraine's borders since 2014" (Harris and Sonne, 2021). Media reports corroborated this analysis, indicating that the number of Russian troops amassed at that time exceeded the forces involved in the annexation of Crimea in 2014 (Holmgren, 2024; Winter-Levy, 2024).

The first formal intelligence disclosures from the United States emerged in December 2021, warning of an imminent Russian military offensive against Ukraine, expected in early 2022. *The Washington Post* was among the first media outlets to publish intelligence-based findings, releasing documents that included satellite imagery displaying the positioning and scale of Russian troop deployments (Harris and Sonne, 2021). Intelligence sources estimated that Russia had positioned approximately 175,000 troops along the Ukrainian border, signalling a large-scale invasion plan (Jonsson, 2024). By late January 2022, British intelligence concluded that Moscow intended to orchestrate a regime change in Kyiv and install a pro-Russian government. British Prime Minister Boris Johnson, addressing Parliament, cited declassified intelligence that revealed Russian plans involving cyberattacks, false flag operations, and the spread of disinformation to justify military intervention (Duffield, 2023; Murauskaite, 2024). Simultaneously, the US intelligence uncovered evidence of Russian efforts to dispatch saboteurs to eastern Ukraine to fabricate incidents that could serve as a pretext for war (Duffield, 2023).

In early January 2022, the US officials obtained further intelligence indicating that Russia was preparing staged attacks, reinforcing concerns that Moscow sought to manufacture a *casus belli* for its invasion (Nakashima *et al.*, 2022). By early February 2022, White House National Security Adviser Jake Sullivan confirmed that Russia had amassed sufficient forces to conduct a full-scale invasion, including the capability to seize Kyiv. Given

the reliability of these assessments, Sullivan urged all US citizens to leave Ukraine within 48 hours, highlighting the urgency of the intelligence findings (Holmgren, 2024).

The strategic use of intelligence disclosure did not cease with the onset of the war; rather, it evolved into a sustained practice of real-time intelligence-sharing by the United States and the United Kingdom. These disclosures were systematically used to counter Russian disinformation, influence public opinion, and reinforce international diplomatic cohesion (Duffield, 2023). The war in Ukraine marked the first instance of Western intelligence services engaging in daily public releases of declassified intelligence, which detailed battlefield developments, military deployments, and Russian operational strategies (Jonsson, 2024). This practice, often referred to as "Twitter intelligence" (Nee, 2025), represents an unprecedented shift in the intelligence landscape, where real-time intelligence updates were disseminated through digital platforms to reach domestic and global audiences. Traditionally, intelligence is a closely guarded asset, shared only with allied states under strict security protocols. However, in the context of the Ukraine War, the deliberate and systematic declassification of intelligence reshaped strategic communication, allowing allied nations and the international public to access real-time operational data (Holmgren, 2024).

For instance, Richard Moore, Director of the British Intelligence Agency MI6, actively engaged in public intelligence disclosure, using his Twitter account to share updates from the UK Ministry of Defence. In one instance, he noted that "Russia is running out of steam," signalling a shift in the war's trajectory (Moore, 2022a). Similarly, William Burns, Director of the US Central Intelligence Agency (CIA), publicly disclosed assessments regarding Russian military casualties, reinforcing Western narratives of Russian strategic miscalculations (Stewart, 2022). This public-facing intelligence strategy not only countered Russian state propaganda but also played a crucial role in shaping international diplomatic responses and maintaining allied unity (Duffield, 2023). While this approach has been largely effective in the context of Ukraine, analysts caution that its applicability in future conflicts remains uncertain. The long-term implications of sustained intelligence disclosure, particularly its impact on trust between intelligence agencies and policymakers, continue to be debated in intelligence and security studies (Gustafson *et al.*, 2024; Shaaban Abdalla *et al.*, 2022).

Public intelligence as deterrence, pressure, and counter-narrative

The use of public intelligence in the Ukraine–Russia conflict was driven by three primary strategic objectives: deterrence, diplomatic pressure, and countering disinformation. According to Riemer (2022), intelligence disclosure functions performatively to reinforce diplomatic narratives and strategically influence international agendas, demonstrating its critical role in modern geopolitical strategies. It marks a departure from traditional intelligence operations, shifting towards a proactive and public-facing strategy designed to shape global narratives and influence international decision-making (Duffield, 2023). The disclosure of intelligence by the United States and the United Kingdom exemplifies a broader shift in intelligence doctrine, leveraging transparency as a tool for strategic influence, rather than relying solely on covert intelligence operations (Holmgren, 2024; Huminski, 2023). The conflict in Ukraine underscores the role of intelligence not just as a tool for decision-makers but also as an instrument of diplomacy, public engagement, and information warfare (Jonsson, 2024).

One of the key rationales behind the intelligence disclosure was to deter Russian aggression by exposing military preparations, thereby increasing the political and strategic costs

of the invasion. The premise was that by revealing Russia's troop movements, military build-ups, and planned false flag operations, the West could instil doubt within Russian leadership and deter the Kremlin from proceeding with its plans (Riemer, 2022; Shaaban Abdalla *et al.*, 2022). In February 2022, just days before the invasion, US President Joe Biden publicly stated that intelligence disclosures were intended to undermine Russia's justifications for war and remove plausible deniability (Holmgren, 2024). British intelligence chief Richard Moore echoed this sentiment, emphasising that the exposure of Russian military planning demonstrated the premeditated nature of the aggression, countering Moscow's disinformation narratives (Moore, 2022b). Intelligence disclosures in the months leading up to the war represent one of the most aggressive intelligence-sharing campaigns by the West since the Cuban missile crisis (Riemer, 2022).

However, the events following 24 February 2022 suggest that public intelligence was insufficient as a deterrent. Despite extensive disclosures, Russian leadership proceeded with the invasion, indicating that either deterrence through transparency failed or Moscow had already resolved to pursue military action regardless of external signals (Jonsson, 2024; Nakashima *et al.*, 2022). The Russian intelligence community was likely well aware of the US and UK penetrations of its decision-making structures but calculated that disinformation and strategic denial would mitigate the resulting impact (Huminski, 2023). Future analyses of Russian decision-making processes may provide further insight into whether intelligence disclosures influenced Kremlin's calculations at any stage. Nevertheless, the failure of intelligence-based deterrence in Ukraine raises critical questions about the effectiveness of the strategy in conflicts where adversaries are committed to offensive action regardless of external pressures (Dylan and Maguire, 2022).

Beyond deterrence, intelligence disclosure served as a means to exert pressure on Western allies, particularly France and Germany, which initially hesitated to take strong action against Russia (Michaels, 2024; Von Der Burchard and Herszenhorn, 2022). The US and British intelligence agencies frequently released reports on Russian troop movements and strategic intentions, aiming to galvanise European support for a unified response. German Chancellor Olaf Scholz, for example, initially sought a diplomatic reset with Moscow and emphasised the importance of maintaining dialogue with Russian President Vladimir Putin (Dettmer, 2022). However, as intelligence disclosures intensified, highlighting Russia's military build-up and aggressive posture, European scepticism began to erode, leading to a gradual alignment with the US and UK positions (De La Baume, 2022).

A key divergence between intelligence strategies among Western allies is evident in the differing approaches of France and Germany, compared to those of the United States and the United Kingdom. While the latter engaged in daily public disclosures, France and Germany refrained from such measures, primarily due to their national security doctrines, which did not view Russia as the foremost threat before the invasion (Marleku, 2022; Meijer and Brooks, 2021). Another case of intelligence failure in the lead-up to the war is that of Sweden. Swedish intelligence initially underestimated Russia's willingness to launch a full-scale invasion, illustrating the broader difficulty of predicting strategic intent. The intelligence misjudgement by France's Directorate of Military Intelligence (DRM) further underscores this challenge, culminating in the resignation of its chief, General Eric Vidaud after the agency failed to anticipate the full-scale invasion (Jonsson, 2024).

A crucial function of intelligence disclosure in the Ukraine War is countering Russian disinformation campaigns. Russia has employed hybrid warfare tactics for long, leveraging state-controlled media, social networks, and intelligence agencies to propagate misleading narratives and justify military aggression (Davies, 2024; Khaldarova and Pantti, 2019;

Marleku and Aliu, 2023; Marleku and Belaj, 2023; Marleku and Belaj, 2025 Marleku and Llalloshi, 2024). Western intelligence agencies sought to neutralise these efforts by proactively releasing intelligence that pre-emptively debunked Russian claims, thereby shaping global public opinion and fortifying allied resolve (Huminski, 2023).

The strategic goal was to expose and delegitimise Russia's justifications for war, particularly its false narratives about threats from NATO and Ukraine's alleged provocations. This approach aligns with the "narrative superiority" concept, wherein a state seeks to control the information space by consistently presenting a fact-based, authoritative counter-narrative. The daily US and British intelligence briefings aimed to flood the information sphere with accurate, verifiable data to challenge Russian propaganda (Duffield, 2023). The extent of Western intelligence disclosures is unparalleled, using Open-Source Intelligence (OSINT) and strategic intelligence leaks to dismantle Russian efforts to control the narrative systematically (Holmgren, 2024; Jonsson, 2024).

While public intelligence proved effective in shaping diplomatic responses and countering Russian disinformation, its implementation faced notable challenges. The success of this approach relies on precise coordination, timely dissemination, and the credibility of the released information (Shaaban Abdalla *et al.*, 2022). If executed poorly, intelligence disclosures risk backfiring, either by undermining trust in intelligence sources or by failing to sway sceptical audiences (Schwartz and Sevastopulo, 2022). The challenge of sustaining credibility is particularly evident in cases where intelligence assessments were later contradicted by battlefield developments, raising concerns about the long-term viability of public intelligence as a strategic tool (Huminski, 2023). Additionally, the repeated exposure of intelligence may diminish its effectiveness over time, as adversaries adapt their countermeasures to limit vulnerabilities (Duffield, 2023).

Ultimately, the Ukraine War demonstrated the benefits and pitfalls of public intelligence as a tool of modern statecraft. While it successfully countered Russian propaganda and strengthened Western diplomatic cohesion, it failed as a deterrence mechanism. Whether this approach becomes a staple of future conflicts or remains an exception dictated by the specific conditions of the Ukraine War remains an open question (Dylan and Maguire, 2022). As intelligence agencies refine their strategies, the balance between secrecy and transparency will continue to shape the evolving landscape of international security and strategic communication (Duffield, 2023; Jonsson, 2024).

Risks and rewards of public intelligence: insights from Iraq, Ukraine, and Israel

Implementing real-time declassified intelligence as a strategic tool presents inherent challenges (Carnegie and Carson, 2020). Using intelligence disclosures to deter adversaries, counter disinformation, and shape diplomatic narratives carries significant risks, particularly in contexts where intelligence credibility has been previously compromised. These risks can dissuade states from adopting this approach and depend on several factors, including the nature of the intelligence being released, the sensitivity of the geopolitical event, the distribution method, and the government's ability to manage such disclosures effectively (Duffield, 2023; Dylan and Maguire, 2022). The Russo-Ukrainian war has demonstrated both benefits and limitations of public intelligence disclosures. While the United States and the United Kingdom employed intelligence to warn of the impending invasion, scepticism persisted among allies, such as Germany and France, due to past intelligence failures (Jonsson, 2024; Michaels, 2024). Intelligence agencies, particularly those in Europe, faced challenges in maintaining their credibility and influence in

domestic and international affairs due to past instances of politicisation (Gustafson *et al.*, 2024; Huminski, 2023). This underscores the importance of maintaining the integrity and independence of intelligence agencies in order to uphold credibility and sustain public trust (Collins, 2019; Duffield, 2023).

The 2003 Iraq War remains a defining example of intelligence used for political ends. In their pursuit of regime change in Iraq, the Bush administration and the British government presented intelligence on weapons of mass destruction (WMDs) as a justification for military intervention. US Secretary of State Colin Powell's presentation to the United Nations Security Council was critical in securing international support for the invasion (Gustafson *et al.*, 2024; Zarefsky, 2007). However, the subsequent failure to locate WMDs in Iraq exposed significant flaws in the intelligence assessments and led to widespread criticism of the intelligence community's role in legitimising military action (Collins, 2019). The intelligence failure in Iraq, widely regarded as one of the most consequential in modern history, severely damaged the credibility of the US intelligence apparatus, fuelling scepticism about intelligence disclosures in future conflicts (Kessler, 2019). This breach of trust had long-term implications: it weakened international confidence in US intelligence assessments and fostered resistance to subsequent intelligence-based diplomatic efforts (Borger, 2021; Huminski, 2023). Furthermore, adversaries, such as Russia, have exploited intelligence failures, like those in Iraq, to discredit Western intelligence claims, adding another layer of complexity to the use of intelligence as a policy tool (Jonsson, 2024; Shaaban Abdalla *et al.*, 2022).

The Iraq case offers a compelling example of orchestrated public intelligence. According to Hastedt (2005), the Bush administration launched a sustained campaign to build public and international support for the 2003 Iraq War, using intelligence selectively to justify pre-emptive military action. Senior officials—including President George W. Bush, Vice President Dick Cheney, and Secretary of State Colin Powell—publicly cited intelligence assessments that were often disputed or later discredited, such as claims regarding aluminium tubes and WMD procurement from Africa. The White House Iraq Group (WHIG) coordinated talking points and media appearances to saturate the narrative with intelligence-based justifications. This case exemplifies what Hastedt (2005) describes as "orchestrated intelligence," where disclosures are sustained, strategic, and largely uncontested during dissemination. The result was a reshaped policy debate that marginalised dissenting intelligence voices and significantly damaged the long-term credibility of US intelligence institutions (Hastedt, 2005).

The repercussions of the Iraq intelligence debacle resurfaced nearly two decades later during the Ukraine crisis. Despite high-confidence warnings from the US and UK intelligence regarding Russia's impending invasion, scepticism persisted among key European allies, particularly France and Germany, due to the lingering credibility deficit from Iraq (Dylan and Maguire, 2022). Intelligence-sharing hesitancy among these nations reflected a broader reluctance to embrace intelligence-based pre-emptive strategies fully (Jonsson, 2024). The delayed recognition of the accuracy of the intelligence reinforces the enduring consequences of past intelligence failures and highlights the complex interplay between historical credibility, intelligence trustworthiness, and geopolitical decision-making (Duffield, 2023; Shaaban Abdalla *et al.*, 2022). Additionally, Swedish intelligence services faced scrutiny for initially underestimating the likelihood of a full-scale Russian invasion, further demonstrating the challenges of accurately interpreting and acting on intelligence assessments in real-time (Jonsson, 2024).

The cases of Iraq (2003) and Ukraine (2022) illustrate how intelligence can be leveraged by policymakers to shape domestic and international opinions, influence political stances,

and justify strategic decisions (Davies, 2024). These instances demonstrate the broader trend of states using intelligence disclosures to assert influence, shape narratives, and manipulate geopolitical alignments (Duffield, 2023; Dylan and Maguire, 2022). During the Iraq War, the Bush administration aggressively sought support from allies, pressuring countries, such as France and Canada, to align with US policy objectives. Intelligence assessments were used to strengthen coalition-building efforts, reinforcing the notion that intelligence serves as a tool for diplomatic persuasion (Barnes, 2020). Conversely, intelligence has also been utilised as a bargaining instrument, exemplified by the Trump administration's pressure on European allies to exclude Huawei from their 5G networks; the pressure came in the form of a threat to curtail intelligence-sharing agreements (Dylan, 2022; Sutherland, 2020). This illustrates how intelligence disclosure is often wielded as a geopolitical lever to shape security policies and strategic alliances. While the use of public intelligence can be effective, experts caution against its indiscriminate application (Shaaban Abdalla *et al.*, 2022). The declassification of intelligence should not be reduced to a deterrence mechanism alone, as it carries inherent risks, including the possibility of misinformation, political manipulation, and unintended diplomatic fallout (Duffield, 2023; Jonsson, 2024).

The Israel–Hamas conflict in 2023–2024 presents a third and more cautious model of public intelligence. While Israeli intelligence had robust surveillance on Hamas, most disclosures remained classified or selectively communicated through official statements, rather than systematic declassification. Israel opted not to engage in real-time public intelligence releases, possibly due to the asymmetric nature of the conflict and operational sensitivities. Unlike Ukraine, where intelligence disclosures aimed to mobilise international opinion, Israel's approach emphasised internal cohesion and strategic ambiguity. This variation demonstrates that intelligence transparency is not a universally applied doctrine but one shaped by the nature of the adversary, the structure of the conflict, and domestic political considerations (Duffield, 2023; Holmgren, 2024).

Public intelligence should be employed selectively, with careful consideration of the reliability of the information, the potential strategic benefits, and the broader geopolitical implications (Huminski, 2023). Policymakers must exercise discretion in determining what intelligence should be made public, as disseminating inaccurate information can significantly damage a state's reputation and erode long-established trust (Gustafson *et al.*, 2024). As critical elements of statecraft, intelligence institutions play a crucial role in shaping perceptions and guiding decision-making. The Iraq case underscores the dangers of releasing flawed intelligence, while the Ukraine case demonstrates the potential for restoring credibility through accurate forecasting and strategic transparency (Duffield, 2023; Gustafson *et al.*, 2024). Furthermore, Swedish intelligence failures in assessing Russian intentions further reinforce the need for rigorous analytical scrutiny and careful management of intelligence disclosures (Jonsson, 2024).

The Ukraine War raises the question of whether public intelligence will become a standard model for deterring aggression, countering misinformation, and shaping global narratives (Schwartz and Sevastopulo, 2022). Some scholars argue that the proliferation of digital communication and technological revolution will accelerate the adoption of intelligence diplomacy, as states increasingly rely on rapid information dissemination to influence audiences (Duffield, 2023). Rolf Mowatt-Larssen, a former CIA operations officer, characterises the Western intelligence approach in Ukraine as a "new paradigm for intelligence," predicting that intelligence-led strategic communication will expand in future geopolitical conflicts. However, the long-term sustainability and effectiveness of this approach remain contested within international relations discourse (Gustafson *et al.*, 2024; Schwartz and Sevastopulo, 2022).

Table 1. Models of public intelligence disclosure. Source: Author's own elaboration, 2025.

Case	Model	Characteristics
Iraq	Orchestrated and politicised	Intelligence used systematically to justify war; driven by top-level political agendas; dissent within agencies sidelined.
Ukraine	Strategic and real-time	Intelligence declassified in near real-time; aimed at deterring aggression, aligning allies, and countering disinformation.
Israel	Selective and cautious	Minimal public disclosure; intelligence retained for internal use due to operational sensitivity and the asymmetry of the conflict.

The Iraq, Ukraine, and Israel cases illustrate three distinct models of public intelligence practice. In Iraq, intelligence was orchestrated and politicised—deployed systematically by top US officials to justify military intervention, often in ways that ignored or misrepresented dissent within the intelligence community (Hastedt, 2005). The Ukraine case represents a strategic and real-time approach, using intelligence transparently and rapidly to influence adversary behaviour and build international consensus. Israel's approach, by contrast, was selective and cautious, reflecting operational concerns and asymmetric conflict dynamics. These cases show that intelligence disclosure is not a one-size-fits-all strategy but, rather, a flexible tool shaped by context, leadership, and intended audience.

Conclusions

The findings of this paper underscore that intelligence dissemination, previously confined to classified circles, has evolved into a public-facing tool of strategic statecraft. The Ukraine War departed from conventional intelligence practices, as the United States and the United Kingdom leveraged real-time declassification to counter Russian disinformation, pressure allies into unified action, and influence global public opinion. This shift represents a significant development in intelligence studies, raising opportunities and challenges for future conflicts.

A crucial finding is that public intelligence disclosures effectively neutralised Russian misinformation and shaped global diplomatic responses. According to the Royal United Services Institute's study on the "Ukraine model," the rapid release of intelligence updates played a vital role in disrupting Russia's ability to control the narrative surrounding the invasion (Duffield, 2023). Unlike past conflicts, where intelligence primarily informed policymakers, the Ukraine War demonstrated that real-time intelligence-sharing could shape battlefield perceptions, prevent adversarial propaganda from gaining traction, and reinforce Western diplomatic cohesion (Jonsson, 2024). However, this model has limitations, as the deterrence effect of intelligence disclosures did not prevent Russia's full-scale invasion, suggesting that intelligence transparency alone cannot dissuade committed aggressors (Holmgren, 2024).

Another key finding is that intelligence disclosure is a double-edged sword when employed as a diplomatic strategy. While it succeeded in rallying Western allies, particularly after initial scepticism from Germany and France, it also revealed deep-seated trust issues stemming from past intelligence failures, notably the 2003 Iraq War (Dylan and Maguire, 2022). The reluctance of some European allies to accept US intelligence assessments before the invasion highlights the long-term impact of intelligence credibility on alliance cohesion. This underscores that while intelligence disclosures can be a powerful diplomatic tool, their effectiveness depends on the historical trustworthiness of the disclosing state and the geopolitical context in which they are deployed (Shaaban Abdalla *et al.*, 2022).

From a broader perspective, these findings suggest that public intelligence is not a universally applicable strategy but, rather, a context-dependent tool. The Israel–Hamas war demonstrated that the "Ukraine model" is not a one-size-fits-all approach. The United Kingdom's reluctance to employ real-time intelligence disclosures in that conflict illustrates that intelligence transparency is most effective in symmetrical warfare scenarios, where disinformation can be countered with authoritative evidence (Duffield, 2023). In contrast, conflicts characterised by insurgency and asymmetrical tactics, such as those involving Hamas, pose greater challenges to intelligence-based deterrence.

The implications of these findings for intelligence studies and international relations are profound. The Ukraine case suggests that intelligence has transitioned from a covert statecraft instrument to an overt strategic influence tool. This transformation calls for the re-evaluation of traditional intelligence paradigms, particularly in an era where open-source intelligence (OSINT) and AI-driven analytics reshape how information is collected and disseminated (Janssen, 2012). Moreover, the ethical and strategic risks of intelligence disclosures—such as the potential for adversaries to adapt their countermeasures—remain the areas of concern for policymakers (Huminski, 2023).

The comparative analysis of Iraq, Ukraine, and Israel demonstrates that public intelligence strategies differ significantly across conflicts. While the Iraq case revealed the dangers of orchestrated and politicised intelligence, Ukraine highlighted the potential of real-time disclosures for narrative control and alliance cohesion. Israel's more cautious approach, shaped by operational sensitivity, underscores that intelligence transparency must be adapted to the context of conflict. These distinctions illustrate that public intelligence is not a standardised model but a strategic tool contingent on geopolitical circumstances, leadership styles, and institutional credibility.

The public intelligence model deployed in the Russo-Ukrainian war represents both innovative strategy and cautionary precedent. While it successfully countered Russian disinformation and reinforced Western unity, its failure to deter aggression raises critical questions about its broader applicability. The credibility of intelligence disclosures, the geopolitical environment, and the nature of the adversary play decisive roles in determining the effectiveness of this approach. Future research should explore whether intelligence transparency will become a standard feature of modern conflict or whether the Ukraine case remains an exceptional instance shaped by unique geopolitical conditions. As intelligence agencies refine their methodologies, balancing secrecy and transparency will be a defining challenge in the evolving landscape of intelligence and international security.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

Disclosure Statement

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

References

Barnes, A. (2020) 'How Canada's intelligence agencies helped keep the country out of the 2003 Iraq war', *Open Canada*. Available at: https://opencanada.org/how-canadas-intelligence-agencies-helped-keep-the-country-out-of-the-2003-iraq-war/ (Accessed: 8 September 2022).

Borger, J. (2021) 'Colin Powell's UN speech: A decisive moment in undermining US credibility', *The Guardian*, 18 October. Available at: https://www.theguardian.com/us-news/2021/oct/18/colin-powell-un-security-council-iraq (Accessed: 8 September 2022).

Brown, D. (2022) 'Ukraine conflict: Where are Russia's troops?', *BBC News*, 23 February. Available at: https://www.bbc.com/news/world-europe-60158694 (Accessed: 25 August 2022).

Buluc, R., Radu, A. and Bogzeanu, C. (2025) 'One voice or many? Stakeholder interactions in building a public intelligence culture', *International Journal of Intelligence and CounterIntelligence*, 38(3), pp. 897–914. doi: 10.1080/08850607.2025.2479997.

Carnegie, A. and Carson, A. (2020) *Secrets in global governance: disclosure dilemmas and the challenge of international cooperation*. Cambridge: Cambridge University Press.

Collins, A. (ed.) (2019) *Contemporary security studies*, 5th edn. Oxford: Oxford University Press.

Corera, G. (2022) 'Ukraine: Inside the spies' attempts to stop the war', *BBC News: Europe*, 8 April. Available at: https://www.bbc.com/news/world-europe-61044063 (Accessed: 31 August 2022).

Davies, P.H.J. (2024) 'Counterintelligence and escalation from hybrid to total war in the Russo-Ukrainian conflict 2014–2024', *Intelligence and National Security*, 39(3), pp. 496–514. doi: 10.1080/02684527.2024.2329419.

De La Baume, M. (2022) 'France spooked by intelligence failures', *POLITICO*. Available at: https://www.politico.eu/article/france-military-intelligence-failure-russia-invasion-ukraine/ (Accessed: 2 September 2022).

Dettmer, J. (2022) 'Smaller European nations uneasy as Germany's Scholz plans to meet Putin', *Voice of America*, 3 January. Available at: https://www.voanews.com/a/smaller-european-nations-uneasy-as-germany-scholz-plans-to-meet-putin/6379981.html (Accessed: 2 September 2022).

Duffield, J. (2023) *The "Ukraine model" for intelligence disclosure may not be the new normal*, Royal United Services Institute (RUSI). Available at: https://rusi.org/explore-our-research/publications/commentary/ukraine-model-intelligence-disclosure-may-not-be-new-normal (Accessed: 6 February 2025).

Dylan, H. (2022) *How has public intelligence transformed the way this war has been reported?*, Feature from King's College London, King's College London. Available at: https://www.kcl.ac.uk/how-has-public-intelligence-transformed-the-way-this-war-has-been-reported (Accessed: 7 February 2025).

Dylan, H. and Maguire, T.J. (2022) 'Secret intelligence and public diplomacy in the Ukraine War', *Survival*, 64(4), pp. 33–74. doi: 10.1080/00396338.2022.2103257.

Gustafson, K., Lomas, D., Wagner, S., Shaaban Abdalla, N. and Davies, P.H.J. (2024) 'Intelligence warning in the Ukraine war, Autumn 2021–Summer 2022', *Intelligence and National Security*, 39(3), pp. 400–419. doi: 10.1080/02684527.2024.2322214.

Harris, S. and Sonne, P. (2021) 'Russia planning massive military offensive against Ukraine involving 175,000 troops, US intelligence warns', *Washington Post*, 3 December. Available at: https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html (Accessed: 29 August 2022).

Hastedt, G. (2005) 'Public intelligence: Leaks as policy instruments – The case of the Iraq war', *Intelligence and National Security*, 20(3), pp. 419–439. doi: 10.1080/02684520500268897.

Hedley, J.H. (2005) 'Learning from intelligence failures', *International Journal of Intelligence and CounterIntelligence*, 18(3), pp. 435–450. doi: 10.1080/08850600590945416.

Holmgren, B. (2024) 'The age of intelligence diplomacy: The Iraq highlighted its risks. Russia's war in Ukraine showcased its opportunities', *Foreign Policy*. Available at: https://foreignpolicy.com/2024/02/19/russia-ukraine-us-intelligence-diplomacy-invasion-anniversary/ (Accessed: 6 February 2025).

Huminski, J.C. (2023) 'Russia, Ukraine, and the future use of strategic intelligence', PRISM, 10(3), pp. 9–25.

Janssen, K. (2012) 'Open government data and the right to information: Opportunities and obstacles', *The Journal of Community Informatics*, 8(2), Special Issue. doi: 10.15353/joci.v8i2.3042.

Jensen, M.A. (2012) 'Intelligence failures: What are they really and what do we do about them?', *Intelligence and National Security*, 27(2), pp. 261–282. doi: 10.1080/02684527.2012.661646.

Jonsson, M. (2024) 'Swedish intelligence, Russia and the war in Ukraine: Anticipations, course, and future implications', *Intelligence and National Security*, 39(3), pp. 443–457. doi: 10.1080/02684527.2024.2325248.

Kessler, G. (2019) 'The Iraq war and WMDs: An intelligence failure or White House spin?', *Washington Post*, 22 March. Available at: https://www.washingtonpost.com/politics/2019/03/22/iraq-war-wmds-an-intelligence-failure-or-white-house-spin/ (Accessed: 8 September 2022).

Khaldarova, I. and Pantti, M. (2019) 'Fake news: The narrative battle over the Ukrainian conflict', in Allan, S., Carter, C., Cushion, S., Dencik, L., Garcia-Blanco, I., Harris, J., Sambrook, R., Wahl-Jorgensen, K. and Williams, A. (eds.) *The future of journalism: risks, threats and opportunities*, 1st Ed. New York, NY: Routledge, pp. 228–238.

Maguire, T.J. (2015) '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*, 30(5), pp. 637–666. doi: 10.1080/02684527.2014.895570.

Marleku, A. (2022) '*Kakofonia strategjike dhe kërcënimi rus* (*Strategic cacophony and the Russian threat*)'. Available at: https://sbunker.net/teh/91299/kakofonia-strategjike-dhe-kercenimi-rus/ (Accessed: 7 August 2022).

Marleku, A. and Aliu, D. (2023) 'Russian influence on the European integration process of the Western Balkan countries: A comparative analysis', *UNISCI Journal*, 21(62), pp. 183–200. doi: 10.31439/UNISCI-175.

Marleku, A. and Belaj, E. (2025) 'The influence of the Ukraine war on threat perceptions and security dynamics in the Western Balkans', *New Perspectives*, 0(0). doi: 10.1177/2336825X251340931.

Marleku, A. and Belaj, E. (2023) 'Impact of the Ukraine war on the evolution of threat perceptions in the Western Balkans', *UBT International Conference*, 10, *UBT Knowledge Center* [Preprint]. Available at: https://knowledgecenter.ubt-uni.net/conference/IC/ps/10/ (Accessed: 15 July 2025).

Marleku, A. and Llalloshi, E. (2024) 'The impact of the war in Ukraine on conscription policies in Western Balkan countries', in Hajrizi, E. (ed.) *Proceedings of the 13th International Conference on Business, Technology and Innovation: Political Science and International Relations Section*. Prishtina: UBT Press, pp. 154–155. Available at: https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=4716&context=conference#page=20 (Accessed: 15 July 2025).

Meijer, H. and Brooks, S.G. (2021) 'Illusions of autonomy: Why Europe cannot provide for its security if the United States pulls back', *International Security*, 45(4), pp. 7–43. doi: 10.1162/isec_a_00405.

Michaels, E. (2024) 'Caught off guard? Evaluating how external experts in Germany warned about Russia's war on Ukraine', *Intelligence and National Security*, 39(3), pp. 420–442. doi: 10.1080/02684527.2024.2330133.

Moore, R. (2022a) 'Running out of steam…'. Twitter (@ChiefMI6). Available at: https://twitter.com/ChiefMI6/status/1553309715299536896 (Accessed: 30 August 2022).

Moore, R. (2022b) 'This attack was long planned, unprovoked, cruel aggression. No amount of Russian disinformation will now disguise that fact from the international community'. Twitter (@ChiefMI6). Available at: https://twitter.com/ChiefMI6/status/1496939918416916484 (Accessed: 1 September 2022).

Murauskaite, E.E. (2024) *U.S. assistance to Ukraine in the information space: Intelligence, cyber, and signaling*. College Park, MD: Asymmetric Threats Analysis Center (ATAC), University of Maryland, pp. 59–80. doi: 10.1515/9783111338965-005.

Nakashima, E., Harris, S., Horton, A. and Birnbaum, M. (2022) 'U.S. intelligence shows Russia's military pullback was a ruse, officials say', *Washington Post*, 17 February. Available at: https://www.washingtonpost.com/world/2022/02/17/ukraine-russia-putin-nato-munich/ (Accessed: 1 September 2022).

Nee, W. (2025) 'Twitter as a source of competitive intelligence', *SCIP*. Available at: https://www.scip.org/page/Twitter_as_a_Source_of_Competitive_Intelligence (Accessed: 11 February 2025).

Phythian, M. (2014) 'Cultures of national intelligence', in Dover, R., Goodman, M. and Hillebrand, C. (eds.) *Routledge companion to intelligence studies*. Milton Park, Oxfordshire: Routledge, pp. 33–42.

Pinkus, J. (2013) 'Intelligence and public diplomacy: The changing tide', *Journal of Strategic Security*, 7(1), pp. 33–46. doi: 10.5038/1944-0472.7.1.3.

Riemer, O. (2022) 'Intelligence and the war in Ukraine: The limited power of public disclosure', *The Institute for National Security Studies*. Available at: https://www.inss.org.il/wp-content/uploads/2022/03/no.-1577.pdf. (Accessed: 15 July 2025).

Rovner, J. (2015) *Fixing the facts: National security and the politics of intelligence*, reprint edn. Ithaca: Cornell University Press.

Schwartz, F. and Sevastopulo, D. (2022) '"A real stroke of genius": US leads efforts to publicise Ukraine intelligence', *Financial Times*, 6 April. Available at: https://www.ft.com/content/9b3bc8c0-d511-4eec-9cbd-5a4f432f6909 (Accessed: 25 August 2022).

Scott, L. and Jackson, P. (2004) 'The study of intelligence in theory and practice', *Intelligence and National Security,* 19(2), pp. 139–169. doi: 10.1080/0268452042000302930.

Shaaban Abdalla, N., Davies, P.H.J., Gustafson, K., Lomas, D. and Wagner, S. (2022) *Intelligence and the war in Ukraine: Part 1*, *war on the rocks*. Available at: https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/ (Accessed: 1 September 2022).

Stewart, P. (2022) 'CIA director estimates 15,000 Russians killed in Ukraine war', *Reuters*: Europe, 20 July. Available at: https://www.reuters.com/world/europe/cia-director-says-some-15000-russians-killed-ukraine-war-2022-07-20/ (Accessed: 30 August 2022).

Sutherland, E. (2020) '5G security – The politics of Huawei equipment in the United Kingdom', *SSRN*, Rochester, NY. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654596 (Accessed: 14 July 2025).

Von Der Burchard, H. and Herszenhorn, D.M. (2022) 'Russian test for Scholz: Ukraine crisis exposes divisions in Berlin', *POLITICO*. Available at: https://www.politico.eu/article/germany-russia-ukraine-crisis-olaf-scholz/ (Accessed: 2 September 2022).

Winter-Levy, S. (2024) 'The emerging age of AI diplomacy: To compete with China, the United States must walk a tightrope in the Gulf', *Foreign Affairs*. Available at: https://www.foreignaffairs.com/united-states/emerging-age-ai-diplomacy (Accessed: 6 February 2025).

Zarefsky, D. (2007) 'Making the case for war: Colin Powell at the United Nations', *Rhetoric & Public Affairs*, 10(2), pp. 275–302. doi: 10.1353/rap.2007.0043.

Zegart, A. (2022) 'Open secrets', *Foreign Affairs*, 20 December. Available at: https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart (Accessed: 11 February 2025).