NEMZETBIZTONSÁGI SZEMLE

13. évfolyam (2025) 2. szám 3–17. | DOI: 10.32561/nsz.2025.2.1

Szabolcs Lóránt[1]

Public Intelligence in Public Diplomacy

U.S. Strategic Intelligence Sharing in the New Age of Great Power Competition

This paper examines the evolution of intelligence sharing as a tool of public diplomacy through analysis of two recent cases: the U.S. intelligence disclosures preceding Russia's 2022 invasion of Ukraine and the 2023 Chinese surveillance balloon incident. Drawing on declassified documents and contemporary reporting, the article demonstrates how intelligence sharing has transformed from a purely operational tool into a sophisticated instrument of public diplomacy. The paper reveals distinct approaches to intelligence disclosure: systematic pre-emptive sharing in Ukraine versus rapid crisis response during the balloon incident. Both cases, however, demonstrate the U.S. Intelligence Community's growing sophistication in balancing operational security with strategic communication needs. Through comparative analysis, the article identifies key patterns in how intelligence sharing can shape international narratives, build coalition support, and counter adversary messaging while maintaining credibility and protecting sources. This evolution in intelligence sharing practices, formalised in U.S. Intelligence Community Directive 405, represents a significant development in how intelligence services engage with both foreign governments and public audiences in an era of digital information warfare and great power competition.

Keywords: *intelligence sharing, public diplomacy, intelligence diplomacy, strategic communication, narrative control*

Introduction

The strategic use of intelligence in international relations has evolved dramatically in recent years, particularly in its relationship with public diplomacy – the practice of openly conducting diplomatic efforts to influence foreign public opinion.[2] Intelligence can serve

[1] PhD candidate, Ludovika University of Public Service, Doctoral School of Military Sciences, e-mail: lorant.szabolcs@stud.uni-nke.hu

[2] See "public diplomacy, n." Oxford English Dictionary Online.

as a powerful tool for public diplomacy, providing governments with evidence-based legitimacy for their decisions rather than relying on ideology or instinct.[3]

This evolution is particularly evident in today's rapidly changing intelligence landscape, where the fusion of technological capabilities with strategic communication has become increasingly crucial. As Anne Neuberger, former NSA Chief Risk Officer, argues, while AI and technological advancement are revolutionising intelligence capabilities – from rapid translation to pattern recognition – the art of intelligence remains deeply human.[4]

Israel's recent Hezbollah pager operation illustrates this duality perfectly. While the technical sophistication of creating untraceable booby-trapped devices was remarkable, the true intelligence mastery lay in the decade-long deception operation, involving elaborate front companies, strategic timing of the attack, and carefully orchestrated information release. As one Mossad agent described it to CBS News: "We create a pretend world […] we write the screenplay, we're the directors, we're the producers, we're the main actors, and the world is our stage."[5]

The strategic use of intelligence in the public domain – what we might call "public intelligence diplomacy" – has become a sophisticated tool of statecraft. The U.S. Intelligence Community, in its directive ICD 405, defines intelligence diplomacy (ID) as follows: "ID is the sharing of intelligence […] either directly with a foreign government or, where appropriate, publicly, to encourage engagement, collaboration, or collective action among foreign governments." The ICD clearly distinguishes between the different layers of activities:

> "An ID effort must satisfy three criteria: First, it has to involve the sharing of objective intelligence, either publicly or directly to a foreign government; this by itself is 'intelligence sharing'. Second, it has to have the goal of exchanging perspectives with a foreign government on a specific threat or issue; this by itself is 'intelligence engagement'. Third, it has to be done in support of advancing a preferred policy objective which may lead to unilateral, joint or multilateral action. The third criterion is what separates intelligence sharing and engagement from ID."[6]

Through selective disclosure of intelligence information, nations can shape international narratives, influence foreign audience perceptions, build coalition support, and counter adversary messaging. This strategic deployment of intelligence serves multiple purposes: from warning allies of imminent threats to exposing adversary operations, from building international consensus to undermining hostile disinformation campaigns.

In this evolving context, today's intelligence landscape is not just about who has the most advanced AI models or the best satellite imagery. It is about how nations strategically leverage their intelligence capabilities – both technological and human – to advance their geopolitical interests in an increasingly complex world.

This conceptual framework helps explain why intelligence sharing can be particularly effective in diplomatic engagement, as the disclosure of intelligence carries unique weight in international discourse.

[3] Pinkus 2014: 33.
[4] Neuberger 2025.
[5] Berg 2024.
[6] Intelligence Community 2025.

This article employs a comparative case study approach, focusing on two recent events: the pre-invasion intelligence sharing campaign regarding Ukraine (2021–2022) and the Chinese surveillance balloon incident (2023). Primary sources include official statements, intelligence releases, media reporting, supplemented by academic analysis of intelligence sharing practices. The use of these sources contributes to our understanding of how intelligence sharing practices differ across contexts and their diplomatic impact. This examination reveals not only the tactical variations in intelligence sharing approaches but also broader strategic implications for public diplomacy in an era of digital information warfare.

Theoretical framework: evolving understanding of intelligence diplomacy

The concept of intelligence diplomacy has undergone significant evolution, particularly in recent years. While existing literature predominantly focuses on intergovernmental aspects of intelligence diplomacy, recent policy developments suggest a broader conceptual framework that includes public engagement and strategic communication.

Traditional scholarly understanding of intelligence diplomacy emphasises intelligence chiefs "coming out of the shadows" to engage in direct diplomatic interactions with foreign counterparts.[7] This classical interpretation primarily concerns government-to-government relations, in line with the scope of the US ICD 403 (2013) directive and its definition of foreign entities as "foreign governments or components thereof; international organizations or coalitions consisting of sovereign states".[8]

The introduction of ICD 405 marks a significant development in intelligence sharing practices in the United States. Pinkus has already identified the concept of "public use of intelligence" (citing Hastedt), which he interpreted as "using intelligence for public diplomacy".[9]

Building on this foundation, this article proposes the term "public intelligence diplomacy" to specifically describe the comprehensive framework formalised by ICD 405, where intelligence sharing becomes an active diplomatic tool aimed at fostering international engagement and collective action. This conceptual distinction helps differentiate between tactical use of intelligence for domestic audiences, as exemplified in the Iraq War case,[10] and the strategic deployment of intelligence as a diplomatic tool for international engagement. The ICD 405 directive explicitly codifies this practice at the policy level, extending beyond both traditional intergovernmental frameworks and tactical domestic communication.

This evolution in intelligence sharing practices represents a significant departure from traditional approaches. As Gioe (2025) highlights, intelligence cooperation has historically operated through what practitioners term "liaison" – deliberately hidden channels meant to remain unaffected by international politics and shifts in foreign policy.

[7] Taylor 2023.

[8] Intelligence Community 2013.

[9] Pinkus 2014: 36.

[10] Hastedt 2013: 26.

These traditional liaison relationships focused exclusively on secret government-to-government exchanges, with intelligence services carefully maintaining separation from public diplomatic channels.[11]

The emergence of public intelligence diplomacy, therefore, marks a fundamental shift in how intelligence services engage with both foreign governments and public audiences. This transformation aligns with broader changes in diplomatic practice and information sharing in the digital age, while presenting new challenges in balancing transparency with operational security.

The distinction between classical intelligence diplomacy and this emerging strategic approach represents a crucial theoretical development. While the former focuses on covert or semi-covert diplomatic channels between intelligence services, the latter encompasses strategic public communication of intelligence to achieve broader diplomatic objectives through both direct and public channels. Unlike tactical intelligence sharing for domestic audiences, this approach explicitly seeks to "encourage engagement, collaboration, or collective action among foreign governments" while maintaining "analytical integrity, objectivity and rigor in accordance with ICD 203".[12]

This evolution aligns with what observers[13] highlight about intelligence services chiefs increasingly taking active roles in diplomatic processes and foreign policy formation, with intelligence diplomacy complementing conventional diplomacy while maintaining strategic intelligence's crucial role in foreign policy decisions.

This theoretical framework helps illuminate the practical challenges of intelligence disclosure. Intelligence sharing in diplomatic contexts operates within what Carnegie and Carson[14] describe as the "disclosure dilemma" – balancing the potential diplomatic benefits of wide dissemination against operational risks and source protection. This dilemma shaped both the proactive Ukraine disclosures and reactive balloon incident response, though with different risk calculations and strategic objectives.

Strategic information environment

The strategic use of intelligence sharing as a diplomatic tool must be understood within the context of fundamental changes in the global information environment. As Leonardson's review of Rid's work highlights, modern information warfare builds on decades of evolution in influence operations, where success relied on mixing verifiable facts with carefully crafted falsehoods. Digital platforms have dramatically accelerated this dynamic – what historically took months to spread now moves from fringe to mainstream media within hours.[15]

[11] Gioe 2025.

[12] Intelligence Community 2025. Note: The mentioning of ICD 203 is particularly relevant here because: It addresses potential criticism that public intelligence sharing might compromise intelligence integrity for diplomatic gains; ICD 203 specifically requires intelligence analysis to be objective and unbiased, so mentioning it shows that public intelligence diplomacy must still adhere to core intelligence principles; It distinguishes this approach from past problematic uses of intelligence for public diplomacy (like the Iraq War case) where intelligence was potentially politicised.

[13] Marinho et al. 2024.

[14] Cited in Brattvoll 2024.

[15] Leonardson 2020.

In the context of what Valle de Frutos identifies as the "unprecedented challenges of hyperconnectivity generated by digital globalization",[16] intelligence sharing has emerged as a strategic response to establish authoritative narratives. As Rid argues, discussed in Leonardson (2020), mainstream media's vulnerability to manipulation through accelerated news cycles has made traditional counter-disinformation approaches insufficient.

This transformation is particularly evident in U.S. approaches to great power competition, where intelligence sharing has evolved from a primarily secret, state-to-state activity to a public diplomatic instrument. Leonardson's (2020) analysis of Rid's work emphasises how the rise of "amateur surrogates" in information operations – such as social media trolls rather than trained intelligence officers – has necessitated new approaches to maintaining narrative credibility in an environment characterised by systematic manipulation through social networks and artificial intelligence.

This evolution reflects what Brattvoll terms the "capital of the secret" – the special social and political status[17] accorded to classified information, "as it is perceived to be more valuable than other forms of information".[18]

Within this transformed information environment, states must balance the diplomatic advantages of intelligence disclosure against operational security concerns, particularly when countering systematic disinformation campaigns.

The evolution of intelligence sharing frameworks

Since 9/11, the U.S. intelligence community[19] has worked to resolve what the Congressional Research Service identified as a fundamental paradox: intelligence is valuable only when shared with those who need it, but wider sharing increases risks of compromise.[20] This tension directly relates to the frameworks established by ICD 403 and 405, which attempt to balance these competing imperatives.

The initial response focused on removing barriers between intelligence and law enforcement agencies, but this soon expanded into a broader reconsideration of how intelligence could be shared more effectively while maintaining security.

Intelligence Community Directive 403 (2013) and its associated guidance, particularly ICPG 403.3 (2014), emerged from this effort to create structured frameworks for intelligence sharing. These directives established clear procedures for both routine and emergency disclosures of intelligence.

This institutional evolution proved crucial in December 2021, when the United States launched what observers called an "unprecedented" campaign of intelligence sharing about

[16] Valle de Frutos 2024.

[17] Note: As ICD 403 highlights "U.S. intelligence is a national asset to be conserved and protected and will be shared with foreign entities only when consistent with U.S. national security and foreign policy objectives and when an identifiable benefit can be expected to accrue to the U.S." Intelligence Community 2013.

[18] Brattvoll 2024.

[19] The U.S. Intelligence Community consists of 18 organisations: two independent agencies (ODNI and CIA), nine Department of Defense elements (including DIA, NSA, NGA, NRO, and the intelligence elements of the five military services), and seven elements within other federal departments (Energy, Homeland Security, Justice, State, and Treasury).

[20] Best 2011.

Russia's planned invasion of Ukraine.[21] The campaign operated within frameworks carefully developed to balance operational security with strategic communication needs. ICD 403 established baseline requirements for protecting sources and methods, while ICPG 403.3 specifically authorised rapid intelligence sharing when necessary to prevent imminent threats or protect critical operations.

The continuing evolution of intelligence sharing frameworks is evident in the recent ICD 405 (2025), which further formalises intelligence diplomacy practices and provides updated guidance on using intelligence disclosure to advance U.S. foreign policy objectives. This directive represents the Intelligence Community's ongoing efforts to adapt its policies to meet emerging strategic communication needs while maintaining essential security protocols.

The CRS 2011 report's discussion of the shift from a strict "need-to-know" to a more flexible "need-to-share" paradigm after 9/11 helps explain the institutional context in which the 2021–2022 Ukraine disclosures occurred.

Intelligence sharing in practice

The 2022 Threat Assessment

The 2022 Annual Threat Assessment, published in February 2022, provides crucial insight into how the Intelligence Community viewed evolving information warfare dynamics on the eve of Russia's invasion. The assessment acknowledged Russia's aggressive posture, noting that "Russia is pushing back against Washington where it can – locally and globally – employing techniques up to and including the use of force".[22]

The assessment was particularly prescient regarding Ukraine, stating that "Russia continues to prepare for a military attack against Ukraine, with well over 100,000 troops massed near the Ukraine border, including Russian military forces in Belarus, occupied-Crimea, and the separatist forces in Eastern Ukraine. Moscow is sending more forces."[23] This clear identification of Russian preparations provided the foundation for subsequent intelligence disclosures.

The 2022 Annual Threat Assessment was particularly significant in its characterisation of Russia's influence operations. The document identified Russia as "one of the most serious foreign influence threats to the United States", noting Moscow's use of "intelligence services, proxies, and wide-ranging influence tools" to divide Western alliances and undermine U.S. global standing. Crucially, the assessment highlighted Russia's adaptability, observing that Russian influence actors were "adept at capitalizing on current events in the United States to push Moscow-friendly positions to Western audiences".[24]

This understanding of Russia's sophisticated influence capabilities provided important context for the Intelligence Community's subsequent approach to Ukraine. By recognising Moscow's established pattern of using multiple channels to shape international narratives,

[21] Brattvoll 2024.
[22] ODNI 2022: 4.
[23] ODNI 2022: 10.
[24] ODNI 2022: 12.

the U.S. Intelligence Community could anticipate and pre-empt Russian disinformation about Ukraine through its unprecedented disclosure campaign. The assessment's emphasis on how Russia would "seek out new methods of circumventing technology companies' anti-disinformation activities to further expand its narratives globally"[25] helps explain why traditional counter-disinformation approaches alone were deemed insufficient.

The U.S. intelligence sharing campaign in Ukraine

The intelligence sharing campaign preceding Russia's invasion of Ukraine represents a watershed moment in the strategic use of intelligence for diplomatic purposes. As Dylan and Maguire (2022) document, this carefully orchestrated campaign marked a significant evolution in how intelligence can be deployed to shape international responses to emerging security threats. Through systematic disclosure of Russian military preparations and intentions from November 2021 through February 2022, the U.S. and its allies demonstrated how intelligence sharing could serve multiple diplomatic objectives simultaneously: building coalition consensus, establishing narrative control, and attempting strategic deterrence.

The campaign's sophistication is evident in its carefully calibrated approach to timing, content, and audience targeting. By gradually escalating the specificity and scope of intelligence disclosures – from early warnings to detailed assessments of military capabilities and ultimately to specific predictions of invasion timing – the U.S. established a pattern of credible intelligence that helped overcome initial scepticism among European allies. However, this unprecedented level of intelligence sharing also highlighted persistent challenges in balancing operational security with diplomatic effectiveness, particularly given the legacy of previous intelligence controversies.

This evolution in intelligence sharing strategy is particularly evident when examining the specific characteristics and implementation of the Ukraine campaign. The Ukraine case demonstrates a shift from reactive to proactive intelligence sharing. Unlike previous instances of public intelligence sharing, such as Colin Powell's widely discredited 2003 UN presentation on Iraq,[26] where Washington pre-emptively shared intelligence to justify military action, the Ukraine campaign emphasised pre-emptive disclosure to prevent and deter aggression and this way shape diplomatic outcomes.

As Dylan and Maguire note, this approach allowed Western allies to "pre-bunk" Russian disinformation rather than merely respond to it. This strategic shift reflects broader changes in the information environment, where rapid disclosure can help establish narrative dominance. This was not revolutionary but rather evolutionary, building on previous experiences from the Cuban Missile Crisis through to recent cyber threat disclosures. However, the scope, vigour, and frequency of intelligence dissemination, particularly between mid-January and mid-February 2022, marked a novel development in modern international statecraft.[27]

[25] ODNI 2022: 12.

[26] Borger 2021.

[27] Dylan–Maguire 2022.

Some of the key elements characterised this novel approach: the use of high-level, highly sanitised intelligence-led communications[28] deployed through accessible formats, in the press,[29] as well as in social media, the unprecedented use of formal intelligence assessment language in public communications (e.g. "we judge it to be highly likely"), which was previously unusual in public discourse, and the coordination between intelligence and policy communities to manage both the message and the risks.

Coalition management challenges

The campaign revealed both opportunities and limitations in using intelligence for coalition building. While U.S. (and U.K.) intelligence sharing helped shift European positions, particularly in Germany, it also exposed tensions in how different allies assess and use intelligence. The French intelligence community's scepticism of Anglo-American assessments, reminiscent of debates before the Iraq War, highlights how different strategic cultures and intelligence traditions can complicate coalition building through intelligence sharing. This divide was particularly stark between East-Central European nations – for example while Hungary maintained its diplomatic presence and unchanged travel recommendations despite U.S. warnings,[30] Baltic security analysts were sounding the alarm bell warning of an imminent invasion.[31]

Strategic framework and implementation

The U.S.-led intelligence sharing campaign during the Ukraine crisis demonstrates a sophisticated understanding of intelligence's dual role – as both an information source and an instrument of diplomatic influence. As Brattvoll (2024) argues, intelligence disclosure gains particular potency through what he terms the "capital of the secret" – the special social status accorded to classified information that makes its disclosure an especially powerful diplomatic tool. The deliberate disclosure of intelligence served multiple purposes: pre-empting adversary narratives – to let "people around the world [...] see it [the Russian invasion] for what it was"[32] –, building coalition consensus, and demonstrating diplomatic resolve. This represents a departure from traditional intelligence practices where secrecy was paramount.

[28] Note: "intelligence-led communication" refers to intelligence information that was carefully screened to remove/protect sources and methods, sensitive technical capabilities, classified operational details, reformatted for public consumption – simplified technical language, removed intelligence jargon, structured for clear public messaging. Example from Riehle (2024): In the Ukraine case, intelligence about Russian military movements was shared publicly but with technical collection methods and specific sources removed while maintaining the core assessment. The "led" component in the term indicates that while derived from intelligence, the final communication is shaped for diplomatic messaging rather than pure intelligence reporting.

[29] Harris–Sonne 2021.

[30] Hungary Today 2022.

[31] Thomas 2022.

[32] Shapiro 2024.

The campaign's evolution also reflects what Brattvoll (2024) identifies as a crucial shift in strategic objectives: while initially aimed at deterring Russian aggression, intelligence sharing ultimately proved more effective in unifying NATO allies and establishing narrative control. This transformation occurred within what he terms the "disclosure dilemma", where states must balance the potential diplomatic benefits of intelligence sharing against operational risks and source protection concerns.

Risk management

Dylan and Maguire identify three primary categories of risk in public intelligence sharing:

- Adaptation costs: the risk that adversaries will change behaviour or improve their security measures in response to disclosures
- Escalation costs: the potential for public disclosures to limit diplomatic flexibility and force escalatory responses
- Audience costs: the challenge of maintaining credibility when intelligence assessments cannot be fully supported with public evidence

The U.S. approach in Ukraine has shown sophisticated handling of these risks through graduated disclosure and careful institutional coordination.

However, this approach has not been without its critics. As experts note, CIA veterans warned that extensive disclosure could enable adversaries to plant misleading intelligence, arguing "our side has said too much".[33]

Operational effectiveness

The Ukraine crisis marked what Brattvoll (2024) documents as an "unprecedented scale" of intelligence disclosure, with U.S. (as well as U.K.) intelligence services making systematic pre-emptive releases rather than reactive disclosures. As Brattvoll, Dylan and Maguire's work documents, while initial disclosures aimed to deter Russian aggression, they ultimately proved more effective in achieving what he terms "narrative superiority" among NATO allies. This shift from deterrence to coalition building represents a significant development in how intelligence serves diplomatic objectives.

The effectiveness of these disclosures seemed to be amplified by weaknesses in Russian covert actions. Despite Russia's attempts to maintain plausible deniability, their actions were unveiled due to what Riehle sees as a combination of "ignorance, indifference, and incompetence". Russian operations appeared to display ignorance of likely Western reactions, indifference to international opinion, and operational incompetence that made their activities easier to expose. This pattern of behaviour, Riehle argues, ultimately limited Russia's diplomatic and strategic options while strengthening the credibility of Western intelligence disclosures.[34]

[33] Dylan–Maguire 2022.

[34] Riehle 2024.

In brief, the effectiveness of intelligence sharing as a diplomatic tool ultimately depends on maintaining credibility while achieving strategic objectives. The Ukraine case demonstrates how this balance could be achieved through careful institutional management and strategic consideration of risks and benefits. As this practice continues to evolve, the integration of intelligence sharing into broader diplomatic strategy will likely become more sophisticated and nuanced.

The Chinese balloon incident

The "spy balloon episode" of 2023 represents a significant case study in modern intelligence disclosure and public diplomacy.

It emerged against a backdrop of growing U.S. awareness of Chinese intelligence collection capabilities. A declassified National Intelligence Estimate from April 2021 had already identified China's focus on developing "new sophisticated technologies and techniques to collect intelligence from space", establishing important context for understanding the subsequent balloon crisis.[35]

On 1 February 2023, residents in Montana spotted an unexpected white object hovering above them, initiating what would become a complex international diplomatic crisis. The U.S. Department of Defense quickly identified it as a high-altitude surveillance balloon from China, while Chinese authorities maintained it was a civilian weather research vessel that had strayed off course.[36]

The incident highlighted fundamental differences in U.S. and Chinese approaches to strategic communication and public opinion management. As Zhang et al. document, CNN characterised the event as "a watershed moment in the world's dangerous new superpower rivalry", while Chinese media viewed U.S. reactions as "too dramatic" and emphasised international legal frameworks. The technical and legal aspects became central to narrative construction: both sides leveraged Article 8 of the Chicago Convention, which specifies requirements for unmanned aircraft. This ambiguity allowed China to emphasise the "balloon" designation to stress its unmanned, uncontrollable nature, while U.S. military sought evidence from debris to refute this characterisation. Public opinion analysis reveals distinct cognitive differences between Chinese and American audiences. Zhang et al. found marked variation in how media coverage framed the incident – U.S. media emphasised surveillance and security threats, while Chinese coverage focused on legal frameworks and proportionality of response.[37]

The incident's significance lies in how it demonstrates the evolution of intelligence disclosure as a public diplomacy tool. The situation presented a unique opportunity for the parties involved to "leverage murky events to justify their behaviours, rally political support, and promote favourable worldviews". The absence of immediately verifiable facts created what Wong and Mulupi term "raw material" for narrative construction, that is to "construct issue narratives that engaged identity and system narratives".[38]

[35] ODNI 2021.

[36] Wong–Mulupi 2024.

[37] Zhang et al. 2024.

[38] Wong–Mulupi 2024: 1, 4.

The U.S. response demonstrated sophisticated understanding of narrative control in modern information environments. Their immediate characterisation of the object as a "surveillance balloon" achieved remarkable penetration in global discourse. Quantitative analysis shows this framing dominated international coverage, with "almost all of the U.S. (99.39%) and international (93.88%) samples, and more than four-fifths of the Chinese news articles circulating this narrative".[39] This success in narrative establishment forced China into a reactive position, struggling to promote its alternative interpretation of events.

The technical intelligence disclosure strategy employed by the U.S. proved effective. The balloon was "flying as high as 60,000 feet above ground, which puts it at about ten times closer than the lowest Earth-orbiting satellites".[40] This technical detail, combined with information about the balloon's path over sensitive military installations, helped the U.S. establish its surveillance narrative. As Wong and Mulupi document, this allowed the U.S. to reinforce the "king of spying" narrative of China. The incident revealed sophisticated layering of narrative elements. Beyond immediate crisis management, the U.S. successfully connected the balloon incident to broader strategic narratives about Chinese surveillance activities. As Wong and Mulupi observe, this allowed the U.S. to reinforce the narrative of "the identity of China as a surveillance state". This expansion from tactical to strategic messaging demonstrates evolution in U.S. intelligence disclosure practices.[41]

China's counter-narrative efforts, while substantial, struggled to gain international traction. Their alternative framing of the balloon as a civilian weather research vessel affected by "force majeure" found limited resonance in international media. Wong and Mulupi (2024) document that while this narrative achieved 71.11% coverage in Chinese media, it failed to effectively challenge the dominant U.S. interpretation in global discourse.

The incident's aftermath revealed the lasting impact of initial narrative establishment. Even as China attempted to shift discussion toward accusations of U.S. overreaction and violation of international norms, the fundamental U.S. characterisation of the event as a surveillance incident remained dominant. Wong and Mulupi[42] argue that this demonstrates how "the framing in the initial issue narrative could be crucial in the following narrative contest that expands to the identity and system levels".

The evolution of intelligence disclosure in public diplomacy: a comparative analysis

This section represents an analytical synthesis of the cases previously discussed in detail.

The Ukraine and Chinese balloon cases demonstrate distinct yet complementary approaches to intelligence disclosure in modern diplomatic practice. While fundamentally different in their circumstances and execution, these cases jointly illuminate the sophisticated development of U.S. intelligence disclosure strategy in contemporary diplomatic contexts. As Wong, Mulupi (2024) and Brattvoll (2024) demonstrate, both cases show how intelligence

[39] Wong–Mulupi 2024: 10.
[40] Ng–Carley 2023.
[41] Wong–Mulupi 2024: 15.
[42] Wong–Mulupi 2024: 16.

disclosures can shape international narratives, though through markedly different approaches and under varying pressures.

The fundamental distinction lies in the approach to intelligence disclosure in each case. The Ukraine disclosures represented systematic pre-emptive disclosure, where intelligence releases were carefully planned and sequenced to achieve specific diplomatic objectives. In contrast, the balloon incident required rapid response under crisis conditions, demonstrating a different aspect of intelligence sharing as a diplomatic tool.

The timing dimension reveals crucial differences in operational approach while highlighting similar strategic principles. In the Ukraine case, the United States could carefully select and prepare intelligence for release, timing disclosures for maximum diplomatic impact. The balloon incident, however, demanded immediate response. The United States demonstrated remarkable agility in establishing narrative control, achieving dominant global narrative power even under time pressure.

Both cases required sophisticated management of what Dylan and Maguire (2022) identifies as the three primary risks in intelligence disclosure: adaptation costs, escalation costs, and audience costs. The Ukraine disclosures demonstrated careful calibration of these risks through graduated release of intelligence, while the balloon incident required rapid risk assessment under crisis conditions. The contrasting approaches to intelligence sharing in the Ukraine and balloon cases reflect what Brattvoll (2024) identifies as a fundamental tension in modern intelligence diplomacy: the balance between strategic effectiveness and the protection of intelligence sources, methods, and capabilities.

The technical nature of intelligence disclosure also evolved between the cases. In Ukraine, the systematic release focused on Russian military capabilities and intentions, requiring careful calibration of what technical intelligence could be shared while protecting sources and methods. The balloon incident, conversely, required careful balance in technical disclosure – revealing enough about surveillance capabilities to support the narrative while maintaining strategic ambiguity about U.S. counter-surveillance capabilities.

Audience targeting strategies differed significantly between the cases. Ukraine disclosures operated on multiple levels: building international coalition support, shaping global public opinion, and attempting to influence Russian decision-making. This multi-tiered approach required careful calibration of intelligence sharing to address diverse audience needs simultaneously. The balloon incident, however, focused primarily on managing bilateral tensions with China while maintaining broader international credibility about U.S. capabilities and intentions.

Together, these cases demonstrate how intelligence sharing has evolved from a purely operational tool to a sophisticated instrument of public diplomacy, capable of serving different strategic objectives under both planned and crisis conditions.

Conclusions and future implications

Drawing together the threads of our analysis, these cases represent more than isolated incidents of intelligence sharing – they signal a fundamental shift in how the United States deploys intelligence as an instrument of public diplomacy in what Valle de Frutos (2024) identifies as an era of digital geopolitical globalisation. This evolution reflects both technological changes and the increasing importance of information warfare in great power competition.

The success of these intelligence disclosure campaigns suggests several implications for future U.S. public diplomacy practice. First, selective intelligence sharing has proven to be a powerful tool for shaping international narratives when deployed with precision and credibility. The Ukraine case particularly demonstrates how early, accurate intelligence disclosures can help build international coalitions and pre-empt adversary messaging, while the balloon incident shows how rapidly shared intelligence can effectively manage crisis situations and maintain narrative control even under time pressure.

Second, these cases indicate that traditional concerns about protecting sources and methods must be balanced against the strategic benefits of public disclosure. The U.S. Intelligence Community's ability to navigate this balance – revealing enough to achieve diplomatic objectives while protecting critical capabilities – will likely become increasingly important in future scenarios.

The cases presented in this paper demonstrated the diplomatic potential of intelligence sharing. Brattvoll (2024), however, argues that such extensive disclosures are unlikely to become the norm, given the persistent operational risks and institutional constraints. The challenge for the future practice of public intelligence diplomacy lies in maintaining the diplomatic leverage gained through the "capital of secrecy" while protecting intelligence capabilities and sources.

Looking ahead, this merger of intelligence sharing and public diplomacy may become a standard feature of U.S. strategic communication, particularly in confronting challenges from peer competitors. However, its effectiveness will continue to depend on maintaining the credibility established through accurate disclosures in these precedent-setting cases.

References

Berg, Raffi (2024): Ex-Israeli Agents Reveal How Hezbollah Pager Attacks were Carried Out. *BBC,* 23 December 2024. Online: https://www.bbc.com/news/articles/cwy3l02wxqdo

Best, R. A. (2011): *Intelligence Information: Need-to-Know vs. Need-to-Share.* Congressional Research Service Report. Online: https://www.everycrsreport.com/reports/R41848.html

Borger, Julian (2021): Colin Powell's UN Speech: A Decisive Moment in Undermining US Credibility. *The Guardian,* 18 October 2021. Online: https://www.theguardian.com/us-news/2021/oct/18/colin-powell-un-security-council-iraq

Brattvoll, Joakim (2024): Intelligence Disclosure as a Strategic Messaging Tool. *NATO Review,* 16 December 2024. Online: https://www.nato.int/docu/review/articles/2024/12/16/intelligence-disclosure-as-a-strategic-messaging-tool/index.html

Dylan, Huw – Maguire, Thomas J. (2022): Secret Intelligence and Public Diplomacy in the Ukraine War. *Survival,* 64(4), 33–74. Online: https://doi.org/10.1080/00396338.2022.2103257

Gioe, David V. (2025): How America's Allies Boost U.S. Intelligence. *Foreign Affairs,* 13 February 2025. Online: https://www.foreignaffairs.com/united-states/how-americas-allies-boost-us-intelligence

Harris, Shane – Sonne, Paul (2021): Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns. *The Washington Post,* 4 December 2021. Online: https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html

Hastedt, Glenn (2013): The Politics of Intelligence and the Politicization of Intelligence: The American Experience. *Intelligence and National Security,* 28(1), 5–31. Online: https://doi.org/10.1080/02684527.2012.749062

Hungary Today (2022): Ukraine Crisis: Hungarian Foreign Ministry Will Not Evacuate Employees. *Hungary Today,* 24 January 2022. Online: https://hungarytoday.hu/ukraine-crisis-evacuation-nato-hungary-russia-orban-biden-putin/

Intelligence Community (2013): ICD Directive 403. *Office of the Director of National Intelligence,* 13 March 2013. Online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives

Intelligence Community (2025): ICD Directive 405. *Office of the Director of National Intelligence,* 14 January 2025. https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives

Leonardson, J. E. (2020): Review of Active Measures: The Secret History of Disinformation and Political Warfare. *Studies in Intelligence,* 64(1).

Marinho, Jorge – Ventura, Júlio – Ribeiro, Lourenço (2024): Strategic Intelligence and Intelligence Diplomacy in the Sphere of Foreign Policy – Diplomat magazine, 2 June 2024. Online: https://diplomatmagazine.eu/2024/06/02/strategic-intelligence-and-intelligence-diplomacy-in-the-sphere-of-foreign-policy/

Neuberger, Anne (2025): Spy vs. AI. *Foreign Affairs,* 15 January 2025. Online: https://www.foreignaffairs.com/united-states/spy-vs-ai

Ng, Lynnette H. X. – Carley, Kathleen M. (2023): Deflating the Chinese Balloon: Types of Twitter Bots in US-China Balloon Incident. *EPJ Data Science,* 12(1), Article 1. Online: https://doi.org/10.1140/epjds/s13688-023-00440-3

ODNI (2021): *Chinese Space Activities Will Increasingly Challenge US Interests Through 2030.* April 2021. Online: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/3645-chinese-space-activities-will-increasingly-challenge-u-s-interests-through-2030

ODNI (2022): *Annual Threat Assessment of the U.S. Intelligence Community.* February 2022. Online: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Pinkus, Jonathan (2014): Intelligence and Public Diplomacy: The Changing Tide. *Journal of Strategic Security,* 7(1), 33–46. Online: https://doi.org/10.5038/1944-0472.7.1.3

Riehle, Kevin P. (2024): Ignorance, Indifference, or Incompetence: Why are Russian Covert Actions so Easily Unmasked? *Intelligence and National Security,* 39(5), 864–878. Online: https://doi.org/10.1080/02684527.2023.2300165

Shapiro, Jeremy (2024): Letter from Washington: All-Knowing America and US Intelligence Diplomacy. *ECFR,* 18 April. Online: https://ecfr.eu/article/letter-from-washington-all-knowing-america-and-us-intelligence-diplomacy/

Taylor, Chris (2023): *'Doing Good Deeds Quietly': The Rise of Intelligence Diplomacy as a Potent Tool of Statecraft.* Australian Strategy Policy Institute Strategic Insights. Online: https://www.jstor.org/stable/resrep53516

Thomas, Matthew (2022): Major Russian Invasion of Ukraine Imminent. *Baltic Security Foundation,* 21 January 2022. Online: https://balticsecurity.eu/major_russian_invasion_of_ukraine_imminent

Valle de Frutos, S. (2024): La opinión pública internacional en el contexto de la geopolítica de la globalización desinformativa. Análisis desde la teoría de la complejidad y de la baja racionalidad. *Relaciones Internacionales,* (56), 75–93. Online: https://doi.org/10.15366/relacionesinternacionales2024.56.004

Wong, Frankie H. C. – Mulupi, Dinfin (2024): Up in the Air: A Strategic Narrative Contest in the U.S.–China Balloon Incident 2023. *International Communication Gazette,* 0(0). Online: https://doi.org/10.1177/17480485241290361

Zhang, Baoyu – Chen, Tao – Li, Qiang – Zhang, Weishan – Wang, Fei-Yue (2024): Spy Balloon or Sputnik Moment: A Comparative Analysis of Public Opinion in China and the United States. *IEEE Transactions on Computational Social Systems,* 11(3), 3729–3740. Online: https://doi.org/10.1109/TCSS.2023.3333954