STRATEGIC
MONOGRAPH SERIES

INTELLIGENCE IN THE MODERN ERA:
STRATEGIC SHIFTS, CULTURAL DYNAMICS, AND TECHNOLOGICAL ADVANCES

DR. FREDERIC LEMIEUX, DR. SHADI ABOUZEID,
DR. SHAY HERSHKOVITZ



VOLUME 08/2025
RELEASE: AUGUST 2025

STRATEGY INTERNATIONAL

All content included in this publication is the property of
Strategy International (SI) Ltd.
Protected from the copyright laws of the Republic of Cyprus and international copyright laws.



Strategy International (SI) Ltd, Copyright ©2022-2027

Strategy International (SI) Ltd is a registered company HE423632 In the Republic of Cyprus

The logo of Strategy International is a registered trademark in the Republic of Cyprus. The trademark and works of strategy international (SI) Ltd and its logo are applied for class 31&45, in the Republic of Cyprus and EU IPO office.

Cyprus copyrights are governed by the Copyright Section of the Department of the Registrar of Companies and Official Receiver.

The governing laws are: N.63/77, N.18(I)/93, N.54(I)/99, N.12 (I)/2001, N.128 (I)/2002, N.128 (i) 2004 and N.123 (I) 2006.

Copyright protection vests automatically in the Republic of Cyprus.

First Published July 2022
Address: 24 Strovolos Str. 2042 Nicosia Cyprus

This publication is the exclusive property, including copyrights, of the author and Strategy International (SI) Ltd.

This publication in its complete form, or any parts of it, may not be reproduced, duplicated, copied, sold, resold, visited, or otherwise exploited for any commercial purpose. For all purposes, there is a need for a first written consent of the author and the legal representative of Strategy International (SI) Ltd.

SI trademark(s) may not be used in connection with any product or service and publication that has not been given any prior written consent first.

The written publication and opinions are considered of scientific and professional value and as such a result of the ongoing work of the author.

Any official statement made or position through all publications, interviews and related communication does not necessarily reflect the mission, objective and works and official opinions of Strategy International (SI) Ltd.

The document produced is endorsed, is its scientific value, and credits are provided to the author.

The editorial Team of
Strategy International (SI) Ltd.

Marios P. Efthymiopoulos (PhD) (CEO)
Josef Demergis (PhD) (Director of Research & Analysis)

Marketing Team: Rebel Online

Intelligence in the Modern Era: Strategic Shifts, Cultural Dynamics, and Technological Advances

Editors

Dr. Frederic Lemieux

Dr. Shadi Abouzeid

Dr. Shay Hershkovitz

Executive Summary 5
Panel Reports 7
Panel 1 – Strategic Surprises and Decision-Making 7
Panel 2 – Intelligence Culture(s) 10
Panel 3 – Voices in Intelligence 13
Panel 4A – AI in Intelligence Research 16
Panel 4B – Open Source Intelligence (OSINT) 22

Executive Summary

The May 2025 Intelligence in the Modern Era conference was convened to critically assess how intelligence organizations are adapting, or failing to adapt, to the converging challenges of geopolitical instability, cultural transformation, and technological disruption. Held in Washington, D.C., this one-day event brought together thought leaders, intelligence practitioners, and scholars for a series of thematic panels that focused on dissecting past failures, examining institutional cultures, exploring emerging technologies, and reimagining the boundaries of intelligence itself. The purpose of the conference was not only to reflect on the changing landscape of intelligence work but also to provide forward-looking strategies that inform practice, research, and policy design.

Throughout five core sessions, the conference revealed that strategic surprise continues to pose a persistent risk in the intelligence field, not due to a lack of information, but because of ongoing structural, cognitive, and cultural shortcomings. Panelists highlighted examples ranging from the October 7th attack in Israel to long-term systemic blind spots preceding the 2008 financial crisis and the Arab Spring. These episodes uncovered a pattern: intelligence failures often result not from ignorance, but from misinterpretation, rigid frameworks, politicization, and failures of imagination. In particular, deeply entrenched cognitive heuristics, such as confirmation bias, status quo thinking, and mirror imaging, consistently distort threat assessments. Organizational dysfunctions, including information silos, a lack of analytic pluralism, and top-down suppression of dissent exacerbate these issues. The conference emphasized that strategic surprise is frequently the cumulative result of systems unable to process complexity, rather than a product of unforeseeable events.

The culture within intelligence institutions emerged as a second critical theme. Panelists explored how internal dynamics, particularly the erosion of a "challenge culture," can either make or break an organization's ability to think critically. Without institutional mechanisms to foster dissent and diversity of perspective, intelligence assessments become vulnerable to conformity, overconfidence, and political pressure. Structured analytic techniques, red teaming, pluralistic analysis units, and leadership models that encourage epistemic humility were all cited as necessary safeguards. Case studies of institutional transformation, such as the evolution of Israeli Defense Intelligence from a strategic early warning function to an operational targeting unit, illustrated both the gains and losses associated with an overemphasis on real-time tactical intelligence at the expense of long-term foresight.

One of the most compelling insights was the repositioning of diversity as a strategic, not symbolic, imperative. Conference discussions emphasized that a lack of diversity within analytic teams results in systemic blind spots, underexplored threat vectors, and a failure to interpret signals from adversaries. Moving beyond traditional metrics, panelists argued that diversity should be measured by its outcomes, such as improved threat identification, analytical creativity, and mission success, rather than solely by demographic representation. Challenges in recruitment, retention, and promotion persist across gender and minority lines, with the security clearance process and rigid workforce expectations often cited as barriers. Addressing these gaps, participants

suggested, requires institutional reform and early-career investment through mentorship and outreach.

Technology, particularly Artificial Intelligence, is both an asset and a risk. Panels examined how large language models (LLMs) can help detect cognitive heuristics, accelerate hypothesis generation, and process vast amounts of information. While AI can serve as a "contextual prosthetic" to human reasoning, enabling younger or less experienced analysts to think divergently, it is also clear that, without careful oversight, AI systems can reflect or amplify existing heuristics, produce misleading outputs, and be vulnerable to data poisoning. The consensus is that AI should enhance, not replace, human analytic judgment, and responsible integration must include transparency, model explainability, and strong human-in-the-loop governance. The final sessions addressed the expanding role of Open Source Intelligence (OSINT) and the need to reconceptualize the intelligence ecosystem. Intelligence is no longer the exclusive domain of classified sources and government agencies. Civilian-led investigations, real-time open-source data, and collaborative information networks are now central actors in producing actionable knowledge. This transformation challenges traditional notions of legitimacy and control but also presents an opportunity: to build a more inclusive, transparent, and adaptive intelligence paradigm that values both institutional and civic expertise.

The strategic takeaways from the conference were clear. For policymakers, the event underscored the importance of investing in institutional reform, safeguarding analytical independence, and cultivating cultures that reward dissent rather than compliance. For intelligence professionals, the lessons were practical: structured analytic methods, diverse team composition, ethical AI usage, and critical review processes are now essential to mitigate risk and maintain relevance. For scholars and educators, the sessions highlighted new research frontiers at the intersection of culture, cognition, and technology in intelligence work, as well as a pedagogical responsibility to prepare the next generation of analysts not only to process information but also to question, imagine, and challenge it.

Ultimately, the *Intelligence in the Modern Era* conference concluded with a clear message: the future of intelligence will not be shaped by better algorithms or faster networks alone. It will depend on the collective willingness to rethink inherited assumptions, reimagine institutional practices, and recalibrate what it means to know in an age where complexity, uncertainty, and surprise are the new constants.

Panel Reports

The conference consisted of five panels, three of which were presented in sequence, while two were presented in parallel. For each panel, the main themes and key takeaways were summarized based on the panelists' individual presentations and the ensuing discussions, which included questions from both the moderator and the audience.

Panel 1 – Strategic Surprises and Decision-Making

Contributors: Mr. Rohin Sharma (moderator), Dr. Frederic Lemieux (speaker), and retired Colonel Yossi Kuperwasser (speaker).

Strategic surprises are unforeseen developments that significantly alter the trajectory of events and disrupt prevailing assumptions or frameworks. These occurrences, which often yield transformative consequences, are closely tied to intelligence failures and the misinterpretation or neglect of critical signals. Some surprises manifest as singular, concentrated events, such as a sudden attack or collapse, while others unfold incrementally over time. Though frequently described as "black swans," suggesting complete unpredictability, a more accurate characterization holds that the relevant information is often available but overlooked due to internal limitations and dysfunctions within intelligence systems, rather than the inherent unpredictability of the events themselves.

The causes of intelligence failures that lead to strategic surprises are multifaceted and often involve an intricate combination of psychological, organizational, technological, and political factors. At the cognitive level, human biases remain one of the most persistent obstacles to sound judgment in intelligence analysis. Analysts may underestimate or overestimate the capabilities and intentions of adversaries, resulting in either unpreparedness or misallocated resources. A particularly salient bias is the availability heuristic, wherein analysts give undue weight to information that is easily recalled or recently encountered, often at the expense of a more comprehensive dataset. Anchoring bias compounds this problem by encouraging overreliance on the first piece of information received, thereby skewing subsequent analysis.

Confirmation bias, arguably the most corrosive of all, leads analysts to seek information that affirms existing beliefs while dismissing disconfirming evidence. In extreme cases, this bias can be so entrenched that analysts disregard disturbing but accurate data, even when clear indications of adversarial intent exist. Mirror imaging, the assumption that others think and behave as we do, and a failure of imagination, the inability to conceive of novel threats, further limit analysts' foresight. Additional psychological pitfalls include status quo bias, which fosters resistance to recognizing change; groupthink, which elevates consensus over critical scrutiny; authority bias, which places excessive trust in the views of superiors; conservatism bias, which inhibits belief revision despite new evidence; the sunk cost fallacy, which perpetuates flawed commitments; and a general tendency to discount dissenting opinions.

Beyond individual cognition, institutional structures themselves often harbor pathologies that compromise intelligence efficacy. These include systemic inefficiencies such as the digital divide, redundant systems, information silos, and the hoarding of intelligence, all of which obstruct the seamless sharing and synthesis of information. Organizational friction and information overload further exacerbate this situation. Other persistent structural

dysfunctions include the failure to report or record information adequately, gaps driven by occupational subcultures, and disjointed responsibility across agencies, which obscures accountability for the broader intelligence picture.

Compounding these issues are deficits in organizational memory, where critical knowledge or historical adversary strategies are forgotten or ignored. Rigid hierarchies discourage dissent from lower-ranking personnel, and a lack of personnel diversity curtails the breadth of perspectives necessary to understand adversaries whose cultural and strategic worldviews may differ significantly from those of analysts.

The effectiveness of intelligence collection also suffers from overreliance on specific technological methods, such as signals intelligence and cyber operations, at the expense of equally vital sources such as open-source intelligence, human intelligence, and tactical field reporting. When agencies presume dominance in intelligence capabilities, a false sense of security may emerge, blinding them to warning signs and critical vulnerabilities.

Dissemination failures can be equally damaging. Even when relevant intelligence is collected and analyzed, it must be communicated clearly and promptly to decision-makers. Too often, this process breaks down. Analysts may fail to frame plausible reference scenarios that contextualize potential threats. Critical early warnings may not be issued in a timely or sufficiently alarming manner. In some cases, decision-makers are not adequately alerted during crucial nighttime hours. Compounding these failures is the problem of false alarms, strategic warnings issued in preceding months that, when unfulfilled, erode the credibility of subsequent alerts. Furthermore, procedural best practices, such as the maxim “if there is doubt, there is no doubt” (which emphasizes caution in the face of ambiguity) or the imperative to awaken sleeping decision-makers during crises, are too often ignored.

Political interference can further erode the integrity of intelligence analysis. Politicization occurs in multiple forms. Bottom-up politicization happens when analysts tailor their findings to influence or align with perceived policy preferences. Top-down politicization results from direct pressure by political leaders to distort or suppress threat assessments. Lateral politicization, perhaps subtler, occurs when agencies pressure one another to maintain interagency consensus, even at the expense of analytical accuracy. Collectively, these forces compromise analytic integrity and increase susceptibility to misjudgements. The growing involvement of private sector intelligence providers, who may cater to client interests, adds another layer of distortion. Internal political turmoil and shifting national priorities can further distract from accurate threat perception and response.

In addition to internal challenges, the broader geopolitical environment introduces further complexity. Global volatility and structural ambiguity—fuelled by shifting alliances, regional rivalries, ideological contestation, and disruptions in energy and supply chains—create fertile conditions for miscalculation and misperception. Climate change and environmental degradation compound these challenges, adding urgency to complex adaptive responses. Meanwhile, emerging strategic frontiers such as cyberspace and outer space introduce novel threats. The inherent ambiguity and deniability of cyber operations, combined with the proliferation of artificial intelligence, quantum computing, and disinformation, blur the boundaries between civilian and military domains. The erosion of global deterrence norms in this context constitutes a strategic surprise in the making.

To increase resilience and mitigate the impacts of future surprises, intelligence institutions must undertake comprehensive reform. Rethinking organizational structures is paramount. This could include separating long-term strategic analysis from tactical military intelligence or consolidating disparate agencies into a cohesive and truly integrative intelligence community. The aim is to achieve a panoramic view of emerging risks and adversary behavior.

Equally important is fostering a culture of self-critique and iterative learning. Intelligence review processes should compel analysts to articulate doubts and intuitions, those "butterflies in the belly", that often signal analytical discomfort. Tools such as devil's advocacy, plural analysis from competing teams, and mechanisms for formally submitting dissenting views must be employed rigorously and made visible at senior decision-making levels.

Technological innovation also offers promise. Artificial intelligence can assist in detecting weak signals, modelling potential futures, and correcting cognitive biases in real time. While AI remains vulnerable to biases embedded in training data, its capacity to process massive volumes of information and flag inconsistencies provides a powerful tool for enhancing situational awareness. Moreover, the so-called "hallucinations" of generative AI may, paradoxically, offer imaginative alternatives worth exploring further.

A renewed focus on the principles of early warning is also required. Revisiting foundational analytic techniques and emphasizing structured, methodical approaches to forecasting can reduce the recurrence of past mistakes. Enhancing diversity in both personnel and analytic approach is another critical reform. Recruitment and promotion should prioritize inclusivity, with deliberate efforts to bring in individuals from diverse backgrounds, including women and underrepresented communities. Diversity is not merely a moral imperative; it is an operational necessity for understanding the strategic logic and cultural nuances of adversaries.

Unconventional talent should also be welcomed. Artists, with their capacity for divergent thinking, emotional intelligence, and subtle perception, may offer valuable insights into adversary intent and societal trends. Cultivating an institutional culture that values open criticism and rejects arrogance or fear in expressing dissent is essential to maintaining epistemic integrity. Simultaneously, intelligence must remain politically neutral, detached from partisan influence, and grounded in objectivity to preserve credibility and enable strategic foresight.

Collection strategies must strike a balance between technological dominance and more traditional, human-centered methods. This requires the integration of open-source and human intelligence into the broader collection apparatus to ensure that no single mode of analysis becomes over-relied upon. Strengthening interagency cooperation and ensuring policymakers receive timely, relevant, and accurate assessments is vital for responsive and informed decision-making.

In sum, while strategic surprises are an enduring feature of complex systems and international relations, intelligence failures need not be. By reforming structures, embracing technological augmentation, and cultivating a culture of epistemic humility and adaptive learning, the intelligence community can not only reduce the likelihood of surprise but also strengthen its capacity to absorb shocks and respond with agility. The goal should not be perfect foresight,

but rather, resilience: the ability to detect, interpret, and act decisively in the face of the unexpected.

Panel 2 – Intelligence Culture(s)

Contributor: Dr. Shadi Abouzeid (moderator), Dr. Barry Zulauf (speaker), and Dr. Ofer Guterman (speaker).

The panel discussion titled *"Culture in Intelligence"* examined the often-neglected but deeply consequential role that culture plays within intelligence institutions. Far from being a peripheral concern, culture was positioned as a central force shaping how intelligence is produced, how it is communicated, and how it influences national security decisions. The discussion drew particular attention to how institutional norms, behaviours, and values underpin both successes and failures in intelligence work, particularly in the context of recent strategic surprises.

The panel began by asserting the primacy of culture in shaping intelligence organizations. Culture, more than individual personalities or formal processes, defines how professionals in the field approach their work, how they interact with decision-makers, and how they make sense of complex environments. Despite its importance, culture remains one of the least interrogated elements in intelligence studies and practice. The speakers emphasized that a healthy intelligence culture requires more than technical proficiency or advanced tools; it demands values, habits, and norms that promote open inquiry, disciplined skepticism, and intellectual independence.

Central to democratic intelligence is the commitment to objective and balanced analysis. Intelligence professionals are not tasked with supporting policy preferences or desired outcomes but rather with presenting "unvarnished" truths to decision-makers. The sovereign is under no obligation to act on intelligence, but a moral obligation exists to listen. The panel underscored that this impartial role is not merely aspirational; it is foundational to the ethical and functional integrity of intelligence in democratic systems.

A recurrent theme throughout the discussion was the need to cultivate a "challenge culture", an environment where dissent is not only tolerated but actively encouraged. Encouraging alternative perspectives helps guard against blind spots and strategic failures. Leaders must model receptiveness to dissent, while institutional mechanisms, such as red teams or structured "Team A/Team B" exercises, should be institutionalized to promote rigorous alternative analysis. Reward structures and professional training should teach when and how to challenge dominant assumptions using structured analytic techniques, thereby embedding dissent into the core practice of intelligence.

This cultural ethos must also be matched by personal integrity. Intelligence analysts must possess the courage to speak truth to power, even at considerable professional or personal cost. The commitment to objective reality, backed by what one panelist called "bulletproof tradecraft", is indispensable in moments when truths may be politically inconvenient. Legal frameworks such as the U.S. Intelligence Reform and Terrorism Prevention Act (IRTPA) reinforce this commitment by mandating the provision of politically neutral analysis. One panelist even recounted being willing to resign rather than compromise analytical integrity

during a politicized presidential election cycle. Such examples underscore the stakes involved and the personal courage demanded by ethical intelligence work.

Politicization of intelligence was identified as one of the most corrosive risks facing intelligence communities. When intelligence is shaped to align with policy preferences, whether through top-down directives, bottom-up accommodation, or lateral pressures within and across agencies, it produces a chilling effect. Analysts become reticent to express minority views, and objectivity gives way to consensus-driven conformity. Over time, this diminishes the institution's strategic relevance and corrodes public trust.

To safeguard objectivity, the panel argued for a disciplined separation between "thinkers" and "doers." Analysts (the "thinkers") are responsible for understanding reality, including adversary capabilities and intentions, and for critically evaluating one's own side. Decision-makers and operators (the "doers") act within that reality. At the highest strategic levels, this separation is vital to prevent the contamination of analysis by operational interests or political pressures. However, the panel acknowledged that at more tactical or operational levels, such as in kinetic targeting, embedding intelligence within operational units can yield efficiency and precision. Thus, while the separation is essential at some levels, the appropriate balance remains context-dependent.

The conversation also explored the growing risks posed by the over-operationalization of intelligence and excessive reliance on new technologies. As intelligence agencies increasingly invest in cyber capabilities, big data analytics, and artificial intelligence, the strategic function of intelligence, the ability to contextualize, anticipate, and explain adversary behavior—, risks being marginalized. Policymakers may come to favor intelligence organizations that prioritize direct action and compliance over those that ask uncomfortable questions or present inconvenient truths. The panel warned that this shift, especially in high-pressure political environments, can erode the reflective and anticipatory functions that strategic intelligence must uphold.

Effective communication of uncertainty was highlighted as another cultural competency of strategic importance. Intelligence professionals must resist the temptation to offer artificial precision, such as numeric probabilities, that may mislead or confuse. Instead, they should communicate clearly what is known, what is unknown, and what assumptions underpin their judgments. Using more accessible terms like "likely" or "unlikely," especially for non-technical audiences, preserves nuance while avoiding the illusion of certainty. This clarity is particularly vital when presenting intelligence to decision-makers unfamiliar with probabilistic reasoning.

The panel also encouraged new intelligence professionals to learn to read the culture of their organizations by observing leadership behaviors in meetings. Do leaders invite alternative perspectives, or do they present their assessments as settled facts? Do they reward truth-seeking or deference to hierarchy? These behavioral cues offer insights into the true values of an organization. Mentorship from experienced analysts who embody critical thinking and ethical integrity was emphasized as a key factor in nurturing a culture of excellence and resilience.

The transformation of Israeli Defense Intelligence (AMAN) offered a powerful case study illustrating how cultural and strategic priorities within an intelligence organization can evolve,

and the consequences of such transformations. From the 1950s through the 1980s, AMAN's central mission was strategic early warning of conventional war. Failures such as the 1973 Yom Kippur War led to a strengthening, not weakening, of this mandate. After the 1979 peace treaty with Egypt, AMAN redirected its focus to Syria, but early warning remained foundational to Israel's security doctrine.

However, the 1990s marked a turning point. The end of the Cold War, the Gulf War, and the diminishing threat of conventional warfare coincided with the rise of asymmetric threats from non-state actors and shifting regional dynamics. Peace processes and the increasing complexity of conflict environments led AMAN to question the continued relevance of strategic early warning. By 1998, an internal AMAN document declared that early warning was losing its explanatory and budgetary appeal, and was likely to drop from the IDF's top priorities within the following decade.

This projection proved prescient. By 2003, a fundamental organizational transformation was underway. With a diminished threat of conventional Syrian aggression, the IDF directed AMAN to shift its emphasis toward operational intelligence, particularly in the realm of targeting. New doctrinal concepts such as "intelligence campaigns" and "operational intelligence" gained traction. In the aftermath of the 2006 Second Lebanon War, AMAN formally assumed a more active role as an operational arm of the IDF by 2007, complete with its own Operations Division.

Between 2010 and 2014, under the leadership of a new head, AMAN deepened this shift. It focused increasingly on offensive capabilities, including cyber operations, and constructed what it termed a "targets factory", a technologically driven apparatus leveraging big data and AI to support real-time battlefield engagement. The 2015 IDF strategy codified this orientation by introducing the doctrine of "intelligence supremacy," thereby displacing strategic early warning as AMAN's primary mission. By 2021, top military officials, including the Chief of Staff and the Deputy Commander of Unit 8200, publicly articulated this transformation: AMAN was no longer simply an observer and assessor of adversaries, but an operational participant, providing tactical intelligence, generating actionable targets, and shaping the battlefield.

By October 7, 2023, this transformation was complete. The "Old AMAN," an organization committed to national assessments and early warning, had become the "New AMAN", a tech-operational intelligence agency engaged in daily tactical operations aimed at shaping adversarial behavior. This transition was driven by changes in doctrine, leadership vision, technological opportunity, and budgetary considerations. Yet the Hamas attack on October 7th raised troubling questions. Despite AMAN's operational successes and its sophisticated intelligence machinery, it failed to provide strategic early warning of a significant adversarial action.

In light of this failure, the panel concluded by posing several pressing questions about AMAN's future trajectory. Will the organization continue to prioritize operational innovation, or will it reinvest in strategic foresight and national-level assessments? How will resources be balanced between these competing imperatives? Will AMAN reestablish a cadre of long-term subject-matter experts, or continue with its fast-moving, command-oriented career model? What values, intellectual humility and critical inquiry, or operational focus and mission execution, will define its institutional identity? Finally, what incentive structures will shape the next

generation of intelligence professionals: those that reward analytical depth and internal challenge, or those that promote tactical creativity and real-time execution?

These questions highlight a complex web of strategic tensions now confronting AMAN. They also offer a broader reflection on the critical role of culture in shaping intelligence performance. Whether an intelligence organization leans toward strategic anticipation or operational engagement, the foundational issues remain the same: the integrity of analysis, the courage to speak truth to power, the cultivation of dissent, and the clarity of institutional purpose. Without attending to these cultural foundations, even the most technologically advanced intelligence systems may fail when it matters most.

Panel 3 – Voices in Intelligence

Contributors: Dr. Shadi Abouzeid (moderator), Dr. Rhian McCoy (speaker), and Ms. Shira Baribay-Shaham (speaker).

The effectiveness of intelligence communities (ICs) hinges not only on technical capability or access to classified data but, critically, on their ability to assess complex, dynamic threats and respond with agility and insight. Among the most consequential factors shaping this capability is diversity—not merely as a demographic benchmark but as a cognitive and strategic asset. A growing body of research and practitioner reflection underscores that diversity of thought, background, and perspective is essential for the IC to achieve its mission, mitigate analytic blind spots, and avoid strategic failures. This chapter explores the strategic imperative of diversity in intelligence, the persistent institutional challenges that inhibit its realization, and the necessary reforms to foster a more inclusive, resilient, and effective intelligence apparatus.

Diversity in the IC must be understood not simply as a matter of equity or representation but as a mission-critical function. Homogeneity in analytic environments fosters groupthink, narrows the scope of threat identification, and increases vulnerability to surprise. The 9/11 attacks remain an enduring case in point: a failure of imagination deeply rooted in a culturally and cognitively homogeneous intelligence workforce. Analysts, sharing similar educational and professional profiles, failed to anticipate non-traditional threats. In contrast, deeper linguistic and cultural knowledge, often found among members of heritage communities, was both available and underutilized. This failure underscored a longstanding structural limitation: the IC's inability to leverage the full spectrum of knowledge and lived experience available within and outside its walls.

Five core benefits highlight why diversity is indispensable to the intelligence mission. First, it enhances mission success by broadening the range of perspectives available to understand multifaceted, ambiguous environments. Second, it improves global threat assessment through culturally informed insights that can illuminate local dynamics otherwise obscured to a monocultural lens. Third, it fosters innovation and creative problem-solving—diverse teams consistently outperform homogeneous ones, especially when tasked with complex, open-ended problems. Creativity, as discussed in the panel, is not a talent but a discipline; and that discipline requires cognitive friction, disagreement, and a multiplicity of frameworks. Fourth, diversity fills critical skill gaps in areas such as language proficiency, social norms, and regional expertise, capabilities often absent in more traditional recruitment pools. Fifth, a diverse

workforce enhances public trust and legitimacy. When intelligence organizations reflect the constituencies they serve, their assessments gain credibility and public support, especially in democratic societies.

However, despite these recognized benefits, substantial barriers prevent the intelligence community from fully realizing the potential of diversity. One of the most significant is the flawed emphasis on outputs rather than outcomes. Efforts to increase diversity frequently measure progress in terms of hiring quotas or demographic representation without assessing the real-world impact of such diversity on analytic performance, decision-making quality, or strategic foresight. This output-driven model risks reducing diversity to a performative exercise, a box to be checked, rather than a substantive transformation of institutional behavior and epistemology. As one comparative example highlighted, the pharmaceutical firm AstraZeneca may employ a high percentage of women, but its focus lies in assessing whether this representation improves innovation and performance. Intelligence agencies must adopt a similar shift: from representation to effectiveness.

Retention of diverse talent remains another acute challenge. Minority personnel and women frequently exit intelligence agencies within the first year at disproportionate rates. For women, career progression is often constrained by structural impediments such as the security clearance process, limited re-entry pathways after career interruptions (e.g., maternity leave), and now, post-pandemic return-to-office mandates that disproportionately disadvantage women and individuals with disabilities. These structural frictions perpetuate the very homogeneity that the IC purports to redress.

A further and subtler challenge lies in the phenomenon of “unthinkability.” Some threats remain outside the analytic repertoire not because they are implausible, but because institutional, cultural, or epistemic filters exclude them from legitimate discourse. Unthinkability operates along two dimensions: empirical availability, what is considered even thinkable based on existing knowledge and imagination, normative acceptability; what is permissible to articulate within professional settings without being questioned for one’s loyalty, competence, or sanity. This results in the exclusion of entire categories of risk.

Multiple factors contribute to the persistence of unthinkability. Epistemic gaps, such as the failure to recognize or integrate data on conflict-related sexual violence, demonstrate the limits of institutional knowledge. Cognitive heuristics reinforce entrenched assumptions about adversary behavior, particularly when informed by notions of deterrence or presumed rationality. Cultural blind spots, especially gendered assumptions about conflict or civilian vulnerability, obscure relevant indicators. Conceptual rigidity, in which “real warfare” is narrowly defined to exclude threats that do not involve kinetic force, further reinforces analytical myopia. Organizational silencing, whether through taboo, lack of vocabulary, or fear of reputational damage, compounds these constraints. Analysts may observe worrisome developments, such as shifts in adversary rhetoric or sociopolitical resolve, yet hesitate to raise alarms if those observations fall outside accepted frameworks. A striking example involved the refusal to publish a scenario invoking “space invaders” for fear of public backlash, a metaphorical illustration of how dominant discourses delimit analytical range and suppress imaginative foresight.

To mitigate these institutional and cognitive obstacles, the IC must pursue a deliberate and multi-pronged strategy. First, it must reframe how it evaluates diversity by shifting from outputs to outcomes. Rather than counting hires and promotions, agencies should assess how diverse teams contribute to better analysis, anticipate threats, or identify blind spots that more homogenous teams may miss. Evaluation metrics must align with mission outcomes, strategic success, analytic rigor, and resilience, not bureaucratic compliance.

Second, intelligence agencies must institutionalize systematic learning from failure. When strategic misjudgments occur, post-mortem analyses should explicitly examine whether insufficient diversity of thought or the marginalization of dissenting voices contributed to the error. This learning process should be structured and iterative, incorporating analytic lessons learned in a manner akin to project management cycles. It should also include reflections on how heuristics, organizational pressures, and unexamined assumptions shaped outcomes.

Third, a culture of dissent and constructive disagreement must be actively cultivated. Disagreement should not be pathologized as disorder but embraced as a productive source of innovation. Structured analytic techniques, such as red teaming, alternative futures, or mind mapping, can provide the necessary scaffolding for divergent thinking. Leaders must model openness to critique and create formal pathways for the expression of dissent. Diversity of opinion cannot thrive without institutional protection and reward.

Fourth, proactive recruitment and sustained mentorship are essential for fostering a pipeline of diverse intelligence professionals. Early engagement, such as with Girl Scouts or ROTC programs, can encourage underrepresented groups to envision themselves in intelligence careers. Mentorship by senior leaders and networks of peer support are crucial to help diverse candidates navigate opaque or inhospitable professional environments. Retention depends not only on entry but on progression, belonging, and affirmation.

Fifth, the security clearance process must be reevaluated. The current system often operates as a gatekeeping mechanism that disproportionately disadvantages those from non-traditional backgrounds, first-generation Americans, individuals with global family ties, or those who have lived abroad. While security concerns are legitimate, they must be balanced with the strategic necessity of linguistic, cultural, and experiential diversity. A shift in mindset is needed: clearances should be seen not as barriers but as tools to enable access to critical expertise. Assigning lower-level clearances to personnel with rare and necessary skills may offer a pragmatic compromise.

Sixth, fostering empathy and bias awareness across the workforce is vital. Analysts and leaders alike must be trained to recognize their own cognitive and cultural biases and to develop the intellectual humility necessary to revise beliefs in light of new evidence. Empathy, seeing the world through another's lens, enables analysts to anticipate threats that emerge from unfamiliar or marginalized contexts.

Looking ahead, the IC, particularly in the United States, stands at a strategic crossroads. There is growing concern that without renewed commitment, existing diversity efforts may erode, necessitating a painful and costly rebuilding of lost capability. A projected reduction in personnel, including foreign language experts and women, signals both a challenge and an

opportunity: the chance to intentionally reconstruct a workforce that reflects the pluralism, resilience, and adaptability required for twenty-first century intelligence work.

To preserve integrity and prevent politicization, especially within democratic societies, ICs must resist instrumentalizing diversity as a public relations goal and instead embed it within their strategic core. As global threats grow more complex, distributed, and unpredictable, intelligence organizations will only remain effective if they are cognitively and culturally equipped to engage with the full spectrum of risk. That demands leadership that seeks out divergent voices, analysts who dare to question, and institutional cultures that regard diversity not as a threat to cohesion but as the foundation of strategic insight.

Ultimately, the transformation of diversity from a metric to a mindset, from numbers to outcomes, will determine whether intelligence communities can remain anticipatory rather than reactive, resilient rather than brittle, and inclusive rather than insular. The stakes are not only institutional performance but national security itself.

Panel 4A – AI in Intelligence Research

Contributors: Dr. Shay Hershkovitz (moderator), Dr. Frederic Lemieux (speaker), Ms. Nicole Washington (speaker), and Dr. Monica Robbins (speaker).

The Integration of Artificial Intelligence in Enhancing Intelligence Analysis: Addressing Cognitive Heuristics and Operational Efficiencies

This panel discussed research on the application of Artificial Intelligence (AI), specifically Large Language Models (LLMs), to enhance intelligence analysis. It focuses on the critical role AI can play in identifying and mitigating human cognitive heuristics, improving hypothesis generation, and streamlining analytical processes. Drawing on insights from a joint academic and industry project, this paper outlines the methodological approach to developing AI-powered heuristic detection tools, discusses the broader benefits and challenges of integrating LLMs into intelligence work, and explores the significant ethical considerations and future developmental pathways for AI in national security. The overarching theme emphasizes a pragmatic approach to human-machine collaboration, leveraging AI to enhance, rather than replace, human analytical judgment.

The Imperative for AI in Intelligence Analysis

Intelligence analysis is a cornerstone of national security, requiring rigorous and objective judgment to inform critical decision-making. However, human analysts are inherently susceptible to cognitive heuristics, which are systematic errors in thinking that undermine analytical judgment and lead to flawed conclusions. The modern intelligence landscape is further complicated by an overwhelming volume of information and the challenge of quickly processing it. Traditional analytical methods are often insufficient to cope with this "information overload" and the unprecedented pace of information flow. This environment necessitates the rapid integration of intelligent automation to enhance analytical capabilities and address these existential threats.

A key area of innovation involves developing AI-powered applications capable of identifying and addressing these pervasive human cognitive heuristics, thereby enhancing the objectivity and reliability of intelligence products. This integration aims not to replace human analysts but to free them to focus on more strategic and complex problem-solving activities by automating routine or computationally intensive tasks. This paper will delve into the methodologies for AI-driven heuristic detection, the broader implications of LLM adoption in intelligence, and the crucial ethical considerations that accompany such technological advancements.

The Pervasive Problem of Cognitive Heuristics

Cognitive heuristics represent a major challenge in intelligence analysis, frequently leading to intelligence failures. These heuristics are ingrained patterns of thought that can distort perception and interpretation of information. The presenters identified six major cognitive heuristics that repeatedly contribute to analytical shortcomings:

- Hidden Assumption: This occurs when an assumption is made but not explicitly stated or supported by evidence. Detecting this can be particularly subtle, even for the person writing or proofreading a document.

- Straw Man Fallacy: This involves misrepresenting or oversimplifying an opponent's argument to make it easier to attack or refute. This type of fallacy often follows a clear pattern of an original argument being distorted, attacked, and then implicitly refuted.

- Confirmation Bias: A tendency to seek, interpret, favor, and recall information that confirms one's preexisting beliefs or hypotheses. This can lead to "cherry-picking" data.

- False Causality: Assumes a causal relationship between two events simply because one follows the other. Like the Straw Man Fallacy, this heuristic often uses an obvious pattern.

- Mirror Imaging: Assumes that other actors will react in the same way as one's own group, projecting one's own values and cultural norms onto an adversary. This is another subtle bias, difficult to detect.

- Circular Reasoning: Uses a conclusion to support an assumption that was necessary to reach that conclusion.

These heuristics, ranging from subtle to obvious, are critical to address because they undermine the objectivity vital for accurate intelligence judgments.

AI-Powered Solutions for Heuristics Detection

A research project was undertaken to develop an AI-powered application specifically designed to identify and address human cognitive biases. The application aims to eliminate bias in various forms of communication, providing suggestions for rephrasing statements.

Prompt Methodology and Training

The core of this AI application lies in its ability to detect specific heuristic patterns or sequences. For each cognitive heuristic, a formal structure or "formula" was developed to represent its typical pattern. For instance, the Straw Man Fallacy is characterized by an original argument (OA) from Person 1, a misrepresented argument (MA) created by Person 2, an attack on the misrepresentation (AM), and an implied refutation (IR) of the original argument. Similarly, False Causality is identified by Event A (EA) preceding Event B (EB), followed by an assumed causation that EA caused EB. The AI model was trained using a "human-in-the-loop" approach. Human annotators, including a small group of students, manually identified these fallacies in massive amounts of text from diverse sources. This human labeling served as the initial training data for the LLM, instructing it on what constitutes a specific heuristic. After the initial training, humans continued to evaluate the model's detections for correctness, ensuring continuous refinement and verification. While manual annotation was a luxury afforded by the academic setting, it was noted that in corporate environments, AI itself is often used for labeling training data, highlighting the human-in-the-loop for the initial training process.

Data Diversity and Balance

To ensure the robustness and fairness of the AI model, a wide diversity of data sources were utilized, categorized by their level of moderation. This included:

- High-moderation sources: Think tank reports, academic papers, and policy briefs that undergo thorough review by experts, peers, or institutions (e.g., peer review), increasing their credibility and trustworthiness.

- Medium-moderation sources: Newspaper articles and podcast transcripts, which have some editorial review but may still contain heuristics.

- Low-moderation sources: Politicians' speeches, social media posts, and personal blogs, which undergo little to no review and are often based on personal opinions.

This diverse dataset, including both refined and subtle heuristics, allowed the model to develop a comprehensive understanding of how biases manifest across various communication styles.

Crucially, balanced data input was emphasized to ensure fairness in detection. Human annotators actively included heuristic from both sides of controversial topics such as gun control, abortion, and climate change. The goal was to train the model to identify flaws in argumentation regardless of the ideological stance, rather than becoming a "truth finder" that validates or invalidates specific positions. This comprehensive heuristic representation across the ideological spectrum fosters a more objective dataset for training the AI.

Results and Model Performance

The results demonstrated the effectiveness of the trained AI model. Using the Mixtral 7x8B model, the researchers achieved almost perfect scores in detecting heuristics when properly trained and provided with engineered prompts incorporating the heuristic formulas. This

significantly outperformed untrained models or other LLMs (like Llama 3 70B) given vanilla prompts, highlighting the importance of both targeted training and well-formulated prompts. The model can now search for all six targeted heuristics simultaneously within a given text. When a heuristic is detected, the system flags it, identifies the specific pattern, and highlights the relevant part of the text, explaining *why* it believes a heuristic is present. This transparency allows the human user to decide whether to dismiss the flag or correct the identified heuristic for a more balanced analysis.

LLMs in Intelligence Analysis: Benefits and Challenges

Beyond specific heuristic detection, LLMs offer broader applications and benefits for intelligence analysis, particularly in areas where human cognition is limited.

Enhancing Divergent Thinking and Hypothesis Generation

A key benefit of LLMs in intelligence analysis is their ability to act as "contextual prosthetics for divergent thinking". Intelligence analysts are often limited by their own imaginations and experiences when generating hypotheses, especially new analysts who lack deep subject matter expertise. This cognitive process, called "flexible recombination," involves rattling around memories, knowledge, and experiences to form new ideas. LLMs, designed to recombine information statistically, can serve as a valuable tool here. With access to billions of documents, LLMs can rapidly organize and calculate meaning based on patterns and probabilities of words in text, effectively "plus-ing up context" for analysts.

Benefits include time savings and functioning as a virtual brainstorming partner, especially for analysts who may not have access to panels of experts or colleagues for discussion. This makes LLMs a relatively low-risk solution for getting started with hypothesis generation, overcoming initial cognitive hurdles and epistemic gaps.

Downsides and Risk Mitigation

Despite the benefits, LLMs also present downsides. They lack grounded understanding and deep subject matter expertise, and their performance is limited by the quality of their training data ("garbage in, garbage out"). Risks include LLM poisoning, where models are trained on disinformation, which can lead to biased or incorrect outputs. However, the existing analytic process itself acts as a crucial mitigation for these risks. The analytical process is designed to thoroughly and rigorously examine each hypothesis, regardless of its source. If an LLM "hallucinates" or provides incorrect information, the subsequent human-led verification and elimination phases are intended to catch such errors. This human-machine teaming approach significantly reduces the risks associated with LLM-assisted ideation. The ability to follow the LLM's logic and source its information, as demonstrated by platforms like Perplexity AI, further enhances transparency and accountability, allowing analysts to evaluate the generated insights critically.

Ethical Considerations and Challenges

The integration of AI into intelligence analysis raises significant ethical questions, particularly regarding critical thinking, data integrity, and the very nature of human-machine collaboration in high-stakes environments.

Impact on Critical Thinking

A primary concern is whether LLMs might weaken human critical thinking. However, this can be reframed as an opportunity for enhanced learning and cognitive development. Instructors can design exercises where students first grapple with a problem independently, experiencing "psychological discomfort" due to context limitations, before consulting an LLM. The subsequent comparison between their own thoughts and the LLM's output creates a "splendid opportunity for teaching" about cognitive flexibility and divergent thinking. Critical thinking is most vital in the "convergent phase" of analysis, where analysts evaluate and eliminate hypotheses to arrive at the best answer, rather than solely in the initial "divergent phase" of idea generation. The objective is to utilize LLMs as a "contextual prosthetic" to empower analysts to think divergently on their own.

Responsible Automation and Data Integrity

The responsible automation of intelligence work involves mirroring what the analyst does and rigorously testing the AI's accuracy. The challenge lies in automating large chunks of intelligence work ethically, particularly when dealing with "matters of life". However, it was noted that machines are already deeply embedded in intelligence processes, providing data and influencing analysis, and the risk of adversarial manipulation of data is already present regardless of AI. The key is to enhance intelligence *with* AI, maintaining a human in the loop for decision-making rather than ceding full autonomy to machines. AI can instantly generate alternative analyses and options, considering constraints, but the final decision remains with the human.

A significant ethical concern is AI poisoning, which involves deliberate tampering with the data used to train AI models. This risk applies to both unstructured data (e.g., social media posts, videos, audio) and structured data (e.g., tables, forms, official reports). The question of how quickly detection systems can identify such deliberate attempts is critical. While there is confidence in developing detection mechanisms, the more complex issue is how to interpret these detections and the ethics of potentially using similar "poisoning" tactics against adversaries. This new paradigm of "cognitive warfare" necessitates developing new "Geneva conventions" for this domain, which currently do not exist.

Cultural and Ethical Alignment of AI Models

A profound ethical challenge arises from the observation that different global regions are developing AI models based on their own cultural contexts and belief systems. For instance, models developed in the West (e.g., adhering to GDPR and AI Acts) will likely embody different values and constraints than those developed in China or other regions. This means that "what model it is" could become a "cultural reference," potentially leading to AI systems that subtly embrace conflicting values or biases based on their training data. Ultimately, the consensus among the presenters is that AI models cannot be expected to be "more ethical than humans". Humans themselves often behave illogically or emotionally, and attribute ethics to

technology, which is inherently neutral. The responsibility for ethical deployment rests with the human users and developers, ensuring that AI is used responsibly and in alignment with an organization's or nation's core values.

Future Development and Implications

The development of AI in intelligence analysis is an ongoing process with several ambitious short-term and long-term goals.

Short-Term Developments

- Human Cognitive Heuristic Tools: Developing tools to infuse specific heuristic for more precise adversarial testing, allowing analysts to intentionally introduce and then identify heuristic and subjectivity in test scenarios.

- Scaling for Post-Production Review: Expanding the heuristic detection tool for widespread use in intelligence production, allowing for systematic review of existing intelligence documents for cognitive heuristics. This directly supports standards like ICD-203, which emphasizes objectivity. The potential to automate grading rubrics for the estimated 50,000 intelligence assessments produced annually could significantly enhance quality control and feedback.

- AI Agent Against Misinformation: Training AI to refute misinformation and disinformation on social media by addressing their underlying cognitive heuristics, which often serve as the root of conspiracy theories and propaganda. While AI can dismantle arguments, its ability to restore trust or undo strong cognitive heuristics like anchoring is a complex challenge.

Long-Term Developments

- Advanced Red Teaming Tools: Developing tools to assist intelligence analysts in identifying and mitigating cognitive heuristics in their own analysis, particularly when simulating adversary tendencies or decision-making patterns.

- Realistic Cognitive Modeling: Utilizing LLMs in simulated multi-agent wargames to enhance strategic decision-making analysis by modeling how leaders with specific heuristics and cognitive heuristics might react in various scenarios. The ability of LLMs to uncover "latent variables" (unidentified factors) could significantly enhance these simulations, providing insights beyond human intuition.

- Bias Tracking in Intelligence Reports: Monitoring the evolution of cognitive heuristics across sequences of intelligence reports, such as National Intelligence Estimates (NIEs), to identify "buildup of a heuristic" over time that could lead to flawed conclusions, as seen in historical intelligence failures like the Cuban Missile Crisis.

Conclusion

The integration of AI and LLMs presents a transformative opportunity for intelligence analysis, particularly in combating the pervasive influence of cognitive heuristics and enhancing overall analytical rigor. Through targeted training on diverse and balanced data, AI models demonstrate significant promise in detecting heuristics, explaining their reasoning, and offering pathways for correction. The benefits extend to augmenting human cognition, facilitating hypothesis generation, and streamlining processes, thereby enabling human analysts to focus on more complex and strategic challenges. However, the responsible deployment of AI demands careful consideration of ethical implications, including the potential impact on critical thinking, the integrity of data against malicious poisoning, and the inherent cultural biases that different AI models may embody. The consensus among experts is that AI should serve as an enhancement, not a replacement, fostering a synergistic human-machine teaming approach where the strengths of both are leveraged while mitigating risks through robust analytical processes and continuous human oversight. As this technology continues to evolve, ongoing research, ethical frameworks, and responsible implementation will be crucial for maximizing AI's potential to bolster national security.

Panel 4B – Open Source Intelligence (OSINT)

Contributors: Dr. Shadi Abouzeid (moderator), Dr. Elena Bailey (speaker), Dr. Giangiuseppe Pili (speaker), Mr. Seth Whitten (speaker), Dr. Ofer Gutterman (speaker), and Mr. David Siman-Tov (speaker).

The Evolving Landscape of National Intelligence: Embracing Open Source and Civilian Collaboration

The field of national intelligence is undergoing a profound transformation, challenging traditional definitions and operational paradigms. Historically characterized by secrecy, state-led activities, and classified information, intelligence increasingly intersects with the open digital sphere and civilian initiatives. This shift necessitates a new conceptual framework that recognizes the growing importance of Open Source Intelligence (OSINT) and the contributions of civil society, leading to the emergence of a broader "intelligence ecosystem." This paper explores the evolving definition of intelligence, the unique value and impact of OSINT and civilian-led initiatives, and the imperative for intelligence organizations to foster integration and collaboration with the civilian sphere while addressing inherent challenges and ethical considerations.

Redefining Intelligence in a Digital Age

Traditional definitions of intelligence often emphasize its secretive, state-centric nature, designed for action on national security goals, addressing adversaries, and involving classified military matters for official policymakers. Intelligence has been viewed as a process of requesting, collecting, analyzing, and providing specific types of national security information to policymakers while safeguarding these processes through counterintelligence and conducting operations as authorized by lawful authorities. However, the rise of open-source information and citizen-generated content has challenged these traditional boundaries.

The current transformative discourse around intelligence highlights OSINT, non-military threats, new labor markets, crowdsourcing, and public-private partnerships as key elements driving change. OSINT, specifically, encompasses more than just searching for data online; it

involves a formal process of collection, analysis, validation, and dissemination to inform decision-making and drive action. While historically viewed as "second-tier," OSINT is now recognized as a critical force multiplier when integrated with other intelligence disciplines like Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and Geospatial Intelligence (GEOINT). This evolution of information technology, characterized by 24/7 news cycles, social media, immersive platforms, and billions of citizens producing information, has created an open-source environment that serves as a "gold mine" for intelligence professionals.

The Unique Value and Impact of Open Source Intelligence

OSINT's power lies in its real-time access, global reach, and insight into human experiences, providing local context, civilian sentiment, and cultural nuances that traditional collection methods may overlook. This rich texture helps close intelligence gaps, enhance context, and facilitate a more comprehensive understanding of complex situations by connecting actors, behaviors, and networks.

Several case studies highlight OSINT's effectiveness:

- The Bellingcat investigation into the downing of MH17 in 2014 analyzed satellite imagery, social media posts, and leaked metadata to trace the Russian BUK missile launcher, uncovering key operational details before official intelligence agencies. This demonstrated OSINT's power to expose state-level military actions, bringing global attention and legitimacy.

- The Russia-Ukraine War (2022–present) showcased OSINT's unprecedented speed and reach in modern conflict, with civilian TikTok videos, Google Maps traffic patterns, and commercial satellite imagery used in real-time to track Russian troop movements. This provided critical early warning and served as a tactical asset.

- The "North Korea Uncovered" project is a landmark crowdsourced intelligence achievement, where volunteers collaboratively analyzed satellite imagery, defector testimony, and open-source reports to create one of the most detailed public maps of North Korea, penetrating one of the world's most secretive regimes.

- The "Don't F. With Cats" investigation (2010) exemplifies grassroots OSINT, where an online community tracked an anonymous animal abuser, evolving into a global effort that helped identify and locate a murderer by analyzing video metadata, background images, social media profiles, and geolocation clues.

These examples demonstrate how OSINT, powered by open-source data and civilian analysts, achieves significant operational victories. Moreover, the integration of Artificial Intelligence (AI) is enhancing OSINT, allowing for quicker and more accurate processing of large data sets. Tools such as large language models, computer vision, and geolocation algorithms are transforming threat detection, environmental monitoring, and foreign content translation, assisting analysts in triaging information, identifying patterns, and concentrating on critical signals. This renders human-AI collaboration both essential and operationally vital.

Civilian-Led Intelligence Initiatives

Beyond formal OSINT functions within intelligence agencies, civil society is increasingly engaged in "intelligence-like" initiatives, often driven by crisis situations. These initiatives

stretch the traditional definition of intelligence and demand a new conceptual framework, as they are expanding and "here to stay". Research highlights several types of civilian initiatives during conflicts, such as the 7/10 War in Israel:

- Tactical Early Warning: Citizens operated civilian command centers to collect information on potential attacks. While some initiatives, when aimed at traditional intelligence clients like military tactical units, faced institutional resistance, others successfully served local civilian officials, enabling communities to protect themselves.

- Countering Foreign Influence: Various civilian actors initiated efforts, often identifying the public or the intelligence community (IC) as their clients. These initiatives proved valuable by filling gaps where intelligence agencies faced limitations in distinguishing between foreign and domestic influence, showcasing a clear advantage for civilian efforts.

- Locating Missing People: Civilian command centers rapidly established themselves during crises, with dozens of volunteers collaborating to locate missing individuals. These initiatives showcased rapid establishment during state organizational delays, leveraging advanced technological solutions and cooperation with tech companies.

These civilian initiatives offer significant advantages, including speed, accessibility, innovation, and diversity. They operate outside institutional structures but are increasingly viewed as part of a broader "intelligence ecosystem."

Fostering an Open Intelligence Ecosystem

The evolving landscape calls for a paradigmatic shift in the relations between intelligence organizations and the civilian sphere across the entire intelligence value chain. This proposed "Open Intelligence framework" suggests several key components:

- Open-digital Intelligence Cycle**:** This concept involves various models of information flow and collaboration.

    - *Model A:* Unidirectional flow of information and knowledge *from* the civilian world *to* the IC (e.g., intelligence agencies harvesting publicly available data).

    - *Model B:* Unidirectional flow of information and knowledge *from* the IC *to* the civilian world (e.g., public sharing of intelligence by some national intelligence services to raise awareness or influence).

    - *Model C:* Elevating the civil sphere as a *new source of information and knowledge*, actively encouraging the population to produce intelligence rather than passively collecting it. This includes crowdsourced intelligence.

    - *Model D:* Collaboration on shared priority intelligence requirements (PIRs) in the digital dimension, representing co-production of intelligence.

- Symbiotic HR Strategies: Recognizing that modern generations seek more dynamic careers, intelligence organizations need to foster strategies that allow movement between the IC and civilian sector, bringing in external experts and allowing internal personnel to gain external experience.

- Publicly Shared Intelligence: Shifting the view of the civilian sphere as a target audience for intelligence, especially in an era of "truth decay" and disinformation, to ensure informed public discourse.

- *Collaboration with STEM Ecosystems:* Partnering with the private sector for technology and innovation in areas like robotics, sensors, and AI, as technological power increasingly resides outside government.

- *Non-military PIR:* Expanding intelligence focus beyond traditional military and security issues to include topics like supply chain, climate change, and rivalry over emerging technologies.

This framework moves beyond a strict classified/secret dichotomy, recognizing practices like OSINT collection and analysis as non-classified activities in the open domain, and influence campaigns as secret practices operating in the open domain. The goal is to establish a broader "intelligence ecosystem" that strengthens collective security through civil initiatives.

Challenges and Ethical Considerations

Despite the significant advantages, the expansion of OSINT and civilian intelligence presents notable challenges and risks:

- Institutional Resistance and Loss of Monopoly: Traditional intelligence agencies often struggle to internalize the loss of their information monopoly and adapt to a culture of secrecy. The classification of OSINT, even when derived from open sources, can occur due to the "mosaic theory," where combining unclassified information with classified knowledge by an intelligence professional can lead to a classified product. Private companies also "paywall" OSINT products due to the substantial processing power, AI, and effort required.

- Ethical Concerns: The line between intelligence gathering and mass surveillance becomes increasingly blurred, raising concerns about privacy, consent, and civil liberties. Issues of data retention, oversight, and accountability remain largely unresolved, with limited frameworks to regulate how open data is used, stored, and shared.

- Environmental Impact: The sheer volume of data collected and stored by OSINT activities places a significant strain on digital infrastructure and physical resources, including the vast amounts of water and energy used to cool massive data centers. A simple conversation with an AI model, for instance, can consume hundreds of milliliters of water.

- Quality and Reliability: While the open nature of OSINT can encourage rigorous practices due to public scrutiny, the lack of standardized practices for all actors can lead to misuse and mistakes. Adversaries also exploit AI to autonomously scrape, process, and summarize open-source material, potentially enhancing their intelligence or automating disinformation campaigns.

- Reluctance of Civil Entities: Civilian entities may be reluctant to cooperate with the IC due to varying ethical standards or concerns about independence.

Recommendations and Future Directions

To navigate this evolving landscape, several recommendations emerge for both the intelligence community and civilian initiatives:

- *For the Intelligence Community:*
    - Recognize and Integrate: Establish integration models for specific use cases of civilian initiatives and OSINT. This involves understanding OSINT as a fundamental intelligence discipline and integrating it effectively with other intelligence sources.
    - Foster an Open Ecosystem: Cultivate an environment where civil initiatives can strengthen collective security, learning from and adopting new techniques and tools from outside the IC. This includes embracing symbiotic HR strategies that allow for movement of talent between the IC and external organizations.
    - Develop Doctrine and Standards: For national intelligence organizations, it is mandatory to develop a doctrine for OSINT, outlining best practices, ethical guidelines, and quality standards to ensure professional and effective use.
- *For Civilian Initiatives:*
    - Recognize Risks: Be aware of the responsibilities and potential for error in unstructured intelligence activity.
    - Build Connections: Establish relationships with relevant actors in the IC when appropriate, while also maintaining direct relationships with the public and other civilian actors.

Future research directions are crucial for further understanding and optimizing this new intelligence ecosystem:

As the boundaries of traditional intelligence systems continue to blur, driven by rapid technological innovation, the decentralization of data access, and increased participation from civilian actors, there is an urgent need for scholarly and policy-driven inquiry to better conceptualize, evaluate, and guide this evolving intelligence landscape. The emergence of what may be termed an "open intelligence ecosystem" demands not only empirical study but also theoretical development to ensure that the integration of new actors, platforms, and practices enhances national security rather than undermines it. Three primary research trajectories stand out as especially pressing.

First, there is a critical need to develop a comprehensive theory of open intelligence ecosystems. Unlike closed, state-centric intelligence structures that have historically dominated the field, open ecosystems are characterized by a multiplicity of actors, including private sector firms, academic institutions, non-governmental organizations, citizen analysts, and decentralized technological platforms, operating in tandem with, alongside, or even independently from traditional intelligence agencies. Future research must seek to define the parameters of this expanded ecosystem, identify the modalities of interaction among actors, and theorize the rules of engagement, information flows, and power asymmetries that shape outcomes. Such a theory would not only help describe the empirical realities of contemporary

intelligence but would also offer normative guidance on how best to structure these relationships to promote security, accountability, and innovation.

Second, empirical and conceptual work is needed to construct viable models of institutional-civilian integration. While traditional intelligence institutions possess established infrastructures, legal authorities, and operational experience, civilian initiatives bring complementary strengths, such as agility, creativity, localized knowledge, and technological expertise. However, the integration of these domains is not straightforward. Challenges include issues of interoperability, differing epistemic standards, legal constraints, information security, and trust. Future research must explore models that allow for meaningful collaboration without compromising state secrecy, operational security, or analytic rigor. These models should identify best practices for coordination, delineate clear roles and responsibilities, and offer adaptive frameworks that can accommodate diverse actors across different operational contexts, from open-source intelligence collection to early-warning systems and crisis mapping.

Third, the proliferation of civilian intelligence initiatives introduces a host of ethical dilemmas that remain under-examined. As non-state actors increasingly collect, analyze, and disseminate intelligence-like information, often in real time and across global networks, traditional ethical frameworks built around state accountability and classification regimes become insufficient. The ethical risks in this domain are multifaceted: the potential for inadvertent harm to individuals and communities, the circulation of misinformation or unverified data, the exploitation of surveillance technologies without oversight, and the politicization or weaponization of open intelligence. Future research must develop normative frameworks and practical guidelines for addressing these grey zones. This includes articulating standards for transparency, consent, data stewardship, and verification practices, as well as proposing institutional mechanisms for oversight and redress when harms occur.

Together, these research agendas will be vital in shaping a resilient, adaptive, and ethically grounded intelligence ecosystem that reflects the complexities of contemporary security environments. As state and non-state actors continue to converge in their capabilities and roles, the imperative for rigorous, forward-looking scholarship becomes ever more urgent. Without such inquiry, the promise of innovation risks being eclipsed by fragmentation, overreach, and unintended consequences.

The future of intelligence lies in fusion and collaboration. While OSINT is powerful on its own, integrating it with other intelligence disciplines and behavioral science makes it exponentially more impactful, offering speed, context, and open access that other methods alone cannot provide. In an era of hybrid threats and information warfare, OSINT must be fully integrated, ethically applied, and strategically valued, with human-AI collaboration becoming essential. The goal is to reduce risk and gain a decision advantage, making the best risk-based choices with the information available.

The paradigm shift towards "open intelligence" emphasizes that intelligence organizations no longer have a monopoly on valuable information or analysis. Embracing this new reality, fostering collaboration, and developing robust ethical and operational frameworks will be crucial for collective security in an increasingly complex and open information environment.

List of speakers and affiliation

Dr. Barry Zulauf: Defense Intelligence Officer for Counternarcotics, Transnational Organized Crime, and Threat Finance

David Siman-Tov: Deputy Head of the Institute for the Research of Methodology of Intelligence

Dr. Elena Taube Bailey: Assistant Professor at the College of Information and Cyberspace a the National Defense University

Dr. Frederic Lemieux: Professor of the Practice and Founding Faculty Director

Dr. Giangiuseppe Pili: Assistant Professor at the School of Integrated Sciences at James Madison University

Dr. Monica Robbins: Behavioral Scientist at Peraton

Nicole Washington: Director at CGI Federal

Dr. Ofer Guterman: Senior Fellow at the Institute for the Research of Methodology of Intelligence (IRMI)

Dr. Rhian McCoy: Professor: International Security Policy • Intelligence • Conflict Analysis

Rohin Sharma: Counter WMD Strategist/Planner at DoD

Seth Whitten: Senior VP, Intelligence Solutions at Recorded Future

Dr. Shadi Abouzeid: Assistant Professor of the Practice and Associate Faculty Director, Georgetown University

Dr. Shay Hershkovitz: National Security Expert, Author, and Adjunct Professor at Georgetown University

Shira Barbibay-Shaham: Ben-Gurion University PhD Candidate and Researcher at the Institute for the Research of Methodology of Intelligence (IRMI)

Yossi Kuperwasser: Retired Brigadier General and head of the Institute for the Research of Methodology of Intelligence (IRMI)



24 Minoos Str., Strovolos, Nicosia,
2042 Cyprus
info@strategyinternational.org
https://strategyinternational.org/