Semi-Annual Lesson Report:

Information Advantage in Peace and Security

October 2023

Table of Contents

Section Title	Page
Introduction	3
People and Organizations	5
Overcoming the Data Neophyte Problem	5
Build Trust to Gain Relevant Information	6
Pandemic Lessons for Virtual Negotiations	8
Programs	11
Potential and Pitfalls for Artificial Intelligence in Peace, Stability, and Humanitarian Activities	11
Digital Technology and the Cease-Fire Fog—Ukraine, 2014-2022	13
China, Peacekeeping, and the Information Advantage: The US Must Respond	16
Improving Information Advantage: Local Political Analysis Systems	19
Educating Government Employees for the Information Environment	23
Policies and Governance	25
International Norm Development for Information Sharing	25
Free Speech is an Information Advantage	29
The Need for Data Governance and Literacy	31
Partnerships	34
The Asymmetric Advantage of Integrating Partners	34
Information Advantage in Non-Kinetic Peace Operations: Getting versus Guarding	37
The Information Sharing Partners Want and How to Give it To Them	40
PKSOI Lesson Reports, SOLLIMS Samplers, and Case Studies (2013-2023) (Selected)	44

Introduction

Information is necessary to make decisions. It is a logical assumption that more information leads to more successful outcomes. Therefore, decision-makers of all levels and professional fields seek more data. Yet, it is increasingly obvious that more data does not always result in an *information advantage* over competitors. The policymakers and practitioners engaged in peace and security efforts face the same information advantage challenges and opportunities as any other global societal entity. *Big Data* overwhelms everyone; picking the right data to call information is often the proverbial needle-in-a-haystack.[1]

To address the *data haystack*, the United Nations (UN) Secretary-General promotes the UN's Data Strategy with "focus not on process, but on learning…to deliver data use cases that add value for stakeholders based on our vision, outcomes and principles" and it recognizes potential "shifts in people and culture, partnerships, data governance and technology."[2] Yet, despite an international entity's published strategy, a group-effort information advantage conundrum—no matter the level or depth of an organization—is that the word *information* and all its related terms have distinct meanings. At the same time, the differences in meaning are often too dense or nuanced for the average person to find useful. As one author notes:

> complex data science terms such as biomes, labeling, big data, clustering, decision trees, neural networks, and the list goes on seemingly *ad infinitum*. Thus, the complexity of data terms can become overwhelming…a mere 32 percent of civilian business executives were "able to create measurable value from data" and only "27 percent said their data and analytics projects produce actionable insights."[3] [Original emphasis]

Beyond the plethora of information-related terms and definitions to confound users[4], some terms are burdened by prejudice. A classic example of a prejudicial term is the word *intelligence*, for which many societal entities disdain. Yet *intelligence* is commonly understood as *analyzed information*. Or, as one source describes, intelligence is information "that is capable of being understood," "with added value," and "evaluated in context to its source and reliability."[5] Therefore, the contempt for the term seems irrational unless one understands the underlying principles for it.[6]

---

[1] Unless otherwise noted, for this Lesson collection the term *Big Data* refers to: "the large, diverse sets of information that grow at ever-increasing rates. It encompasses the volume of information, the velocity or speed at which it is created and collected, and the variety or scope of the data points being covered (known as the "three v's" of big data). Big data often comes from data mining and arrives in multiple formats." See: Troy Segal, "What Is Big Data? Definition, How It Works, and Uses," *Investopedia*, November 29, 2022, https://www.investopedia.com/terms/b/big-data.asp (accessed September 30, 2023).

[2] "Secretary-General's Data Strategy," *United Nations*, https://www.un.org/en/content/datastrategy/index.shtml (accessed August 20, 2023).

[3] Jerry Landrum, "Overcoming the Data Neophyte Problem," *The War Room*, United States Army War College, August 17, 2023, https://warroom.armywarcollege.edu/articles/data-neophyte/ (accessed August 20, 2023).

[4] A 2022 Congressional Research Service reports outlines for the US Congress many information and information operation terms. It also asks *Who Is Responsible for the "I" in DIME*? The report notes the relationship between *information* and *irregular warfare* and that "much of the current information operations doctrine and capability resides with the military." However, it further notes that military leadership in the information environment may indicate "the militarization of cyberspace, or the weaponization of information" and that "the military may not possess the best tools to successfully lead information efforts" in the US government. See: Catherine A. Theohary, "Defense Primer: Information Operations (IF10771)," *Congressional Research Service* (CRS), December 9, 2022, https://crsreports.congress.gov/product/details?prodcode=IF10771 (accessed June 10, 2023).

[5] United Nations, "From Information to Intelligence," *Criminal Intelligence Manual for Analysts*, 2011, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf (accessed August 19, 2023).

[6] One paper explains individual and organizational disdain for the intelligence concept as follows: "Democratic societies…heed freedoms, rights, diversity, transparency, accountability, and so on. They also craft intelligence agencies to protect their national security and, ultimately, to maintain their democratic trajectory. Paradoxically, however, to serve democracies, intelligence agencies must engage in clandestine activities or exploit secret sources and methods—measures that, on their face, do not comport with the open, free society that democracies seek to sustain." See: Florina Cristiana Matei and Carolyn

The US Army's updated doctrine, ADP 3-13, *Information*, publication pending, acknowledges the conundrum of terms and definitions. Referring to the draft document, one advocate notes that "Information means different things depending on context," but the projected doctrine intends to "provide a foundation for thinking about information and the information dimension, as well as a framework for how Army forces, as part of a joint force, gain and maintain an information advantage."[7]

Governments and other organizational entities address the information environment to secure information advantage. To name just two, the North Atlantic Treaty Organization's (NATO) Allied Command Transformation (ACT) published its *Information Environment Assessment Capability Programme Plan* in April 2023,[8] and the United States (US) Defense Department (DoD) published its *Strategy for Operations in the Information Environment* (OIE) in July 2023.[9] The DoD's *Strategy for OIE* provides the structure for this Lesson collection, leveraging its four Lines of Effort (LOEs):

- *People and Organizations*, which includes individual and organizational information capacity and culture. Culture is both tangible (data literacy, language, e.g.) as well the intangible (i.e., trust).
- *Programs*, which include individual and organizational training and education as well as hard- and soft-technology and equipment.
- *Policies and Governance*, essentially, the management of information at various levels and situations.
- *Partnerships*, to include the multinational, interagency, non-governmental, academic, and private.[10]

This Lesson compilation contains three Lessons against each LOE with one exception. The *Programs* section contains five Lessons as training and technology topics appear to be a common concern among researchers and authors. Unsurprisingly, the LOEs are interdependent on each other; therefore, the Lessons contained within each section may also reflect on another section in this volume. In addition, this Lesson collection does not represent a comprehensive inventory of all terms and topic areas included in the information advantage discourse. Finally, some of the Lessons herein may use information and its related terms interchangeably and some topic areas may be incomplete. The intent is to provide an overview as well as insights that may encourage further study.

PKSOI's Lessons Learned Analyst, Colonel Lorelei Coplen (US Army, Retired), authored or edited the Lessons in this volume between April and September 2023, unless otherwise indicated. These lessons are also found in the Joint Lessons Learned Information System (JLLIS) database, identified by the JLLIS number adjacent to each lesson title. There are other Lessons on this topic found there as well but not included here due to space. JLLIS access is at https://www.jllis.mil and requires a Department of Defense Common Access Card (CAC) for registration.

Halladay, "The Role and Purpose of Intelligence in a Democracy," *The Conduct of Intelligence in Democracies: Processes, Practices, Cultures* (excerpt), London: Routledge Lynne Reinner Publishers, 2019. ISBN: 9781626378216 https://www.rienner.com/uploads/5cc34ebfcc2a4.pdf (accessed September 30, 2023).

[7] U.S. Army Intelligence Center of Excellence, "Emerging Army Doctrine on Information," *Always Out Front*, April-June 2021, https://www.ikn.army.mil/apps/MIPBW/MIPB_Features/AlwaysOutFront.pdf April–June 2021 (accessed May 30, 2023). The newsletter also indicates "*Information advantage activities* are the employment of capabilities to enable decision making, protect friendly information, inform domestic audiences, influence international audiences, and conduct information warfare." [Original emphasis] See also: Combined Arms Doctrine Directorate, "ADP 3-13 – Information," July 12, 2023, https://www.youtube.com/watch?v=aq8PuxyNswM (accessed September 30, 2023).

[8] North Atlantic Treaty Organization, "NATO's Allied Command Transformation's Information Environment Assessment Capability Programme Plan Initiated," *Allied Command Transformation*, April 3, 2023 https://www.act.nato.int/article/information-environment-assessment-capability-programme-plan-initiated/ (accessed July 30, 2023).

[9] U.S. Department of Defense, *Strategy for Operations in the Information Environment*, July 2023. (Not available online as of this writing.)

[10] Ibid.

People and Organizations

Overcoming the Data Neophyte Problem, JLLIS #230901-5126

Observation. Colonel Jerry Landrum, in his August 2023 online article, *Overcoming the Data Neophyte Problem*, suggests "a straightforward and natural question" often occurs to professionals who deal in data: "I need to become data literate, but where do I start?" He notes that:

> The good news is that becoming a data scientist is not a requirement, but having a mental model to navigate through the concepts is useful. *Set convergence*… (is a) … does not hold all the answers to the data puzzle, but it helps to begin asking the right questions. [Emphasis added]

Discussion. In a May 2021 memorandum to Defense senior leaders, Deputy Defense Secretary Kathleen Hicks declared that data was a strategic asset, and she directed the DoD to seek ways to make data more accessible and easier to integrate. Consequently, the US Army subsequently issued its eleven strategic objectives Data Plan[11] to become *data centric*. Yet, the data-centric operations concept is at least thirty years old, derived in part from the US Army's 1993 Force XXI transformation model. This model purported that information technology would revolutionize warfare because they could enable "commanders to make decisions faster, dominate the battlespace, and win throughout the full spectrum of operations." However, the Hicks directive focuses less on the technology—the information systems—and more on the data itself. In other words, how to manage the data.

The author describes Daniel Jones' book *Data Analytics: A Comprehensive Guide to Learn and Understand Data Analytics and Its Functions* which outlines the importance of *skillset*, *mindset*, *dataset*, and *toolset* in data analytics. He proposes *set convergence*[12], "a term borrowed from design thinking in which various ideas are filtered to generate new perspectives," as "a good foundation for sorting through the complexities surrounding data thinking."

"*Skillset* is arguably the easiest part of the model to obtain" because the US Army "is full of trained and educated specialists who routinely generate data." Yet, "practitioners do not understand that they are also Data Generators and the relevance their data has in operational decision-making." As the author notes:

> Thus, you are not just an Infantryman; you are an Infantryman who is a Data Generator. This might sound like a trivial distinction, but it is an important adjustment in self-perception that is necessary for data-centric operations. It also requires the practitioner to understand that her data is important to the overall operation. Too often skilled practitioners mistakenly perceive their data as specialized and unrelated to the larger operational approach, but all data sets are worthy of examination. Once a practitioner fully understands the significance of being a Data Generator, he or she can develop a mindset that looks at data differently.

"*Mindset* is the ability to identify and read data that might describe, diagnose, predict, and/or prescribe." [Emphasis added] There are several related questions to "read data":

> Is the data categorical, quantitative, temporal, or spatial? Is your data structured in an Army system of record, or is it unstructured data residing on an obscure and inaccessible file server? Is it semi-structured within a spreadsheet or database?

[11] US Army Public Affairs, "Army announces consolidated Data Plan," October 13, 2022, https://www.army.mil/article/261114/army_announces_consolidated_data_plan (accessed September 30, 2023).
[12] It also features prominently Joint Operational Design and Army Design Methodology.

As the author asserts, “Obtaining a basic level of data literacy helps data neophytes identify datasets.” The he notes “datase*t* identification might be the most difficult challenge” to set convergence but emphasizes that “data neophytes often need only to explain and provide information to professionals who assist units in the development of data capabilities.” These experts may be civilian employees who are data scientists and help organizations with data requirements. He outlines four questions for the neophyte to address:

- “Is the data transparent?” That is, does the data expert know the data source and can trust it? “For a plethora of reasons ranging from time available to language barriers, the data you are ingesting might be flawed and lead to faulty analysis.”
- “Is the data precise?” Data is helpful only to assist decision-making. “Again, the mindset that all data is important and worthy of examination is important.”
- “Is the dataset large enough?” Determining “reoccurring patterns” rather than “anomalous events” is difficult, “especially given that anomalous cases occasionally have outsized effects.”
- “Is the data timely?” Data “cloistered on computer hard drives or buried deep in a file server” is not useful.

A *toolset* assists task execution. The US Army already has “hundreds of systems and applications” that “may sense (input layer), apply algorithms (hidden layer), or produce deductions (output layer).” Or, as the author notes, “all three at once.” Yet, to conduct data-centric operations effectively, systems must be “open standard and interoperable…and... contracting processes should mandate interoperability in statements of work.” Further, “Organizations should seek to purchase the data used on its systems because the data is more important than the system…and…Defense-related and associated organizations should prioritize dataset ownership over dataset consumption.”

Recommendations. The author suggests, “as data literacy increases, the sophistication of interactions will also increase.” Meanwhile, *set convergence*—the convergence of skillset, mindset, dataset, and toolset—is one model to assist data neophytes transition to data-centric operators. The Defense Department, in coordination and conjunction with the US government interagency, should leverage its training and exercises and other interactions to accelerate this transition.

Lesson Author: Colonel Jerry Landrum, US Army, is a 2000 graduate of the University of North Georgia. His last assignment was with the XVIII Airborne Corps at Fort Liberty where he was introduced to data-centric operations and observed the practical implementation of JADC2. Colonel Landrum attended Kansas State University where he earned a PhD in Security Studies. He is currently serving as a Faculty Instructor at the United States Army War College. COL Landrum was a member of the Carlisle Scholars Program and a graduate of the AY22 Resident Course at the US Army War College. This Lesson is derived from the recent publication: Jerry Landrum, “Overcoming the Data Neophyte Problem,” The War Room, United States Army War College, August 17, 2023, https://warroom.armywarcollege.edu/articles/data-neophyte/ (accessed August 20, 2023).

Build Trust to Gain Relevant Information, JLLIS #230606-3062

Observation. In June 2023, the *United States Institute of Peace* (USIP) marked the 75th anniversary of the United Nations (UN) with an article assessing peacekeeper skills and competency needs for current and future peace missions: “To fulfill their increasingly complex mandates, U.N. peacekeepers need the *skills to build trust* with vulnerable communities.”[13] [Emphasis added] Linking *trust* to *information*, the authors continued:

[13] Ouiem Chettaou and Gbenga Oni, “What’s Next for the Blue Helmet 75 Years Later?” *United States Institute for Peace*, June 1, 2023, https://www.usip.org/publications/2023/06/whats-next-blue-helmet-75-years-later (accessed June 3, 2023).

> …some peacekeeping missions continue to struggle with *community trust*, which in turn leads to *informational gaps* that rebel groups utilize to their advantage…To thrive and effectively fulfill their mandate to protect civilians, peacekeepers require an entirely different, complementary set of skills and dispositions that empower them to better assess needs and interests, *build trust*, communicate with care, and manage conflict nonviolently.[14] [Emphasis added]

The rising use of digital technologies for diplomacy and negotiations also brings concern over trust between parties and the relationship between trust—or distrust—to relevant information gain. A three-year study of European Union (EU) online diplomatic engagement notes the common belief that "exchanging through and with digital tools is particularly challenging as it hinders the formation and upkeep of one of the core elements of diplomacy: trust."[15] While the authors found "that digital tools…contrary to commonly held assumptions, do not negatively impede diplomatic trust,"[16] they also noted:

> First…digital tools create both new opportunities for and challenges to diplomatic trust, though these opportunities are more accessible to some than others. Second, whereas trust is taken online, it is not easily built digitally. Third, digital tools lead to a rearticulation of the place of transparency and confidentiality in diplomatic negotiations. *It pushes diplomats to reconsider what it means to share information in an (un)trustworthy manner*.[17] [Emphasis added]

Both these observations suggest that information accuracy as well as its accessibility depends in large part on the trust between parties in the information exchange, whether in physical proximity or in a virtual environment. Further, both require training and education to develop appropriate competencies to elicit and facilitate trust and, consequently, information.

Discussion. The Merriam-Webster online dictionary includes the following as part of its definition of *trust*: a. *assured reliance on the character, ability, strength, or truth of someone or something*, and b. *one in which confidence is placed*.[18] [Emphasis added] The EU online diplomacy study authors offered their own *trust* definition: "the momentary suspension of uncertainty and vulnerability vis-à-vis the intentions and actions of others."[19] They further acknowledged:

> Our analysis started from the premise that information sharing is indispensable for diplomatic negotiations…[but] Diplomats, however, make themselves vulnerable when sharing information as they can never be certain that information is sincere, properly received, or kept from outsiders…trust allows them to act in the illusion that vulnerabilities will be handled with discretion.[20]

In their conclusion, the study authors found "trust can indeed be taken and maintained online."[21] Yet, successful trust building in the online environment may depend on two factors: The work online in tandem with or adjacent offline engagements (such as physically proximate meetings); and "the power of

---

[14] Chettaou and Oni, "What's Next for the Blue Helmet 75 Years Later?"
[15] Kristin Anabel Eggeling and Larissa Versloot, "Taking trust online: Digitalisation and the practice of information sharing in diplomatic negotiations," *Review of International Studies* (December 2022), Cambridge University Press, https://www.cambridge.org/core/journals/review-of-international-studies/article/taking-trust-online-digitalisation-and-the-practice-of-information-sharing-in-diplomatic-negotiations/F1E90D2FEAAC8F586094C8A3F15DE5B5 (accessed June 15, 2023).
[16] Ibid.
[17] Ibid.
[18] "Trust," https://www.merriam-webster.com/dictionary/trust (accessed June 29, 2023).
[19] Eggeling and Versloot, "Taking trust online."
[20] Ibid.
[21] Ibid.

unspoken rules in diplomatic practice and the boundaries they draw around diplomatic work" (the norms).[22]

Recommendations. The USIP June 2023 article on peacekeeper competencies offered some reasons for the poor trust relationship between peacekeepers and the community. The authors pointed out the deployment briefness precludes trust-building due to a simple lack of time, as example. However, they also noted the lack of training for peacekeepers on *soft skills* "such as communication, conflict analysis and management, and collaborative problem-solving."[23] Pre-deployment training currently focuses on technical skills rather than the actions—and the mindsets—that can create conditions to build trust and access information that may protect the mission and the population.[24] Similarly, the EU online diplomacy study authors also rejected technology as either a promotional or a detrimental instrument for trust building and relevant information sharing. Instead, they asserted:

> More than the use of certain soft- or hardware, questions of the digitalisation [sic] of diplomatic practice speak to the professions' self-understandings, norms and ways of doing things.[25]

In other words, technology can assist, but cannot replace, the human interaction needed to build trust and gain information. Further, human interaction skills require deliberate education and training.

Pandemic Lessons for Virtual Negotiations, JLLIS #230606-3061

Observation. In 2022, Corneliu Bjola and Michaela Coplen of Oxford University published their analysis of "perceptions of efficacy, tactics, and legitimacy" of *virtual venues* based on a survey of diplomats with negotiation experience during the COVID-19 pandemic period. They noted, in part:

> While diplomats expressed reservations regarding the efficacy of virtual venue negotiation and specifically the confidentiality of these venues, they generally supported the legitimacy of virtual negotiation processes and agreements reached therein. Diplomats agreed that virtual venues are here to stay, and for the most part have adapted accordingly.

While *virtual venues* may be "here to stay," the authors acknowledged that diplomats may continue to perceive virtual venues as "stand-ins" or in lieu of *physically proximate venues*. In other words, some may consider *virtual venues* as a necessary but less-satisfactory means to continue negotiations when the environment cannot support physical proximity between parties. Instead, the authors suggested *virtual venues* may have advantages over *physically proximate venues* in addition to some disadvantages. Consequently, both venues may have appropriate roles in negotiations and both may be appropriate to affect an *information advantage*[26] of one negotiating party over others, depending on context, environment, and purpose.

Discussion. The COVID-19 pandemic travel restrictions forced many personal interactions to online or *virtual venues*. Post-pandemic, there are a few studies and much anecdotal evidence that share the relative advantages and disadvantages of the virtual or remote communication means over or in conjunction with physically proximate venues. The authors acknowledged:

---

[22] Eggeling and Versloot, "Taking trust online."
[23] Chettaou and Oni, "What's Next for the Blue Helmet 75 Years Later?"
[24] A 2023 study of peacekeeper mindsets observed "unbiased peacekeepers are the most effective at promoting trust" thereby suggesting "impartiality as an important condition under which peacekeepers build trust post-conflict." See: Jared Oestman and Rick K. Wilson, "The Effect of Biased Peacekeepers on Building Trust." *Journal of Experimental Political Science*, 2023, 1–12.
[25] Eggeling and Versloot, "Taking trust online."
[26] As of this publication, the updated Army Doctrine Publication (ADP) 3-13, *Information*, is pending publication.

> Practitioners and scholars of diplomacy have long recognized that venue selection is an important part of the negotiation process. Diplomats consider factors such as expedience, negotiation format, tradition, and prestige in determining the appropriate venue for sensitive international negotiations…virtual venues have often been selected out of necessity. The instrumental, symbolic, and strategic considerations that commonly inform venue selection in face-to-face negotiations, as mentioned above, are arguably less relevant when applied to the virtual medium, or at least their impact is more difficult to gauge.

They further noted that most research indicates face-to-face negotiations can be trust-building opportunities. By implication, virtual venues do not have the same prospects for trust between parties. What they do offer over physically proximate venues is the ability to work collaboratively on negotiation documents ('track-change diplomacy') with increased "shareability, visualization, and immediacy of information," but with some related disadvantages as well:

> These technologies also reflect and exacerbate existing power dynamics in a negotiation. Disputes over the control of virtual text can lead to confusion and inefficiency. Parties may take advantage of procedural 'disorder' to influence the course of the negotiation…

Other summarized research indicates: "digital diplomacy has expanded the 'negotiating table'" through social media as an example; that "virtual venues succeed when they are built on existing 'normal negotiation practice' and collective 'background knowledge'"; that participants in virtual venues may notice greater "accessibility, frequency, and equity of participation," but the "'social bonding' processes and diminished faith in confidentiality can be detrimental"; and, conversely, "while negotiators were able to adapt and build trust in new technologies and modes of communication, concerns about equity, transparency, and process were pervasive." The survey findings regarding perceptions of *virtual venue effectiveness* were similarly conflicted[27]:

> For some, the change induced by virtual venues is quite positive as they ensure that everyone receives the same information, the meeting is faster…and they make it easier to have pre-meetings or post-meetings with other diplomats engaged in the negotiations…For others, the change is not necessarily beneficial since virtual venues make it more difficult to build coalitions, information-sharing is graphics rather than content-oriented, and there is minimal or non-existent backchannelling…

Most of the surveyed diplomats expressed *virtual venue efficacy* concerns as their (in)ability to "'read the room' in virtual venues, that is, to follow who is paying attention to the discussion, what issues resonate with whom, how participants engage with each other, etc." However, the authors made an interesting observation, noting that "the distribution by diplomatic rank among those capable of 'reading the room' was relatively even, suggesting that virtual venues might dilute the inherent advantage of senior diplomats in capturing the dynamic of the conversations."

Virtual venues also changed some of the normal negotiating tactics. The authors specifically asked diplomatic respondents about the use of *persuasive* and *coercive tactics*.[28] They determined more impact

[27] The authors note: Several additional limitations to this survey methodology warrant consideration. While respondents were not exclusively representatives of Western states (43% of respondents were diplomats from nations outside Europe and North America), there remained a significant Western bias. Additionally, the respondent pool reflected a gender bias (only 25% of respondents self-identified as women).

[28] The authors note: The first category refers to methods by which negotiators seek to build a positive understanding with their interlocutors by facilitating information-sharing, coalition-building, or backchanneling. The second category includes methods by which negotiators seek to extract benefits by weakening interlocutors' resolve using stonewalling, ultimatums, or threats.

on coercive tactics than on persuasive tactics in a virtual negotiating environment, but even that impact was assessed by some as a positive but by others as a negative:

> Specifically, 57% of the diplomats in our sample agreed that virtual venues impacted the use of coercive tactics…the "virtual room softened the impressions of personal antagonism" and therefore the use of coercive tactics was expected to be more subdued online. The short duration of online meetings could also make coercive tactics more difficult to deploy. For others, virtual venues made it easier for delegations to stonewall and stall the discussions by invoking technical difficulties or postponing meetings…Specifically, virtual venues make it easier to deploy these tactics than in face-to-face meetings, thus generating a more direct and immediate effect on the structure of incentives and opportunities of the negotiating parties.

The survey uncovered a coercive negotiation tactic unique to the virtual venue: "the performance of technical difficulty." Whether real ("digital literacy") or feigned ("transparent theater"), technical difficulties often resulted in negotiation disruption or stalling.

The one aspect most of the respondents agreed with was the *legitimacy* of the negotiated outcomes in virtual venues. That is, most were confident their negotiations would not be reopened over the same ground in later physical proximate meetings. This led the authors to assert:

> The strong level of confidence in the quality of the negotiation outcomes concluded online suggests that virtual venues are no longer seen as exotic places, located outside the realm of diplomatic activity. In fact, they are increasingly perceived as a credible alternatives [sic] to face-to-face negotiation arenas.

Interestingly, the confidence in the virtual negotiations' legitimacy remained even when "Faith in the confidentiality and security of virtual venue negotiation was generally low."

Recommendations. The authors acknowledged there are more aspects of diplomatic negotiations in *virtual venues* to research. One area they highlighted for future study is *participant inclusivity and engagement*. They asked:

> How does the number of participants in a virtual negotiation impact diplomats' ability to read the room and reach agreement? Is there a 'limit' to the number of participants that can be meaningfully included, and how is this related to the 'view' format of the virtual venue selected? Similarly, how can mediators, meeting chairs, and negotiating parties better engage reluctant or withdrawn parties – and how should mediator/chair selection adapt to include these considerations? How does 'Zoom fatigue' differ from the forms of travel and negotiation fatigue common to face-to-face diplomacy? How can 'Zoom fatigue' be mitigated to make virtual negotiation more effective? What are the effects of time zone differentials in virtual venue negotiations? In general, what makes one virtual venue more effective than another – and how can existing venues be adapted (or new ones built) to provide the 'best' international negotiation platform?

They also noted "the potential for virtual venues to exacerbate power imbalances between negotiating parties" for further study:

> Venue selection is always a careful navigation of benefits and trade-offs, and selecting a virtual venue is no different. Depending on the negotiation context and content, choosing a virtual venue may benefit one party over others; in such cases, continued in-person contact and/or increased hybridity may be necessary to rebalance power dynamics for more fair and effective negotiation outcomes.

Lastly, they suggested "further examination of the opportunities and challenges presented by these venues and may require diplomats and negotiators to undertake additional specialized training on effectively operating in these spaces."

This Lesson's ideas and quotes derive from the paper indicated below, except as otherwise noted:
Corneliu Bjola and Michaela Coplen, "Virtual Venues and International Negotiations: Lessons from the COVID-19 Pandemic," International Negotiation (June 2022): 1-25,
https://www.researchgate.net/publication/361240078_Virtual_Venues_and_International_Negotiations_Lessons_from_the_COVID-19_Pandemic (accessed January 30, 2023).

Programs

Potential and Pitfalls for Artificial Intelligence in Peace, Stability, and Humanitarian Activities, JLLIS #230601-3616

Observation. In July 2023, the International Telecommunication Union (ITU), the United Nations' agency for information and communication technologies, hosted "The AI for Good Summit 2023."[29] While the final report from the Summit is not yet available, several articles and papers of the past few years provide similar focus on the benefits as well as the risks of existent and emerging Artificial Intelligence (AI) technology for peace, stability, and humanitarian activities. As one article notes:

> The image of intelligent machines freeing us from drudgery and allowing us to focus on more fulfilling work competes with dread over the possibility of computers possibly gaining autonomy and turning against humans… (the images) reflect a growing recognition of the need for guardrails around these technologies and for discussion of how to spread its benefits evenly…(or) how to harness (AI's) tremendous power for good and mitigate any potential harm.[30]

Prudent practitioners and policymakers alike should be aware of both the *potential* and the *pitfalls* of AI use in missions and operations to create and maintain *information advantage*.

Discussion. Several recent documents share some governmental approaches to address both AI *potential* and related *pitfalls*. These include, but not limited to, the 2021 adoption of the *Recommendation on the Ethics of Artificial Intelligence by* the Member States of the UN Educational, Scientific and Cultural Organization (UNESCO) that "defined the common values and principles needed to ensure the healthy development of AI."[31] Another United Nations report is the *United Nations Activities on Artificial Intelligence 2022* which provides an overview of the UN's initiatives in AI and highlights the need for regulatory frameworks, transparency, and human rights protections.[32] The African Union began a series of workshops in 2022, apparently still ongoing, to develop "the continental strategy" for AI.[33] Last of this list is the European Commission's *A European approach to artificial intelligence*.[34] None of these

[29] *AI for Good*, https://aiforgood.itu.int/summit23/ (accessed July 15, 2023).
[30] Politically Speaking, "Exploring the Potential and Pitfalls of Artificial Intelligence as a Tool for Prevention and Peacebuilding," *Medium*, June 2, 2023, https://dppa.medium.com/exploring-the-potential-and-pitfalls-of-artificial-intelligence-as-a-tool-for-prevention-and-77fb3e15b442 (accessed July 3, 2023).
[31] UN Educational, Scientific and Cultural Organization, "Draft Text of the Recommendation on the Ethics of Artificial Intelligence," *United Nations*, https://unesdoc.unesco.org/ark:/48223/pf0000377897 (accessed July 15, 2023).
[32] International Telecommunication Union, "United Nations Activities on Artificial Intelligence 2022," https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2022-PDF-E.pdf (accessed July 9, 2023).
[33] "Artificial Intelligence is at the core of discussions in Rwanda as the AU High-Level Panel on Emerging Technologies convenes experts to draft the AU-AI Continental Strategy," *African Union*, March 29, 2023, https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging (accessed July 29, 2023).
[34] Shaping Europe's Digital Future, "A European approach to artificial intelligence," *European Commission*, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed July 3, 2023). A succinct and accessible

documents share their definitions of differing terms of reference. However, Ana Beduschi's paper for the International Review of the Red Cross suggests:

> AI is broadly understood as "a collection of technologies that combine data, algorithms and computing power." These technologies consist of software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal.[35]

Further:

> This definition comprises two main elements: knowledge-based systems and machine learning systems. Knowledge-based systems are seen in computer programs that use an existing knowledge base to solve problems usually requiring specialized human expertise. Machine learning is "the systematic study of algorithms and systems that improve their knowledge or performance with experience." Through machine learning, machines can be trained to make sense of data.[36]

In the realm of AI *potential* for peace, stability, and humanitarian activities, AI use may allow for predictive analyses of actors and their behaviors which could, in turn, provide for preventative measures deployment to avoid or mitigate conflict or other harms. One example is the use of disaster mapping to forecast population displacement to enhance response and resources. In another example, AI language interpretation can enhance "public voices in the specifics of peace negotiations…for mediators and actors to hold real-time consultations with a large group of individuals in local dialects and languages."[37] Essentially, AI can expand the toolkit of humanitarian missions in their three main dimensions: preparedness, response, and recovery.[38]

Yet, there are the *pitfalls* of AI use in the same contexts "as they may expose populations already affected by conflict or crises to additional harms and human rights violations."[39] Beduschi summarizes some of the overarching concerns in a "range from the dangers of *surveillance humanitarianism* to the excesses of *techno-solutionism* and the problems related to a potential rise in *technocolonialism*."[40] [Emphasis added] Yet she emphasizes three areas "of particular relevance in the context of humanitarian action: data quality, algorithmic bias, and the respect and protection of data privacy." She furthers notes that data quality combined with algorithmic bias is a concern across many professional fields as the analyses results may be faulty.[41] But in the humanitarian context, it can have terrible consequences beyond simple error.

---

comparison to the European Union and the United States status for AI governance can be found at Alex Engler, "The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment," *Brookings*, April 25, 2023, https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/ (accessed July 25, 2023).

[35] Ana Beduschi, "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks," *International Review of the Red Cross* 104, no. 919 (2022): 1149-69, https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/harnessing-the-potential-of-artificial-intelligence-for-humanitarian-action-opportunities-and-risks/C8C491CC24DE1BEBC836DA77069F3F63 (accessed June 28, 2023).

[36] Ibid.

[37] The Department of Political and Peacebuilding Affairs (DPPA), "Project: AI-powered large-scale synchronist dialogues," *AI for Good,* https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/undppa/ (accessed July 29, 2023).

[38] Beduschi, "Harnessing the Potential…"

[39] Ibid.

[40] Ibid.

[41] Often referred to from a phrase derived from early computing, "garbage in, garbage out" or GIGO. See https://www.techopedia.com/definition/3801/garbage-in-garbage-out-gigo.

Recommendations. AI can have functions from the lowest level staff entity through the policymaker and the governing body. The UN already recognizes how AI applications could address more mundane tasks which in turn allows for more innovation, but staff needs training.[42] In May 2023, the European Commission, apparently also in recognition of both AI's potential and pitfalls, established five main rules for its staffers to follow when using AI tools and products:

- Not disclosing information not in the public domain when using a generative AI tool.
- Being aware that the AI's responses might be inaccurate or biased.
- Considering whether the AI might be violating intellectual property rights.
- Never copy-pasting AI-generated output into official documents.
- Avoiding the use of AI tools when working on "critical and time-sensitive processes.[43]

On a more philosophical level, Beduschi avers a "do no harm" philosophy to resolve the inherent conflict between AI *potential* and its *pitfalls*:

> As *AI systems are not inherently neutral*…they may introduce new, unnecessary risks to already vulnerable populations.…Accordingly, to put AI at the service of humanitarian action, leveraging its benefits while outweighing its risks, humanitarian organizations should be mindful that there is no ready-made, "one-size-fits-all" AI solution applicable to all contexts. They should also evaluate whether AI systems should be deployed at all in certain circumstances, as such systems could cause more harm than good to their beneficiaries. On certain occasions, *the fact that technology is available does not mean that it must be used*.[44] [Emphasis added]

In the "do no harm" context, organizations and governments must "strengthen *accountability* and *transparency* in the use of AI in the humanitarian context…(and)…In the digital age, avoiding or mitigating harm also entails the protection of *data privacy*."[45] [Emphasis added] She defines *transparency* as "whether and how they use AI systems" and *accountability* as "holding someone to account for their actions or omissions."[46] Further, any AI governance framework should account for *redress* mechanisms, or the means for individuals to "challenge decisions that were either automated or made by humans with the support of AI systems if such decisions adversely impacted those individuals' rights.[47]

Digital Technology and the Cease-Fire Fog—Ukraine, 2014-2022, JLLIS #230400-1303

Observation. In early 2023, a group of researchers and authors produced a paper series focused on digital technology use during peace processes. Each paper addressed a specific technology type. This is one of the Lessons derived from that paper series. It is a review of the digital technologies used by the Organization for Security and Co-operation in Europe (OSCE) Special Monitoring Mission (SMM) to monitor the cease-fire in Ukraine from 2014 until the 2022 Russian invasion. The authors assert:

> the use of new technologies by cease-fire monitoring missions strengthens their *epistemic* abilities, but their ability to work at the *ontological* level is primarily shaped by politics, which

[42] Politically Speaking, "Exploring the Potential and Pitfalls of Artificial Intelligence as a Tool for Prevention and Peacebuilding."
[43] Gian Volpicelli and Jacopo Barigazzi, "European Commission tells staff: Don't use AI for 'critical' work," *Politico*, May 31, 2023, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed July 30, 2023).
[44] Beduschi, "Harnessing the Potential…"
[45] Ibid.
[46] Ibid.
[47] Ibid.

> defines missions' mandates and implies rules about third-party engagement in conflict management situations.[48] [Emphasis added]

Digital technology use can provide more knowledge or information *certainty* to assist in mission decisions. However, the mission environment's very nature inserts *uncertainty* into the decision process. They conclude:

> policymakers and peacemakers should not assume that adding remote sensing technology to cease-fire monitoring missions will reduce challenges associated with all types of un-certainty [sic]. Rather…they should seek to match technology to the specific uncertainties of the conflict context and to what end data are gathered, while keeping in mind the wider implications of the advantages and disadvantages of such technological means.

Discussion. All participants need to address *uncertainty* in their peace and stability policy decisions and programs. In the introduction to their paper series, the authors acknowledge:

> International organizations with conflict prevention and peacebuilding mandates have recently spearheaded a range of policy and practice initiatives to harness the power of digital technologies in their struggle against uncertainty. …Overall, these policy initiatives demonstrate a larger trend *to identify the lack of sufficient credible information as a key hurdle for effective conflict prevention and peacebuilding*, and consequently advocate to bolster efforts to employ digital technologies to overcome such information challenges. [Emphasis added]

In other words, the policy and practice initiatives for digital technologies seek *information advantage*, an emerging term in US Army *information* doctrine.[49] Maggie Smith and Nick Starck, writing for the *Modern Warfare Institute (MWI) at West Point* in May 2022, define *Information Advantage* as "a condition of relative advantage that enables a more complete operational picture and leads to decision dominance—the sensing, understanding, deciding, and acting faster and more effectively than the adversary."[50] The *Information Advantage* concept also applies in those circumstances when one seeks to better understand the sources of conflict and the motivations of the parties involved, as found in peace and stability efforts to include, but not limited to, cease-fire monitoring.

The authors reviewed 2014-2022 OSCE SMM in Ukraine to determine how digital technology created *information advantage* to improve the monitoring efforts. The SMM's deployment supported a request from the Ukraine's government and followed the Russian annexation of Ukraine's Crimean Peninsula in February through March 2014.[51] Their choice of OSCE SMM in Ukraine as a case study was due to its repute as "the most technologically advanced cease-fire monitoring mission deployed to date."

Prior to the OSCE SMM review, the authors described three mechanisms used "to create more durable cease-fires" regardless of conflict: alter incentives to violate cease-fires (i.e., make violations "unattractive"); "reduce uncertainty about intent and actions" of one conflict party for another; and "mitigate the risks of involuntary escalation"—that is, accidental violations. For all three mechanisms, digital technologies are considered effective "to gather, verify, and share credible information about the

---

[48] *Epistemic* and *ontological* are philosophical terms. *Epistemic* refers to the knowledge necessary—or lack of it—to decide or make a statement. *Ontological* refers to the nature of things or a relationship between concepts which may facilitate or complicate decisions. See: Alexander Nyland, "6 Types of Moral Dilemmas in Life and How to Resolve Them," *Learning Mind*, April 13, 2019, https://www.learning-mind.com/moral-dilemmas-types-resolve/ (accessed April 30, 2023).
[49] As of this writing, the updated Army Doctrine Publication (ADP) 3-13, *Information*, is pending publication.
[50] Maggie Smith and Nick Starck, "Open-Source Data Is Everywhere—Except the Army's Concept of Information Advantage," *Modern Warfare Institute at West Point*, May 24, 2022, https://mwi.usma.edu/open-source-data-is-everywhere-except-the-armys-concept-of-information-advantage/ (accessed April 20, 2023).
[51] Organization for Security Co-operation in Europe (OSCE), Special Monitoring Mission to Ukraine (SMM), https://www.osce.org/special-monitoring-mission-to-ukraine-closed (accessed May 2, 2023).

specific circumstances and about culpability" for cease-fire violations, but "the effectiveness of such information is conditioned by the political authority and legitimacy of a mission and its ability to provide a contextualized understanding of conflict events." They assert:

> Technology, in particular the use of remote sensors, can help gather information that facilitates the interpretation of incidents and that may be shared with conflict parties as documentary evidence of a violation. The use of technology may therefore help a monitoring mission to (re)establish some…authority, if it allows monitors to gather and verify information through means that are not accessible to the parties themselves.

In caution, they also note that monitoring technology may answer what happened in a cease-fire violation, but it cannot always address why it happened—i.e., the perceived intent, deliberate or accidental. Yet other technologies, such as videoconferencing and evidence-sharing can serve as "ritualized space" to meet and resolve disagreements.

The OSCE SMM in Ukraine manifested many of these observations regarding digital technology in cease-fire monitoring. As the OSCE notes:

> The SMM was an unarmed, civilian mission, operating on the ground 24/7 Ukraine. Its main tasks were to observe and report in an impartial and objective manner on the security situation in Ukraine; and to facilitate dialogue among all parties to the conflict.[52]

In its eight-year mission, the SMM reported innumerable cease-fire violations with a full array of machine technology and images/sounds. The mission was able to always receive and record data, with minor risk to the unarmed mission personnel. Some observers noted the technologies applied allow access to primary evidence in real time in a manner and volume previously unknown. This information was essential to address mis- and disinformation promoted by both conflict parties and provide accurate findings about violations. Yet, the monitor personnel determined the type and placement of remote monitoring technology, so their analysis by default measured at self-selected places and times. In addition, the volume overwhelmed them as they analyzed only part of the information at a time. Further, the analysis depended on eyewitness verification. All these elements suggest "that the use of technology offered more complementarity to human monitors than substitution." Lastly, the SMM appeared hampered by its own mandate which allowed no attribution of violations to either conflict party. The authors point out:

> The inability of the mission to name the perpetrator, and much less to directly sanction violations, limited the costs conflict parties faced for cease-fire violations. As one former SMM official noted, "it is easy to count" violations as long as they are unattributed (former SMM official, online event, April 2021).

The SMM's work, consequently, addressed two of the three mechanisms for durable cease-fires—it reduced uncertainty about intent and actions and it mitigated the risks of involuntary escalation. However, it did not appear to alter the incentives to make violations unattractive. As the authors note:

> For the conflict parties…uncertainty about what happened on the ground was not the key obstacle to conflict settlement. Instead, cease-fire violations often served to turn up the heat in reaction to political tensions, and each side appeared convinced of the other's bad faith…which events from February 2022 onward [the Russian invasion of Ukraine] seem to affirm.

[52] Organization for Security Co-operation in Europe (OSCE), Special Monitoring Mission to Ukraine (SMM), https://www.osce.org/special-monitoring-mission-to-ukraine-closed (accessed May 2, 2023).

In this case, more "certainty about cease-fire violations [did] little to shape perceptions of intent and resolve."[53] In other words, cease-fire monitoring through digital technologies provided valuable information and allowed for improved monitor protections, but the technology use and resulting information was not enough to keep the peace.

Recommendations. The authors remind the reader that the OSCE mission in Ukraine "was considered a model to emulate in other cease-fire monitoring contexts"—until the Russian invasion in 2022. While they emphasize the benefits of technologies in the cease-fire missions, they caution:

> technical data gathered by technological means lack the narrative dimension that might enable actors to determine resolve and intent. Most importantly, remote sensing technology does not change the fundamental problem that cease-fire monitoring missions face in contexts where parties lack the intent to fully comply with a cease-fire, and where third parties are not willing or able to sanction violations in a way that would change the cost–benefit analysis of cease-fire compliance.

In other words, technology may aid in conflict resolution, but it will not, by itself, make and keep the peace.

This Lesson's ideas and quotes derive from the paper indicated below, except as otherwise noted:
Andreas T. Hirblinger, Martin Wählisch, Kate Keator, Chris McNaboe, Allard Duursma, John Karlsrud, Valerie Sticher, Aly Verjee, Tetiana Kyselova, Chris M. A. Kwaja, Suda Perera, "Forum: Making Peace with Un-Certainty: Reflections on the Role of Digital Technology in Peace Processes beyond the Data Hype," International Studies Perspectives*, 2023, https://doi.org/10.1093/isp/ekad004 (accessed April 24, 2023).*

China, Peacekeeping, and the Information Advantage: The US Must Respond, JLLIS #230901-5134

Observation. In the past two decades, China's support to United Nations (UN) peacekeeping has grown significantly. Beijing is now the second largest financial funder to the UN peacekeeping budget and tenth largest troop contributor – providing more personnel to peace operations than any other member of the permanent Security Council.[54] Strong participation in UN peace operations is an ideal mechanism for China to "exert diplomatic and political influence globally."[55]

To this end, China effectively uses the information environment to amplify its growing role in peacekeeping, establish its reputation as a responsible and constructive global power, and ease international concerns of it as a hegemonic threat. Specifically, Beijing seeks to leverage its peacekeeping achievements to gradually erode United States (US) and ally influence, position itself as a leader in UN peacekeeping operations, and advance its own discrete foreign policy objectives. Therefore, U.S. civilian and military leaders of peacekeeping and stabilization operations must recognize China's core motivations in the collective security environment and be prepared to develop and apply appropriate mitigation measures in planning and execution. Specifically, peacekeeping is a valuable area where the US government still has a strong comparative advantage relative to China and "can achieve strategic effects in support of national competitive strategies."[56]

---

[53] OSCE, Special Monitoring Mission to Ukraine (SMM).
[54] "Troop and Police Contributors," United Nations Peacekeeping, https://peacekeeping.un.org/en/troop-and-police-contributors (accessed September 11, 2023); Luisa Blanchfield, *United Nations Issues: U.S. Funding of U.N. Peacekeeping*, (Washington, DC: Congressional Research Service, January 20, 2023), 1, https://crsreports.congress.gov/product/pdf/IF/IF10597/21 (accessed September 11, 2023).
[55] ChinaPower, "Is China Contributing to the United Nations' Mission?" *Center for Strategic and International Studies*, https://chinapower.csis.org/china-un-mission/ (accessed September 11, 2023).
[56] Joint Chiefs of Staff, *Joint Concept for Competing* (Washington, DC: Joint Chiefs of Staff, 2023), 18.

If the US does not design and execute a timely engagement plan to counter Chinese peacekeeping propaganda, then the Chinese disinformation messaging campaign could undermine UN mission effectiveness, as well as negatively affect US interests and erode broader international peacekeeping norms.

Discussion. Official justifications for China's participation in peacekeeping operations highlight its commitment to global peace and stability and confirm to the international community Beijing is a global leader, dutifully fulfilling its *Great Power* responsibilities. For several years now, Chinese officials describe Beijing's support to peacekeeping as a natural output of its increased participation in global governance. In 2006, China's UN Ambassador Wang Guangya declared that as "major powers are withdrawing from the peacekeeping role…China felt it is the right time for us to fill this vacuum."[57] In September 2015 at the UN Leader's Summit on Peacekeeping, Chinese President Xi Jinping pledged to commit 8,000 troops for a UN standby force, join the UN peacekeeping capability readiness system, and promised $100 million in military assistance to the African Union to support the creation of an African standby force for crisis response.[58] So far, it appears China is following through on its promises. They registered the 8,000-troop standby force with the UN, and actively contribute personnel and materiel to missions as well as maintain its financial commitments.[59]

In September 2020, China commemorated the 30th anniversary of its contributions in UN peacekeeping by issuing its first-ever official *white paper* on the topic.[60] It is primarily a strategic messaging document that highlights China's past successes and outlines its six principles in UN peacekeeping: uphold the purposes and principles of the UN Charter; follow the basic principles of UN peacekeeping operations; champion a vision of global governance based on extensive consultation, joint contribution, and shared benefits; pursue common, comprehensive, cooperative, and sustainable security; stay committed to peaceful means in settling disputes; and build stronger peacekeeping partnerships.[61]

In recent months, Beijing distributed a short English language promotional film on its Ministry of National Defense website (and now on YouTube) called "Here I Am," depicting its People's Liberation Army as a benevolent force that upholds justice and peace.[62] The two-minute video is a combination of live-footage and animation that depicts China's military achievements in UN peacekeeping. While the video's declarations may seem far-fetched to some, it is good publicity. Chinese media and government officials portray these deployments as a positive investment of the country's promise to support multilateral international peace and stability missions.

---

[57] Colum Lynch, "China Filling Void Left by West in U.N. Peacekeeping," *Washington Post*, November 24, 2006, https://www.washingtonpost.com/wp-dyn/content/article/2006/11/23/AR2006112301007.html; James Siebens and Ryan Lucas, "Military Operations Other Than War in China's Foreign Policy," *The Stimson Center*, (2022): 40, https://www.stimson.org/2022/military-operations-other-than-war-and-chinas-foreign-policy/.

[58] Michael Martina and David Brunnstrom, "China's Xi says to commit 8,000 troops for U.N. peacekeeping force," *Reuters*, September 28, 2015, https://www.reuters.com/article/us-un-assembly-china/chinas-xi-says-to-commit-8000-troops-for-u-n-peacekeeping-force-idUSKCN0RS1Z120150929.

[59] Sarah Zheng, "China completes registration of 8,000-strong UN peacekeeping force, defence ministry says," *South China Morning Post*, September 29, 2017, https://www.scmp.com/news/china/diplomacy-defence/article/2113436/china-completes-registration-8000-strong-un.

[60] The State Council Information Office of the People's Republic of China, "China's Armed Forces: 30 Years of Peacekeeping Operations," September 18, 2020, https://english.www.gov.cn/archive/whitepaper/202009/18/content_WS5f6449a8c6d0f7257693c323.html#:~:text=Over%20the%20past%2030%20years,world%20peace%20and%20common%20development; Mauro Barelli, "China and Peacekeeping: Unfolding the Political and Legal Complexities of an Ambivalent Relationship," *Asian Journal of International Law* 12, (January 2022): 157, https://www.cambridge.org/core/journals/asian-journal-of-international-law/article/china-and-peacekeeping-unfolding-the-political-and-legal-complexities-of-an-ambivalent-relationship/DABD14E52185E870C96E9A7894C872CA.

[61] The State Council Information Office, "China's Armed Forces."

[62] China Ministry of National Defense, "Here I Am," http://eng.mod.gov.cn/xb/News_213114/Videos/16228815.html (accessed September 21, 2023); Sarah Sicard, "Propaganda film casts Chinese Army as saintly liberators," *Military Times*, June 7, 2023, https://www.militarytimes.com/off-duty/military-culture/2023/06/07/propaganda-film-casts-chinese-army-as-saintly-liberators/.

Lastly, the Chinese government leverages the United Nations Association-China (UNA-China), a self-proclaimed non-governmental organization to advance and memorialize China's UN peacekeeping accomplishments.[63] China steadily promotes its role in peace missions as a "force of justice for world peace and development," and "China's diplomatic calling card."[64] However, China's support to UN peacekeeping provides it a low risk means to gain operational experience and exposure to a range of missions, train and become proficient on military pre/post deployment activities, understand logistical challenges to support an overseas presence, build multilateral cooperation, and strengthen host country relations.[65]

In the meantime, the US government and international community have yet to openly respond to Chinese claims and has no comparative websites or videos. It rarely makes public pronouncements or touts its longstanding support to UN peacekeeping or global stability writ large. For example, the US Military Observer Group (USMOG) – the Department of Defense focal point for military members serving in the UN – does not have a social media presence and the Department of State has few online articles or news updates announcing its successes in support of UN peacekeeping.

Yet, the US has a story to tell. It has a long history of funding, materiel provision, and training support to UN peace operations – these accomplishments should be known. Since the first mission in 1948, the US remains the largest financial contributor to UN peacekeeping at roughly $2.5 billion per year.[66] In addition to its enormous financial commitments, the US leads in the training and equipment to assist partner nations develop the key enabling capabilities to sustain peacekeeping proficiencies. This is accomplished through efforts such as the US State Department-led Global Peace Operations Initiative (GPOI) and the African Peacekeeping Rapid Response Partnership.[67] With a total budget of more than $1.4 billion from fiscal years 2005-2022, these programs provide a critical funding activity to prevent personnel readiness shortfalls in UN peace operations.[68]

Recommendations. The US government should be open and transparent of its UN peacekeeping support. It should develop a comprehensive and active engagement plan to communicate all the ways it contributes to UN peacekeeping operations. A frequent broadcast of these milestones on US government social media accounts and public-facing internet webpages is a low-cost strategic investment that will enable the US to enhance its image and effectively use peacekeeping as a tool to advance its key national security and foreign policy objectives.

Moreover, publicly published US peacekeeping themes and messages may encourage its geographic Combatant Commanders to develop complementary talking points. This, in turn, will foster better relations and increase US credibility when it engages in bilateral discussions with major UN peacekeeping troop contributing countries.[69] Further, the preponderance of these large troop contributors is the Indo-Pacific and Africa – two strategically important regions to US security interests. This messaging should also emphasize the importance of upholding Western-backed peacekeeping norms – protecting civilians,

---

[63] United Nations Association-China, "Home Page," https://www.unachina.org/en/ (accessed September 3, 2023).
[64] Siebens and Lucas "Military Operations," 38.
[65] ChinaPower, "Is China Contributing;" Siebens and Lucas "Military Operations," 39.
[66] Antony J. Blinken, Press Statement "International Day of UN Peacekeepers," May 29, 2023, https://www.state.gov/international-day-of-un-peacekeepers-2/#:~:text=This%20May%2029th%2C%20on%20the,to%20international%20peace%20and%20security; Heather Peterson, "U.N. Peacekeeping Is a Good Deal for the U.S.," *TheRandBlog*, April 2, 2017, https://www.rand.org/blog/2017/04/un-peacekeeping-is-a-good-deal-for-the-us.html.
[67] "Key Topics – Office of Global Programs and Initiatives," U.S. Department of State, https://www.state.gov/key-topics-office-of-global-programs-and-initiatives/ (accessed September 11, 2023).
[68] U.S. Department of State, "Key Topics – Office of Global Programs and Initiatives," https://www.state.gov/key-topics-office-of-global-programs-and-initiatives/ (accessed September 11, 2023).
[69] Interview with U.S. military officer with responsibilities for UN peacekeeping, September 2023.

monitoring and preventing human rights violations, and pursuing governance and security sector reforms.[70]

The Department of State Global Engagement Center is best suited for this engagement plan as it is chartered to direct, lead, and coordinate US interagency efforts to proactively address foreign adversary attempts to undermine US interests.[71] In addition, the recently formed State Department Office of China Coordination (also known as the "China House") has a critical role to oversee coordination among the US diplomatic corps on managing competition with China beyond the Indo-Pacific region and to uphold an open, inclusive international system.[72]

The US is doing its part—if not more—in support of UN peacekeeping efforts. It must respond to China's influence or be left behind.

Lesson Author: Lieutenant Colonel Claude A. Lambert is a U.S. Army Strategic Plans and Policy Officer. He is currently serves as a United States Army War College Fellow and Visting Scholar at the Stanford University Center for International Security and Cooperation.

Improving Information Advantage: Local Political Analysis Systems, JLLIS #230901-5141

Observation. Too often donor officials and multilateral organizations invest in conflict affected contexts – holding workshops and trainings, building infrastructure, or conducting military operations –with an incomplete picture of the key political dynamics at play. Current analysis (such as internal reporting from those implementing programs or external research from academics or Non-Governmental Organizations, or NGOs) give some insights but have important limits, which can mean officials making billion Euro decisions about peacekeeping and stability operations are doing so partly in the dark.

GPPi spent a year examining this dark area. Through over 60 interviews with policymakers (mostly German, British and US government officials), practitioners and contractors, we identified key deficiencies of current analysis. Importantly, most information feeding operation decision-making rarely does three essential things simultaneously, further discussed below.

In the future, this gap in analysis is likely to have an even more profound impact on operations. Countless strategic whitepapers from every major donor – including the United Nations (UN)[73], the United States (US)[74], the United Kingdom (UK)[75], and Germany[76] –note that stabilization programming needs to shape

[70] Bryce Loidolt, "Doing Well by Doing Good? Strategic Competition and United Nations Peacekeeping," ed. Denise Natali, *Institute for National Strategic Studies Strategic Perspectives*, no. 36 (September 2021): 3, https://inss.ndu.edu/Portals/82/Documents/Strategic%20Perspectives/Strategic-Perspectives-36.pdf (accessed September 3, 2023).
[71] United States Department of State, "Global Engagement Center," https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (accessed September 3, 2023).
[72] United States Department of State, "Secretary Blinken Launches the Office of China Coordination," December 16, 2022, https://www.state.gov/secretary-blinken-launches-the-office-of-china-coordination/(accessed September 3, 2023).
[73] United Nations Peacebuilding Fund (2020), "Secretary General's Peacebuilding Fund: 2020-2024 Strategy" (United Nations, March 2020), https://www.un.org/peacebuilding/sites/www.un.org.peacebuilding/files/documents/pbf_strategy_2020-2024_final.pdf%20 (accessed September 30, 2023).
[74] Bureau of Conflict and Stabilization Operation (2022), "2022 Prologue to the United States Strategy to Prevent Conflict and Promote Stability," (United States Department of State, April 1, 2022), https://www.state.gov/2022-prologue-to-the-%20united-states-strategy-to-prevent-conflict-and-promote-stability/ (accessed September 30, 2023).
[75] "Conflict, Stability and Security Fund: Annual Report 2021 to 2022," UK Government, https://www.gov.uk/government/publications/conflict-stability-and-security-fund-annual-report-2021-to-2022 (accessed July 17, 2023).
[76] German Federal Foreign Office (2022) "Shaping Stabilisation: Foreign and Security Policy Concept for an Integrated Action for Peace" (German Federal Foreign Office, December 2022), https://www.auswaertiges-

the political environment, be willing to take risks and be adaptive and flexible. All of this necessitates better, timelier, and more granular analysis.

Discussion. The three key deficiencies of current analysis are as follows:

One, a need for key information about hard-to-reach and potentially dangerous areas. The geographic and social distance (in terms of language, culture and lived experience) between long-marginalized communities and life in capital cities is rarely bridged by researchers. Because of that, their findings seldom represent the reality in areas where programming could be most useful.

Two, the necessity of actionable and timely analysis to inform decision-making. Much published reporting is too late or in a fashion – academic papers, for example – that busy officials find hard to absorb and use.

Finally, there is a requirement to triangulate data and counter *blind spots* or conflicts of interest at the local level. Often, implementers working on programs in a certain area are the ones who are physically closest to the action – but they are usually in a weak position when it comes to reporting about realities that the respective local authorities (or an armed group) would rather not see relayed to donors.

The good news is that systems exist that could address this problem, with the right investment. Our own research focused on the benefits of a model we refer to as *local political analysis systems* (outlined below), which attempt to address the three essential gaps in current analysis simultaneously: providing timely, reliable data from hard to reach and violent places. Unfortunately, these systems remain an exception as they are undertaken mostly as pilot programs with limited financial, staff or political investment.

In our recent paper ("Close the Gap: How to Leverage Local Analysis for Stabilization and Peacebuilding," pending publication'), we examine how these systems could be further developed and deployed to improve strategic decision-making in peacebuilding and stabilization missions. Several governments (such as the US, the UK and Germany) commissioned private companies[77] to undertake analysis of local conflict dynamics on a frequent basis in, among other places, Afghanistan[78], Somalia[79], Libya, Ukraine, Syria, the Sahel, and Honduras. These systems use many of the same techniques as development or humanitarian third party monitoring (TPM), such as opinion surveys (conducted by telephone or face-to-face and varying from "yes"/"no" questions to semi-structured interviews), expert interviews (with community leaders or local experts), researchers in the area (conducting individual interviews or group discussions), evaluation of social and traditional media, stakeholder mapping, tracking outbreaks of violence and political context analysis.[80] However, they are distinct from the bulk of TPM in three ways. First, the focus is the politics of conflict rather than humanitarian needs or program outputs. Second, coverage is provided more continuously, as frequently as useful and feasible (for instance, monthly cycles for simpler questions, 6-monthly or annual for more demanding analyses). Third, they provide analytical

amt.de/blob/2586726/4810ccbbc8aa4d2140817311f68afe74/aussen--und-sicherheitspolitisches-konzept-fuer-ein-integriertes-friedensengagement-data.pdf (accessed September 30, 2023).

[77] These companies usually employ researchers based in the region, though unfortunately sometimes only from the national capitals.

[78] Stabilisation Unit, "Monitoring and Evaluation of Conflict and Stabilisation Interventions: What Works Series," *Government of the United Kingdom*, October 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765613/What_Works_-_Monitoring_and_Evaluation_of_Conflict_and_Stabilisation_Interventions.pdf (accessed September 30, 2023).

[79] Ibid.

[80] Julia Steets and Elias Sagmeister, "The Use of Third-Party Monitoring in Insecure Contexts," *GPPi*, November 9, 2016, https://gppi.net/2016/11/09/the-use-of-third-party-monitoring-in-insecure-contexts; Stephanie Diepeveen, John Bryant, Farhia Mohamud, Mahad Wasuge, and Hassan Guled, "Data sharing and third- party monitoring in humanitarian response," *ODI*, September 14, 2022, https://odi.org/en/publications/data-sharing- and-third-party-monitoring-in-humanitarian-response/ (accessed September 30, 2023).

products rather than just data, recognizing how contextually specific it is to accurately interpret seemingly objective observations, without infringing upon the exclusive authority of policy makers to take strategic decisions.

Tracking data on a regular basis allows some local analysis systems to gather information about how key conflict trends change over time, such as social cohesion, faith in government, prevalence of non-state and competency of state forces. This is not just a technical addition to programming but is fundamental to improving all aspects of how strategies are developed and delivered. When used effectively, local political analysis can enable better stabilization and peacekeeping programming. In our own research, we found examples of these systems used to do four key things:

First, they can inform investment decisions, including which actors are likely to share the same strategic goals, which issues are most pivotal or which geographic areas are more open to change.

Second, they can enable the continuation of programming in violent areas or in places overtaken by violent proscribed groups by providing regular and granular data on the local context to help manage risks.

Third, they can build collective understanding between different departments and key diplomatic, defense and development stakeholders by providing a shared evidence base on which to debate, discuss and decide together.

Finally, they can improve diplomatic engagements by providing alternative perspectives to elites and tracking perceptions from different geographic areas, ethnic groups, and potentially marginalized communities to better understand and navigate conflict trends.

Despite the potential of these systems, our interviews along the 'production chain' from contractors, analysts and policy officials suggest that governments have yet to make the leap from developing pilot or experimental local analysis systems, to deploying them as standard parts of the stabilization toolkit. There appear to be four interrelated barriers to the effective use of local political analysis for decision-making in stabilization and peacebuilding interventions:

First, these systems are perceived as a tentative, experimental approach, which has made it difficult to secure consistent and reliable investment. When built too small or for short time horizons only, however, local political analysis systems are set up to fail.

Second, where investments happened at a promising scale, strategic direction has sometimes gotten lost. Without clear guidance from decision-makers, the analytical output produced by analytical mechanisms became more of a burden to those same decision-makers than an effective way of empowering them. This was true even for powerful new analysis systems.

Third, to effectively steer and frequently adapt their programs, officials must effectively translate highly localized analytical findings to the needs of political decision-makers in ways that avoid overwhelming the latter with more information than they can process, and without compromising their decision-making autonomy. This is both a translation challenge and a resource challenge: if decision-makers are insufficiently equipped (in terms of staff) to understand and engage even with well-aggregated, well-presented analysis, that information will be left unused. That makes it not just pointless to generate that information in the first place, it also becomes dangerously irresponsible for external actors to run interventions in volatile conflict spaces while flying at least half-blind.

Fourth and finally, local political analysis works only if decision-makers can act on it; that is, if they adapt their policy interventions and programming. When the information output produced by granular local

analysis systems outpaces the adaptiveness and flexibility of the programs themselves, meaning decision-makers cannot act on the information in a timely manner, it becomes politically undesirable for them to identify problems or opportunities in the first place. At worst, the result can be a vicious cycle of "I don't want to know what I cannot change" and "I cannot change what I do not know."

Recommendations. These barriers are not inevitable but need sustained investment to overcome; therefore, donors and major multilateral intermediaries need to improve their approach everywhere. This is particularly important where there is a "triple gap" in community-level political awareness, that is, where: (1) the operating environment or a key part of it is remote, dangerous and volatile; (2) existing sources of actionable and reliable political analysis do not suffice; and (3) the international institution itself has an important stake in steering the joint international intervention to maximize impact and/or minimize unintended effects. In these areas, we present as a step-by-step guide to setting up and using effective local political analysis for adaptive stabilization and peacebuilding:

First, custom-tailor (and resource) local political analysis system together with its intervention. Such a system will only be effective if sufficiently resourced for a clearly defined purpose, and if its outputs are used effectively for adaptive programming. How much it costs to have "sufficient resources" will depend on the context, the purpose, and the requirements for making its analytical products actionable for policymakers steering the adaptive programs.

Second, define steering goals, analytical indicators, and decision-making mechanisms. Along with the goals and adaptive mechanisms of the intervention itself (country, subnational or regional strategy), it is key to clearly define how the evidence from local political analysis will help to achieve their goals (including interim steps, how evidence serves to support the key steps necessary to achieving longer term goals).

Third, assign clear ownership of who does what: There are four key questions which need to be answered, and to which there are likely to be different answers for every country or regional context and/or donor: Who controls the system as a whole? Who collects the data? Who analyzes the data? Who translates the data into actionable information? Who decides based on the evidence?

Lastly, assign the necessary staff and financial resources to not just produce, but also to use the data: Local political analysis does not just cost whatever the budget of any external entity procuring the data, but also the staff capacity to translate community-level political observations into actionable information, the staff capacity to take key decisions for steering the overall intervention, and the staff capacity to manage the continuous review and adaptation of the local political analysis system – its goals, analytical requirements or indicators, processing and product design – itself.

Lesson Authors: Philipp Rotmann is a director of the Global Public Policy Institute (GPPi) in Berlin, where he leads the work on peace and security. His interests include how to better anticipate, prevent, and reduce mass violence, including through peace operations, stabilization programs, improving security governance, monitoring and evaluation, and how Germany and the European Union could contribute more effectively to these efforts. His latest book is "Krieg vor der Haustür: Die Gewalt in Europas Nachbarschaft und was wir dagegen tun können" written with Sarah Brockmeier. He is a member of the German Federal Foreign Office's independent evaluation panel and co-directs GPPi's PeaceLab project.

Abi Watson is a research fellow at GPPi, where she contributes to the institute's work on peace and security, specifically on understanding stabilization programs. Her interests include security force assistance, light footprint military operations, and British foreign and defense policy. She is part of the core team for the Stabilization Lab project. Before joining GPPi, Abi was a conflict and security policy coordinator at Saferworld and a research manager at the Oxford Research Group.

This Lesson is based on their pending publication of their research, "Close the Gap: How to Leverage Local Analysis for Stabilization and Peacebuilding," due for release October 2023.

Educating Government Employees for the Information Environment, JLLIS #230901-5143

Observation. Thirty years ago, the US Army did not have a professional cadre of information practitioners. Today, it does. However, few of these practitioners achieve rank above the grade of colonel. Consequently, although the US Army now has leadership advisors for information issues, these practitioners are not the decision-makers. At the same time, to counter malign actor advances on the information field, the US Army invests in people, resources, and management of the information domain. A key component of that investment is the post-graduate education of US Army officers at the Command & General Staff College (CGSC) and the Army War College (AWC). Increased emphasis on core curricula lessons (common instruction given to all students), electives and specialized study tracks at both institutions will increase the US Army's ability to field a force to successfully compete with adversaries for control of information, particularly at levels below large-scale conflict.

The US Army—and the US government writ large—must continue to codify Information Activities into its education system. Education is the opportunity to ground fundamental knowledge in an organization, which better prepares it to face current and evolving challenges. This is particularly true in a rapidly changing field such as information.

Discussion. The information environment is a critical field of competition for modern nation-states and non-state actors, particularly those engaged in peacekeeping and stability operations. The ability to influence both mass audiences and individuals over a variety of modern media is expanding at a dizzying pace. This cacophony of information vectors is generated by many government and non-government entities; several of which routinely disseminate misinformation and disinformation. International disputes and conflicts ranging from Ukraine to Korea demonstrate the ability of information to help or hinder nations as they pursue their national security goals.

What role should a government play in furthering or countering these activities, particularly its armed services? For the US, the 2022 *National Defense Strategy* states, "To strengthen deterrence while managing escalation risks, the Department (of Defense) will enhance its ability to operate in the information domain."[81] At the military service level, the US Army, Navy and Air Force each have graduate-level institutions for ongoing, focused education of their officer corps. It is this system that provides an opportunity to meet the intent of the Joint Staff and educate its future leaders to understand the role of information in helping secure U.S. national security objectives. They may serve as models for other government education programs in this field.

Problem resolution begins with problem understanding. The professional military education (PME) program for US Army's mid-grade officers is where this understanding occurs. The Joint Staff provides education guidance in the form of Special Areas of Emphasis (SAEs) expected to be integrated into curricula at all levels. A Joint Staff Memorandum on this topic dated May 6, 2019, lists six SAEs. The second SAE listed is Globally Integrated Operations in the Information Environment. The memorandum goes on to stipulate that, "JPME curriculums should provide students with the following knowledge:

1) The importance of understanding human, physical and informational aspects of the security environment.
2) How to formulate options that integrate informational and physical capabilities and activities.
3) How the Joint Force executes operations in the information environment and modifies those operations as audiences respond."[82]

Core curricula forms the bulk of contact time in both schools and includes instruction on US Army forces, resources, and techniques available to operate in and influence the information environment. Instruction

[81] U.S. Department of Defense, *2022 National Defense Strategy*, p. 9. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-national-defense-strategy-npr-mdr.pdf (accessed November 11, 2022).
[82] U.S. Joint Chiefs of Staff, *Special Areas of Emphasis for Joint Professional Military Education in Academic Years 2020 and 2021*, 6 May 2019, p. 2. https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jpme_sae_2020_2021.pdf (accessed November 12, 2022).

can include lectures, guest speakers and exercise practicum, although the intent is for learning to occur primarily through the Socratic method.

Fig 1. AWC IO Instructional Slide

In Academic Year 2022, the US Army War College had one three-hour block of instruction titled "Special Operations Forces and Information Operations." (See Fig 1) The lesson authors were former Information Operations (IO) practitioners, but all faculty conducted instruction. The instruction described cognition, joint doctrine regarding employment, and Army force structure available for IO.

The CGSC AY23 core curriculum features a two-hour block of instruction titled M333 "Information Advantage," with the objective described as, "…to understand the Army's doctrine regarding information and achieving information advantage and applying information doctrine to the planning and execution of large-scale ground combat operations." The first hour of the lesson introduces the foundational Army doctrinal concepts and discusses the nature of the information domain. The second hour includes a practicum for student opportunity to apply their knowledge against a tactical problem.

In both schools, electives provide opportunity for students to delve deeper into various details of information. The information elective developed at AWC, *WF 2303 Joint Warfighters in the Information Environment*, while not intended to create certified IO practitioners, goes deeper into the topics raised during the curriculum lesson for those with an interest in the field.

At CGSC, the Department of Tactics hosts A323 *Army IO Planning*. The syllabus describes it as a course of instruction in, "…Army Information Operations doctrine at the tactical echelons. Students will learn to plan, integrate, synchronize, coordinate and assess IO to support an approved course of action, line of effort, or named operation." Like the AWC elective offering, the course does not create certified IO practitioners: rather, it gives interested officers more study for integrating information into the work of their own specialties at a tactical to high-tactical level of warfighting in the information domain.

In addition to the education opportunities discussed above, CGSC offers an Information Scholar's Program to qualified students. Students compete for the program in November: those selected are placed into a dedicated seminar for the remainder of the academic year. According to the program syllabus, the goal is to, "…offer a select group of students a range of accelerated, rigorous, graduate-level studies that promote analysis, stimulate the desire for learning, and reinforce academic research skills. Information Advantage Scholars strive to understand the complexities inherent in the integration of information technology in the joint force and the importance of compelling narratives to achieve operational success."

AWC has introduced an electives information concentration that would encompass taking WF 2303 *Joint Warfighters in the Information Environment* along with other information-related electives such as *Cyber Operations* or *Military Deception*. Students who meet the requirement would receive a certificate of completion upon graduation. Much of the challenge comes from deconflicting the applicable electives to enable students interested in the concentration to take all offerings. There are three elective terms: because of the small size of the AWC faculty, they can usually only offer an elective once per academic year. If any of these electives are offered in the same term, then an interested student will be unable to take both.

In both colleges there is a continuing debate over whether to run electives as classified. The advantage is that it allows faculty to bring in additional learning materials and scenarios based on real-world situations. The disadvantages are that special facilities are required to conduct classified classes, and that classification would exclude international students. For courses of this length and depth, there seem to be ample open-source materials available to achieve the course intent.

Recommendations. The US government must consider the means to educate its workforce in Information Activities and operating in the Information Environment to better prepares it for the rapidly changing field such as information. The curricula found in the US Army's two mid-grade professional education programs serves as a model for this effort.

Lesson Author: Dr. J.R. Reiling, U.S. Army, Retired, is a former US Army Psychological Operations officer and currently serves as an Assistant Professor in the Department of Joint, Interagency and Multinational Operations at the Command and General Staff College at Fort Leavenworth, Kansas. He holds a PhD in International Relations from Old Dominion University, Virginia. In his military career, he deployed in support of conventional and special operations forces in Saudi Arabia, Afghanistan, and Iraq. This Lesson is based on his submitted essay, "Educating US Army Officers To Operate In The Information Environment."

Policies and Governance

International Norm Development for Information Sharing, JLLIS # 230700-4601

Observation. As the UN's Department of Economic and Social Affairs (DESA) asserts, "Knowledge-sharing is a superpower."[83] This may be especially true in the multinational peace or peace-related military operations in which the UN commits forces. However, a dearth of internationally agreed upon policies and procedures for data and information sharing among partners may be the *Kryptonite* for that superpower.

According to the United Nations (UN) news website, in July 2023, Secretary-General António Guterres spoke at the first United Nations (UN) Security Council (UNSC) meeting about Artificial Intelligence (AI) and international governance of the same. As the site reports:

> The best approach, he went on to say, would address existing challenges while also creating the capacity to monitor and respond to future risks. *The need for global standards and approaches makes the United Nations the ideal place for this to happen*, and he therefore welcomed calls from some Member States to create a new United Nations entity to support collective efforts to govern this technology.[84] [Emphasis added]

While the availability and rise of AI utilization may be the most dramatic global adoption of technology to date[85], it is not the only area of information technology that needs codified international norms or the reform of national approaches to sharing amongst partners for greater efficiencies.

Discussion. Some international and regional organizations are already reevaluating their information sharing processes.[86] Gordon Davis, writing for the *Atlantic Council* in March 2023, notes the North Atlantic Treaty Organization's (NATO) 2022 Madrid Summit recommendations about sharing, derived from Russian invasion in Ukraine. One lesson he emphasizes is the "outsized role" of private industry "in

[83] UN's Department of Economic and Social Affairs (DESA), DESA's Digital Learning Center, https://www.un.org/en/desa/knowledge-sharing-superpower (accessed August 23, 2023).
[84] United Nations News, *International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards*, July 18, 2023, https://press.un.org/en/2023/sc15359.doc.htm (accessed July 20, 2023).
[85] Ibid. The article shares further: "Noting that this technology has been compared to the printing press, he observed that — while it took more than 50 years for printed books to become widely available across Europe — "ChatGPT reached 100 million users in just two months."" For more about international norm development specific for AI, see: Pragya Jain, "The Importance of International Norms in Artificial Intelligence Ethics," *Council on Foreign Relations*, August 10, 2022, https://www.cfr.org/blog/importance-international-norms-artificial-intelligence-ethics (accessed August 14, 2023).
[86] For this Lesson, the term *information sharing* covers all examples of data exchange, to include intelligence products, between operational partners.

enabling the Ukrainian response to the Russian aggression."[87] Another lesson he highlights is the interrelationship of "Digitalization, connectivity, and Big Data":

> More comprehensive intelligence analysis (as well as research in general) has long been hampered by several limitations: the number of documents or signals available in digital form, disconnected private and public data silos containing exploitable information, *the lack of common protocols and interfaces to access and share data*, and *the lack of data management tools* in general. While data management and cloud services have become the norm in the private sector, the public defense sector has been wary and slow to adopt. But necessity is the mother of invention and Ukraine is a particularly relevant proving ground.[88] [Emphasis added]

Well before the Russian invasion, the U.S. intelligence community also advocated greater information sharing among partners. As *Voice of America* reports, "U.S. intelligence agencies are looking to vastly expand the roster of countries, companies and even nonstate actors with whom they partner in order to get — and share — information on threats to the United States and its allies."[89] This approach acknowledges "a range of threats that are no longer limited to traditional nation-state competitors such as China and Russia or terrorist groups such as al-Qaida and the Islamic State group."[90] More specifically,

> the strategy envisions U.S. intelligence agencies exchanging information with private companies and what it describes as "nonstate and subnational actors." That includes relationships with nongovernmental organizations, think tanks and other entities that could help provide the U.S. intelligence with local or on-the-ground expertise.[91]

The *International Committee of the Red Cross* (ICRC) also advocates for more information sharing between partners, to include between humanitarian organizations and donors. While noting that data exchanges are "namely for the improved coordination, accountability, transparency, and efficiency of their operations," they also caution "Each partner may have different obligations that need to be observed" for governing and protecting data.[92] Further,

> The potential or perceived use of humanitarian data for non-humanitarian purposes could also put affected populations at risk of harm and undermine trust between humanitarians and the people they seek to serve. Anticipating and mitigating such risks is key to principled humanitarian action. *Getting this right requires collective action across the system*.[93] [Emphasis added]

---

[87] Gordon B. Davis Jr., "The future of NATO C4ISR: Assessment and recommendations after Madrid," *The Atlantic Council*, March 16, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-future-of-nato-c4isr-assessment-and-recommendations-after-madrid/#recommendations-share-transform-implement-modernize-and-invest (accessed August 19, 2023).

[88] Davis, "The future of NATO C4ISR: Assessment and recommendations after Madrid." C4ISR stands for Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR).

[89] Jeff Seldin, "New US Intelligence Strategy Calls for More Partners, More Sharing," *Voice of America News*, August 10, 2023, https://www.voanews.com/a/new-us-intelligence-strategy-calls-for-more-partners-more-sharing-/7220725.html (accessed August 18, 2023).

[90] Ibid.

[91] Ibid. See Office of the Director of National Intelligence, *National Intelligence Strategy, 2023*, https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf (accessed August 20, 2023).

[92] Vincent Cassard, Stuart Campo, and Jonas Belina, "Responsible data sharing between humanitarian organizations and donors: towards a common approach," *International Committee of the Red Cross*, June 22, 2023, https://blogs.icrc.org/law-and-policy/2023/06/22/responsible-data-sharing-humanitarian-organizations-common-approach/ (accessed August 5, 2023).

[93] Ibid. The authors note some frameworks already exist by and for humanitarian organizations, such as the Inter-Agency Standing Committee (IASC) *Operational Guidance on Data Responsibility in Humanitarian Action* and the ICRC *Handbook on Data Protection in Humanitarian Action*.

Recommendations. While there may not be international norms for information sharing in the general sense, many specific entities/functions, such as health and medicine and/or scientific research, have developed data governance guidelines/frameworks/principles for their own work.[94] For example, in a meeting convened by the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data, the ICRC worked with the Humanitarian Data and Trust Initiative (HDTI) to develop a six-guideline framework for information sharing between agencies and donors. Summarized and paraphrased here, the guidelines are:

- *Humanity*. Donors and humanitarian organizations should work to ensure that data sharing processes keep affected people at the center.
- *Clear communication of the purpose*. Whenever data is requested or shared, the reasons for doing so should be clearly articulated.
- *Common requirements for responsibility*. Formalizing these technical and procedural requirements at the outset of a partnership allows for consistent engagement and monitoring over time.
- *Common approach to potential risks*. Humanitarian organizations and donors should collaborate to identify potential risks and mitigation measures throughout the course of the data sharing activity.
- *Invest in training and procedures*. Humanitarian organizations and donors should work together to provide their staff with clear instructions on how the framework applies in different operational settings.
- *Learning and accountability initiatives*. Humanitarian organizations and donors should support inter-sectoral collaboration and research to advance knowledge in this area.[95]

In a second example, the UN Development Programme (UNDP) offers *eight data principles* for their own work. Five of these principles reflect the *OCHA's Principled Framework*: *Safeguard personal data*; *Uphold the highest ethical standards*; *Manage data responsibly*; *Empower people to work with data*; and *Expand frontiers of data*.[96] However, three of them are unique: *Make data open by default*; *Plan for reusability and interoperability*; and *Be aware of data limitations*.[97]

Regardless of the function, authors for *Data & Policy* journal suggest, "global governance may be beneficial…particularly on (a) global coordination to prevent harmful fragmentation, (b) the advancement of global principles and values, and (c) using data as a resource to advance global public goods."[98] Among their several recommendations, one stands out as most relevant to multinational and/or partnered operations:

> *Translate values and recommendations into practical tools*: In collaboration with diverse policymakers and stakeholders, identify the most valuable tools to facilitate and accelerate the

[94] Another example is: United Nations Office for the Coordination of Humanitarian Affairs (OCHA), "Information Sharing Protocol Ukraine, 17 May 2023," May 23, 2023, https://reliefweb.int/report/ukraine/information-sharing-protocol-ukraine-17-may-2023-enuk (accessed August 26, 2023).
[95] United Nations *Office for the Coordination of Humanitarian Affairs* (*OCHA*), *A Principled Framework for Responsible Data Sharing Between Humanitarian Organizations and Donors Humanitarian Data and Trust Initiative*, June 22, 2023, https://www.uninnovation.network/innovation-library/a-principled-framework-for-responsible-data-sharing-between-humanitarian-organizations-and-donors (accessed August 26, 2023).
[96] United Nations Development Programme (UNDP), *Data Principles: 8 Data Principles for UNDP*, https://data.undp.org/data-principles/?_gl=1*i9i9z6*_ga*MTA0MDE2NTkyNy4xNjkzMDgzMzg2*_ga_3W7LPK0WP1*MTY5MzA4MzM4NS4xLjAuMTY5MzA4MzM4Ni41OS4wLjA (accessed August 20, 2023).
[97] Ibid.
[98] Sara Marcucci, Natalia González Alarcón, Stefaan G. Verhulst and Elena Wüllhorst, "Informing the Global Data Future: Benchmarking Data Governance Frameworks," *Data & Policy*, Volume 5, 2023, e30, August 18, 2023, https://www.cambridge.org/core/journals/data-and-policy/article/informing-the-global-data-future-benchmarking-data-governance-frameworks/23C5B7F8C65F21602DD5175DDE49E3BF (accessed August 20, 2023).

implementation of a data governance policy. The analysis identified three practical tools that should be considered to help data stewardship: model consent forms, checklists for data quality, data security and data protection, and data risks assessment step-by-step guidelines. These tools may indeed prove useful to guide implementation, document progress, and monitor compliance.[99] [Original emphasis]

Free Speech is an Information Advantage, JLLIS #230806-5091

Observation. Following the Arab Spring civil protests in 2011, there was a significant decrease in the percentage of civil resistance movements that successfully achieve their stated goals. Ensuring nations honor their citizens' free speech is essential to peaceful democratic processes. As free speech suppressing technologies become ubiquitous, the opportunities to settle polarizing disputes below the threshold of violent armed conflict proportionally decrease. Therefore, civilian and military leaders operating within the international relations domain must understand why the decline has occurred and give outlets to elevate citizen voices without relying upon violent armed conflict.

Discussion. The most notable social movement in recent history was the series of anti-government protests in 2011, known as "the Arab Spring."[100] The Arab Spring began in December of 2010 when a Tunisian street vendor named Mohamed Bouazizi self-immolated in response to the confiscation of his wares and harassment from municipal members of his local government.[101] Bouazizi's act catalyzed the Tunisian Revolution, which involved 28 days of civil resistance, protests, and social media content.[102] WikiLeaks played a supporting role in the protests, with leaked documents revealing the corruption and repression by the Tunisian regime.[103] The protests led to the ousting of Tunisian President Zine El Abidine Ben Ali and eventual democratic elections.[104]

The unrest in Tunisia inspired similar movements in Algeria, Jordan, Egypt, Yemen, Libya, Bahrain, Syria, Iraq, Jordan, Kuwait, Morocco, Oman, and Sudan, with minor protests in Mauritania, Saudi Arabia, Djibouti, and Western Sahara.[105] Social media played a pivotal role in the spread of the demonstrations, as seen in research of the power of social media to support collective action movements.[106] However, these lessons learned are not necessarily about the Arab Spring but lessons gathered by observing governments in a post-Arab Spring world.

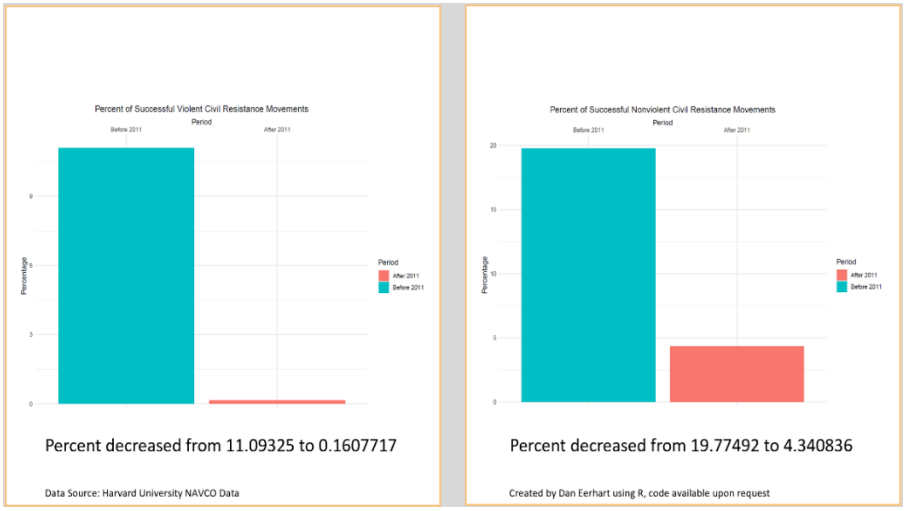
The movement resulted in seven overthrown governments, policy reforms occurring in six countries, and four civil wars.[107] Citizens with their eyes toward democracy and government reforms were not the only ones to notice these dramatic results. Governments began implementing controls and safeguards to reduce the likelihood of an Arab Spring repeat.[108] Following the Arab Spring, two things changed that

---

[99] Marcucci, et al, "Informing the Global Data Future: Benchmarking Data Governance Frameworks."
[100] Abdul QadirMushtaq and Muhammad Afzal, "Arab Spring: Its Causes And Consequences," *Journal of the Punjab University Historical Society,* 2017, https://www.international.ucla.edu/cseas/article/267292 (accessed September 30, 2023).
[101] Ibid.
[102] Ibid.
[103] Simon Mabon, "Aiding Revolution? Wikileaks, Communication and the 'Arab Spring' in Egypt," *Third World Quarterly* 34, no. 10 (November 1, 2013): 1843–57, https://www.tandfonline.com/doi/abs/10.1080/01436597.2013.851901 (accessed September 30, 2023).
[104] QadirMushtaq and Afzal, "Arab Spring…"
[105] Adnan Abdulrahman Naef Farhan and P. A. Varghese, "Facebook Utilization and Arab Spring Movement: A Study among Yemeni Youth," *International Journal of Social Sciences and Management* 5, no. 1 (January 20, 2018): 5–9, https://www.researchgate.net/publication/322627363_Facebook_Utilization_and_Arab_Spring_Movement_A_Study_among_Yemeni_Youth (accessed September 30, 2023).
[106] Ibid.
[107] "The Arab Spring at Ten Years: What's the Legacy of the Uprisings?," *Council on Foreign Relations*, accessed August 29, 2023, https://www.cfr.org/article/arab-spring-ten-years-whats-legacy-uprisings (accessed September 30, 2023).
[108] Ibid.

dramatically favor the efforts of oppressive governments. First, the academic research field of predicting civil unrest exploded, creating opportunities for governments to predict risks to their regimes and act against them. Second, technologies advanced to the point that a government willing to spend large amounts of money can influence the information domain and gain an advantage. As a result, the percentage of successful non-violent social movements plummeted from 19.8 percent before the Arab Spring down to 4.34 percent afterward.[109]

One possible reason for the decrease is simply an issue with the data. After all, a two-sample test revealed a rejection of the null hypothesis (that there was no difference in the proportion of successful civil resistance movements before and after 2011) at a significance level α (alpha) that is less than or equal to 0.05618 (in other words a confidence level approximately 94.38, slightly below the conventional threshold of 95 percent). Additionally, there is a possibility that there is an insufficient sample size in the post-Arab Spring group, given that there were 518 data points before 2011 (4.666 average resistance movements per year) and only 87 afterward (12.43 average resistance movements per year through 2019). While it is certainly a possibility that the change is a statistical anomaly, there is nothing to be learned by chalking change up to chance; instead, let us examine the changes oppressive governments have made in response to the Arab Spring to reduce the likelihood of it repeating.



Civil unrest prediction involves analyzing social media, technology, and social science data to identify trends and attempt to regress future behavior based on previous patterns.[110] Generating effective protest predictive models in democracies has benefits that reduce economic and social risk while enabling governments to preemptively implement policies that may appease the protestors, reduce the likelihood of occurrence, and better serve democracy. However, for the authoritarian regimes attempts to keep their citizens docile and submissive, this predictive ability of civil resistance also provides opportunities to be more aggressive in their operations to silence dissent.

One example of this is in Iran, where citizens rose in protest after a 22-year-old Kurdish woman named Mahsa Amini died following detainment by Iranian morality police and detention at a reeducation center.[111] The Iranian government arrested thousands during the protest, and over 300 died.[112] In August of 2023, predicting that protests would occur in September in conjunction with the anniversary of Amini's death, the Iranian government preemptively arrested likely protestors and their families.[113] A significant

[109] Erica Chenoweth, Jonathan Pinckney, and Orion A. Lewis, "NAVCO 3.0 Dataset" (Harvard Dataverse, November 6, 2019), https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/INNYEO (accessed September 30, 2023).
[110] Kamrul Islam et al., "An Online Framework for Civil Unrest Prediction Using Tweet Stream Based on Tweet Weight and Event Diffusion" 19, no. 1 (February 6, 2020): 65–101, https://e-journal.uum.edu.my/index.php/jict/article/view/jict2020.19.1.4 (accessed September 30, 2023).
[111] Mahsa Rouhi, "Woman, Life, Freedom in Iran," *Survival* 64, no. 6 (November 2, 2022): 189–96, https://doi.org/10.1080/00396338.2022.2150441 (accessed September 30, 2023).
[112] Ibid.
[113] "Iran Rounds up Activists and Relatives of Killed Protesters Ahead of Mahsa Amini Anniversary," https://www.msn.com/en-us/news/world/iran-rounds-up-activists-and-relatives-of-killed-protesters-ahead-of-mahsa-amini-anniversary/ar-AA1fFRSr (accessed August 29, 2023).

lesson learned for the post-Arab Spring world is to not give similar regimes the tools to oppress their people more efficiently.

Governments worldwide have begun to develop propaganda armies of fake social media accounts called "sockpuppets."[114] Government-run *sockpuppet* social media accounts for peddling propaganda, centrally controlled censorship, internet filtration tools, internet shutdowns, and advanced surveillance systems are stables for global authoritarian regimes.[115] The Russian Internet Research Agency and the Chinese "50 Cent Army" are two examples that have gained media prominence in the US.[116] The networks of fake accounts push government-backed themes and reduce the prominence of government detractors.[117] Oxford University's *Computational Propaganda Research Project* analyzed social media manipulation and found evidence of organized social media manipulation campaigns by governments or political parties in 81 countries.[118] With the increase in individuals voices stifled, it is difficult for legitimate movements to control the narrative and achieve their objectives.

Surveillance and censorship technologies are a profitable market, beyond giving governments the tools to silence dissent quickly. Through collecting biometric information (such as gait, facial measurements, voice, and DNA), governments can pinpoint participation in opposition movements and track down individuals. Social media provides the perfect supplement to state-sponsored surveillance and gives repressive governments all the tools needed to generate an enemy list and dispose of them with little resistance. If citizens continuously provide their data to internet-based programs, they feed the information machine with the tools to oppress them and thwart their resistance. Journalists have long known the necessity of privacy and security to enable their work and keep the identities of their sources confidential. However, citizens in dangerous situations may not have the tools necessary to protect themselves and remain private. Following the US withdrawal from Afghanistan, anyone who had supported the United States suddenly became a target for the Taliban.[119] With no US presence on the ground, there was no means of teaching individuals in danger how to protect their identity. The necessity of privacy and security is the third major lesson of the post-Arab Spring World.

Recommendations. In a post-Arab Spring world where oppressive governments can predict future civil resistance movements and unleash advanced technologies on their citizens, who have no privacy or security skills, it may seem hopeless to support peace and stability. However, the war in Ukraine provides some hope in this domain, where their genuine content has fought against Russian artificial content and is winning.[120] Ukrainian social media demonstrates the second major lesson of the post-Arab Spring world: real people are more potent than bots and sock puppets. Therefore, some recommendations include:

---

[114] Brad Stone and Matt Richtel, "The Hand That Controls the Sock Puppet Could Get Slapped," *The New York Times,* July 16, 2007, https://www.nytimes.com/2007/07/16/technology/16blog.html (accessed September 30, 2023).
[115] "NIC-Declassified-Assessment-Digital-Repression-Growing-April2023.Pdf," https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-Assessment-Digital-Repression-Growing-April2023.pdf (accessed August 29, 2023).
[116] Tim Hwang and L. Rosen, "Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps," 2017, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf (accessed September 30, 2023).
[117] Ibid.
[118] "CyberTroop-Report20-Draft9.Pdf," https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf, (accessed August 29, 2023).
[119] Charles J. Sullivan, "Afghanistan in Anarchy: America's Withdrawal, Taliban Rule and Regional Implications for Central Asia," *Journal of Asian Security and International Affairs*, October 30, 2022, https://journals.sagepub.com/doi/10.1177/23477970221129908 (accessed September 30, 2023).
[120] "Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?," *Baker Institute*, September 6, 2022, https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months (accessed August 29, 2023).

First, the US State Department with the Department of Defense must develop a privacy and security curriculum that it can distribute through encrypted means to individuals suffering from oppression. Distributing the curriculum may look like accessing a multi-relay browser (such as the one from the TOR project), a temporary public website through a discreet platform, or even a file sent over an encrypted messaging app. This curriculum could potentially be sent to US-aligned personnel in Afghanistan to teach themselves how to obscure their identity better and remain safe despite being pursued. In areas with a US Embassy or military presence, personnel could provide in-person instruction to ensure that the people who need it most are afforded the tools to survive.

Second, governments should advocate for social media platforms that require identity verification as a prerequisite for use. With authoritarian government access to limitless numbers of fake social media profiles, platforms are responsible for cleaning up their platforms and ensuring that users are legitimate. Unfortunately, social media companies' monetary value relies upon monthly active users, so they have an incentive to ignore fake profiles. Creative incentive programs could offset the costs of removing fake profiles and enforcing universal user verification programs. If banks, schools, utilities, and libraries require user verification, should the primary weapon of the information war not need it, too? When used with a fake-profile bounty program, which would pay users for uncovering foreign government fake social media profiles, social media could return to its original intent of connecting people and away from its role as an authoritarian government tool for oppression.

Third, while research into predicting social movements has a legitimate purpose, it creates a liability for individuals who may seek to engage in those movements. Fortunately, there are a variety of non-governmental organizations that train citizens in social movements and understand this dynamic. Those organizations must hire academic staff members who understand the predictive models and which flags arise to indicate an impending movement. By knowing the flags, trainers can consciously avoid those activities and ensure their movement can proceed without oppressive intervention.

Without actions to ensure individuals can express themselves and control their destinies, it seems likely that the success rates for social movements will continue to decline. It is no coincidence that as the success rates for social movements decline, the global democracy ratings are also declining.[121] When citizens have control of their destiny, they can demand policies that respect their free will. However, when oppressive governments can control narratives, preemptively arrest protesters, and track down every dissenting opinion, the places where peace can flourish will continue to decline.

Lesson Author: Captain Daniel Eerhart is an U.S. Army Psychological Operations Officer currently serving as a Cyber Policy, Law, and Strategy Research Scientist at the Army Cyber Institute. His work focuses on Infrastructure security policies, information warfare, and digital privacy policy and is part of the team that coordinates the annual Jack Voltaic critical infrastructure cyber exercise. He has published work relating to secure source distributed microgrid systems. As a Psychological Operations Officer he has operational experience in five US Central Command countries, including those impacted by the Arab Spring. He was a graduate student at the University of California, Los Angeles (UCLA), where he earned a Master of Public Policy specializing in Technology and Cyber Policy. He holds professional and graduate level certifications in Cybersecurity and Data Analytics.

The Need for Data Governance and Literacy, JLLIS #230601-3615

Observation. The Organization for Security and Co-operation in Europe (OSCE) Special Monitoring Mission (SMM) for the cease-fire in Ukraine, initiated in 2014, was considered technologically "cutting edge"—until the 2022 Russian invasion of Ukraine. Naturally, there have since been several published assessments regarding the apparent failure of the mission and the *lessons learned* from it. One of these

[121] Lucia Garcia, "Democracy Index 2021: Less than Half the World Lives in a Democracy," *Economist Intelligence Unit*, https://www.eiu.com/n/democracy-index-2021-less-than-half-the-world-lives-in-a-democracy/ (accessed September 30, 2023).

assessments suggests "the idea of more technology seems intuitively valuable to ceasefire monitors" but may be "suboptimal… *when methods and capacities for effective data analysis are not in place*."[122] [Emphasis added]

Ceasefire monitoring is only one of the critical components to maintain peace and stability in post-conflict arenas. Clearly, more information about the people, the place, and the issues at hand should be helpful to those efforts. However, from both academic studies and anecdotal remarks, it appears *more* is not always *better* when considering information usefulness for organizational purposes or mission. Instead, too much information may overwhelm individuals and organizational entities. This vast data flow may simply overtake the individual or collective cognitive capacity. In other words, individuals or groups may miss an important data point hidden among the other information of less-relevance. Worse, too much information may lead to various levels of *decision paralysis*.[123]

Data management is a key to *Information Advantage*. Simply, if one cannot assess data relevance adequately, one cannot use it to advantage. In recent months and years, many observers suggest modern *Artificial Intelligence* (AI) tools will assist in data management and address the information overload of most organizations. This may be true. In the interim, some of the existing literature—academic and anecdotal—suggest two other aspects of data management to develop: *data governance*—that is, the way organizations handle its data; and *data literacy*—that is the individual and collective skills needed to both assess and communicate the information data provides.

Discussion. A February 2023 online paper observes:

> Information overload…has probably been an issue for human beings since the beginning of civilization.... However, in the so called digital age and the seemingly infinite amounts of information that the average employee is exposed to is daunting. There are literally billions of current internet users around the world, billions of people using social media everyday, and billions of people sending trillions of emails every year. It is estimated that globally several zettabytes of data are produced annually.[124]

Another author notes:

> the term "information overload" traces back to 1964 when Bertram Gross…described it as an occurrence wherein the input to a system surpasses its processing capacity, leading to reduced decision quality due to the limited cognitive processing capacity of decision-makers.[125]

The same author suggests the causes of information overload are "multifaceted," but highlights three contemporary contributions: the vast *information availability*; the *multiple information channels*; and the

---

[122] Aly Verjee, "Ceasefire monitoring under fire: The OSCE, technology, and the 2022 war in Ukraine," *Global Policy*, 13, no. 5 (November 2022): 808-817, https://doi.org/10.1111/1758-5899.13123 (accessed July 7, 2023). The author offers three other lessons from the OSCE's SMM as well: vague or inconsistent interpretations of the monitor mandates; the need for consequences when ceasefire violations occurred; and a plan for mission suspension and termination "beyond the steps of relocating and evacuating personnel."

[123] "What Is Decision Paralysis In Behavioral Economics?" *Jason Hreha*, https://www.thebehavioralscientist.com/glossary/decision-paralysis#:~:text=In%20behavioral%20economics%2C%20decision%20paralysis,an%20overwhelming%20amount%20of%20information (accessed July 28, 2023). The website notes: In behavioral economics, decision paralysis, also known as choice overload or analysis paralysis, refers to the phenomenon where individuals struggle to make a decision or take action when confronted with an excessive number of options or an overwhelming amount of information.

[124] Jamey A. Darnell and Shalini Gopalkrishnan, "Digital Information Overload: How Leaders Can Strategically Use AI to Prevent Innovation Paralysis," *SSRN*, February 6, 2023, http://dx.doi.org/10.2139/ssrn.4349895 (accessed July 16, 2023).

[125] Fatjona Gërguri, "Reducing information overload in your company," *Employee Experience Magazine*, July 25, 2023, https://www.emexmag.com/reducing-information-overload-in-your-company/ (accessed July 26, 2023).

issue of *information credibility*.[126] However, another group of researchers suggest *information availability* is only part of the challenge. They assert:

> Information volume, as it turns out, is only a partial driver of information overload…the real culprit is the information itself — and specifically the degree to which the accessing and interpreting of the information imposes extra "work" on its recipient.[127]

They call this *extra work* to access and interpret data as the *information burden* and they define it as information that is *duplicative*, *irrelevant*, *effort intensive*, and *inconsistent* or internally conflicted.[128] As they highlight, addressing information and data management is a complex but necessary challenge to an organization. At the one end, "an overload-induced energy drain could compound pre-existing problems with staff disengagement such as burnout, fatigue, and distrust in leadership."[129] At the other end, "inability to get control of information at your organization cuts to the heart of your ability to set and deliver on strategy."[130]

Several authors suggest *data governance* and/or *data literacy* as mechanisms for organizations to use now to create valued information. *Data governance* can be defined as "the set of policies, processes, and standards that ensure the quality, security, and usability of your data."[131] *Data literacy*, in at least one academic paper, is defined as "a competency encompassing five dimensions as a second-order construct: Data Identification, Data Understanding, Data Uses, Data Communication, and Data Reflexivity."[132] Both require careful thought and often specific training and education.

Recommendations. Writing for the Harvard Business Review, some authors suggest two steps to reduce organizational information overload: create a "low-burden" data culture and reinforce accountability.[133] For the low-burden culture creation, the authors note:

> Unspoken communication norms prevail in today's workplace, leaving employees unsure of what good behavior looks like. … Without a mutual understanding of how information should be shared at the organization, employees tolerate dysfunction and feel disempowered to surface dysfunction — and so the cycle of burden continues…Organizations should instead establish clear expectations for how information flows. Shared norms are beneficial for a variety of reasons — they improve psychological safety on teams and empower employees to surface and address instances of channel abuse.[134]

Accountability, the authors assert, must come "from the top":

> The phrase "drinking from a fire hose" is a familiar one, but we really should talk more about who's holding the hose. In the case of information burden, water is coming from everywhere…Part of the challenge of understanding where the burden is coming from is a lack of visibility…The second part is the drudgery of administration.[135]

---

[126] Gërguri, "Reducing information overload in your company."
[127] L.K. Klein, Emily Earl, and Dorian Cundick, "Reducing Information Overload in Your Organization," *Harvard Business Review*, May 1, 2023, https://hbr.org/2023/05/reducing-information-overload-in-your-organization (accessed June 1, 2023).
[128] Ibid.
[129] Ibid.
[130] Ibid.
[131] "How do you design effective data governance training for your data stewards?" *Linkedin*, July 25, 2023, https://www.linkedin.com/advice/0/how-do-you-design-effective-data-governance (accessed July 25, 2023).
[132] Guido Ongena, "Data literacy for improving governmental performance: A competence-based approach and multidimensional operationalization," *Digital Business* 3, no. 1 (June 2023), https://www.sciencedirect.com/science/article/pii/S2666954422000308#s0100 (accessed July 8, 2023).
[133] L.K. Klein, et al, "Reducing Information Overload in Your Organization."
[134] Ibid.
[135] Ibid.

In some respects, *data governance* is the most achievable of these two aspects of data management. There are many extant examples of data steps governance for governmental organizations, including the European Data Governance Act (in full effect in September 2023)[136] and the United Nations (UN) Secretary-General Data Strategy, especially its Priority 6: *Governance and Ethics for the Future*.[137] While different sources suggest different components to a data governance framework, the common three address: the people providing or using the data; the processes to ensure security/privacy as well as it's apparent opposite, transparency; and the technology to generate, analyze, and communicate data.

Data literacy, while also necessary for effective data management, may not be as achievable. The organizational challenges vary from generational perspectives of data and devices, then through and including the awareness of (or lack of it) to media manipulation. Experts predict that AI will be both an asset and a detriment to data literacy. On the one hand, it may assist to channel or group data—to include excluding it—which by its nature reduces information overload. On the other hand, the information exclusion may be harmful and/or the data can be compromised. Regardless, research indicates:

> that data literacy has a direct positive impact on internal performance. Making employees data literate thus improves the effectiveness of governmental bodies…More specifically for the public sector, it is suggested that data skills support the improvement of public services as well as decision and policy-making processes by government employees.[138]

Certainly, the improvement of both data governance and literacy can only enhance the effectiveness of peace and stability operations and activities in the future.

Partnerships

The Asymmetric Advantages of Integrating Partners, JLLIS #230806-5092

Observation. Strategic competition is asymmetric. By nature, it is a struggle between revisionist and status-quo states. The current character is the struggle between authoritarian regimes and democratic states.[139] The author recently conducted a case study to examine the strategic competition between China and Russia, and the United States (US). In this case study, he examined the asymmetric elements of narrative and culture, and found that integrating partner nation (PN) officers into a Marine task force exponentially strengthened partnerships in Latin America and the Caribbean (LAC) at an insignificant cost.

The study's problem statement was that China and Russia have significantly increased their influence in LAC in ways that jeopardize US influence and threaten democratic governance. They exploit the ambiguity of gray zone activities through predatory, opaque lending practices and the spreading of disinformation.

US Forces, Southern Command (SOUTHCOM) counters China's and Russia's gray zone activities through transparency, which it promotes through cooperation activities that strengthen partnerships and

---

[136] "European Data Governance Act," European Commission, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (accessed July 26, 2023).
[137] "United Nations (UN) Secretary-General Data Strategy," United Nations, https://www.un.org/en/content/datastrategy/index.shtml (accessed July 26, 2023).
[138] Guido Ongena, "Data literacy for improving governmental performance…"
[139] Christopher Paul, Michael Schwille, Michael Vasseur, Elizabeth M. Bartels, and Ryan Bauer, *The Role of Information in U.S. Concepts for Strategic Competition* (Santa Monica, CA: RAND Corporation, 2022), vi & 16.

build trust in LAC. SOUTHCOM accomplished this, in part, through Special Purpose Marine Air-Ground Task Force – Southern Command (SPMAGTF-SC), whose mission was to conduct mutually beneficial engagements with partner nations (PN) to address shared challenges in the region.

Over the course of several deployments with this Marine task force, the author observed a significant increase in its influence starting in 2018. From 2015 to 2017, the Marine task force conducted cooperation activities with only four PNs. In 2018, this grew to eleven PNs, and in 2019 it grew further to twelve PNs. Even more surprisingly, this Marine task force had no significant increase in personnel, funding, or duration. The one change while everything else appeared constant is that in 2018 it shifted from a US-only task force to a multinational task force. In 2018, the task force integrated a Colombian Lieutenant Colonel to serve as the Deputy Commander. In 2019, it integrated an additional nine PN officers from Colombia, Brazil, Peru, Chile, Argentina, Belize, and the Dominican Republic.

The purpose of the study was to investigate if integrating PN officers into this Marine task force strengthened partnerships and countered China's and Russia's influence in LAC. And if so, can it be generalized as a model for other geographical regions and the interagency community?

Discussion. This study first examined the degree to which integrating PN officers into the Marine task force strengthened partnerships in the region. It then compared those findings with theories on narrative and culture to explain why integrating PN officers strengthened partnerships. Through this research, the author proposed the concept of a shared regional narrative (SRN) and defined some of the asymmetric characteristics of strategic competition in LAC.

The study consisted of three research subjects. The first was the correlation between the quantity of integrated PN officers and the degree that partnerships were strengthened. The second research subject was the shared regional narrative. The third research subject was the regional and national elements of culture.

To analyze the correlation between the quantity of integrated PN officers and the degree that partnerships were strengthened, the first research subject needed a method to measure strengthened partnerships. First, *Joint Force in Strategic Competition* defines the purpose of military engagements as, "to build trust and confidence, assure and strengthen allies and partners, share information, coordinate mutual activities, and maintain access and influence."[140] Second, SOUTHCOM identifies *Strengthening Partnerships* as one of its three Lines of Effort (LOEs) and outlines the types of military engagements used to achieve it.[141] Therefore, strengthening partnerships was measured by the quantity and total value of military engagements conducted by the Marine task force. The quantity and value of military engagements were then correlated with the quantity of integrated PN officers for each deployment.

The first research subject found that while remaining a US-only task force from 2015 to 2017, it had no significant increase in the degree to which it strengthened partnerships. Integrating PN officers, on the other hand, correlated with a two- to five-fold increase in the quantity and value of military engagements, an increase in the quantity of PNs the task force conducted military engagements with, and an increase in the quantity of integrated PN officers for the subsequent year. At an insignificant cost, integrating PN officers into the Marine task force in 2018 and 2019 exponentially strengthened partnerships in LAC.

---

[140] Chairman of the Joint Chiefs of Staff, Joint Doctrine Note 1-22, *Joint Force in Strategic Competition* (Washington, DC: Joint Chiefs of Staff, 2 February 2023), III-7.

[141] Commander, SOUTHCOM, "United States Southern Command Strategy: Enduring Promise for the Americas," (SOUTHCOM, Doral, FL, 8 May 2019), 5, https://www.southcom.mil/Portals/7/Documents/SOUTHCOM_Strategy_2019.pdf?ver=2019-05-15-131647-353; and *Statement of General Laura J. Richardson, Commander United States Southern Command before the 118th Congress, House Armed Services Committee*, 8 March 2023, 12. The other two LOEs are: 1. Counter Threats, and 2. Build Our Team.

The second research subject was on the author's concept of the SRN. An SRN is a narrative with mutual contribution and equal ownership from all PNs among which it is shared. In 2018 and 2019, the Marine task force developed an SRN by integrating PN officers and becoming a multinational task force.

The second research subject resulted in two primary findings. First, that the planning and development of an SRN in cooperation with PNs increases the accuracy, legitimacy, and will of the narrative, and exposes US blind spots. Second, by employing an SRN, the Marine task force strengthened the meaning, identity, and content of the narrative. And third, the SRN is an asymmetric advantage because it cannot be replicated by an authoritarian regime like the PRC or Russia.

The third research subject analyzed the asymmetric aspects of culture through Geert Hofstede's cultural dimensions.[142] The author's initial assumptions were that the US shared more cultural values with PNs in LAC than the PRC and Russia, and that the US's closer cultural values were an asymmetric advantage in strengthening partnerships. Surprisingly, both these assumptions were wrong.

Out of Hofstede's six cultural dimensions, the US aligned closest with LAC only in the Long-Term Orientation and Indulgence-Restraint dimensions. The PRC aligned closest with LAC in the Power Distance and Individualism-Collectivism dimensions. Russia aligned closest with LAC in the Masculinity-Femininity and Uncertainty Avoidance dimensions.

Even more surprising, the US's misalignment in the Power Distance and Individualism-Collectivism dimensions provided an advantage in strengthening partnerships. The US's low Power Distance value is an advantage in developing multinational organizations. Conversely, the PRC and Russia's high Power Distance value is a disadvantage in developing multinational organizations. Additionally, US's high Individualism-Collectivism value (less shared values between the US and LAC) is an advantage over the PRC's and Russia's low Individualism-Collectivism value (more shared values between the PRC, Russia, and LAC). A high Individualism-Collectivism value is a strength in working with another culture, regardless of that culture's Individualism-Collectivism value.

Recommendations. The joint force and interagency community should integrate allies and partners in the planning and execution of diplomatic, information, and military activities to achieve the National Security Strategy's goal of a "free, open, prosperous, and secure international order."[143] The SRN concept is the method for how integrating partners into the Marine task force strengthened partnerships. It strengthened partnerships by helping identify and address the US's blind spots, and improving regional expertise, and empowering our partners. Understanding how the SRN strengthened partnerships reveals its fundamental principles, which can be generalized for the joint force and interagency community.

Integrating partners in the planning of an SRN effectively identifies and addresses the US's blind spots because of its two underlying principles: mutual contribution and equal ownership. Mutual contribution includes the partner's participation in the planning and execution of the SRN. Equal ownership makes the partner's participation optional. Therefore, by choosing to participate, the partner accepts to be represented by the SRN. This incentivizes the partner to identify and address US planning considerations that do not accurately represent them (i.e., US blind spots). If the US fails to address the identified blind spots, which could be a result of poor planning, biases, groupthink, etc., then the partner may decline the invitation to participate. This serves as a forcing function for the US to either acknowledge its blind spots or accept the partner's refusal to participate.

---

[142] Geert Hofstede, Geert Jan Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind; Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York: McGraw-Hill, 2010).
[143] US President, *National Security Strategy* (Washington, DC: The White House, 12 October 2022), 10.

Integrating PN officers in the execution (i.e., the task force's deployment) improves the regional expertise and empowers our partners. This strengthens the meaning, identity, and content of the narrative. Integrating PN officers is a low-cost solution to building cultural expertise, improving cross-cultural communication, and strengthening partnerships. Often, the US views burden sharing in terms of financial contributions. This perspective deprives our partners of the opportunity of responsibility when they lack financial resources. Integrating them, however, serves as an alternative method, thus empowering them to address our shared regional challenges.

The principles of the SRN—mutual contribution and equal ownership—are generalizable to the joint force and interagency community. Depending on the situation, the SRN may not always be appropriate or feasible. However, the joint force and interagency community can develop an activity built on the principles of mutual contribution and equal ownership. Integrating partners in the planning and execution of that activity will yield the same advantages of addressing blind spots, improving regional expertise, and empowering our partners.

The joint force can replicate this through other military task forces, headquarters elements of combatant commands, or more integration with the interagency community. Potential applications for the interagency community are the US embassy country team, foreign policy development committees, or a whole-of-government task force. When considering a whole-of-government approach, these findings could just as easily be applied to integrating partners across departments. This case study proposes a method for leveraging our most important strategic asset–our allies and partners–as the asymmetric advantage that they are.[144]

Lesson Author: Maj Max Nauta is a Civil Affairs Officer in the US Marine Corps who recently completed his thesis at the US Army Command and General Staff College. His thesis investigates observations from his experiences in the US Forces, Southern Command area of responsibility, where he deployed with Special Purpose Marine Air-Ground Task Force – Southern Command in 2016, 2018, and 2019. In 2018, he served as the liaison officer to the US embassy in Tegucigalpa, Honduras. In 2019, he served as the key leadership engagement coordinator, which included planning and participating in key leadership engagements with the US embassies and partner nation senior leaders in over ten countries in the region. This Lesson is based on his thesis publication:

Maxwell W. Nauta, "Multinational Operations in Strategic Competition: Leveraging the Inherent Informational Aspects through Culture and Narrative," U.S. Army Command and General Staff College, September 9, 2023, https://cgsc.contentdm.oclc.org/digital/collection/p4013coll2/id/4082/rec/1.

Information Advantage in Non-Kinetic Peace Operations: Getting versus Guarding, JLLIS #230901-5113

Observation. The US Army's concept of *Information Advantage* implies the use of a considerable amount of open-source data to include information sharing with partners and other stakeholders in peacekeeping and stabilization operations. Yet, concerns of the military's ability to properly use 'friendly information' results in an unwillingness of non-governmental organizations, other US Agency for International Development (USAID) implementing partners, and international organizations such as United Nations (UN) agencies, to share information with the US military services. Meanwhile US. military actors are often (and often necessarily) hesitant to share information with partners that may put at risk the safety and effectiveness of the military mission.

Although use of open-source data for intelligence is not new, the abundance of social media platforms, online public databases, use of commercial satellites and public relations and communication efforts

[144] US President, *National Security Strategy*, 11.

makes it likely that information sharing as part of partnered engagement can create vulnerabilities for all concerned by making sensitive information accessible to unfriendly actors.

To maximize information advantage through data collection, but not jeopardize operations, the question is one of 'getting versus guarding' information. Partnered engagement must regard sharing information as a "two-way street." To ensure the effectiveness and efficiency of a mission or operation, considerable effort and resources dedicated to data collection can be streamlined when information is shared.

Discussion. A 2022 online article refers to the US Army's achievement of information advantage around five interrelated core tasks. "Commanders must (1) enable decision making; (2) protect friendly information; (3) inform and educate domestic audiences [to include public affairs activities]; (4) inform and influence international audiences; (5) conduct information warfare."[145] However, to what point do we share and to what point do we protect data? This dilemma exists not just between military and civilian actors, but amongst civilian stakeholders and includes host country governments.[146]

There are many constraints to seamless sharing. Sometimes, it is merely due to time available. As example, too often at the start of a mission, with different actors arriving at staggered times, a partner starts from nothing to do its own data collection, when much of the data already exists with other stakeholders. The USAID mission in Yemen grappled with this issue during the Arab Spring in 2011. Humanitarian assistance organizations and USAID implementing partners were in a precarious position, with the ever-looming possibility of a rapid evacuation, which happened in May of that year.

During the USAID mission, the Agency established the Yemen Monitoring and Evaluation Project (YMEP), an umbrella monitoring and evaluation contract to consolidate and analyze all USAID project information as it pertained to drivers of conflict/stability. This meant YMEP coordinated with two implementing partners (Counterpart International and Creative Associates International); and USAID's Office of Transition Initiatives (OTI), all of whom were on the ground prior to YMEP. YMEP built an information management system capable not just of serving as a warehouse for project data, but one designed to test assumptions on whether various project activities achieved the intended objective of stabilizing Yemen.

The database was designed to be able to feed OTI project data and the implementing partners' internal project databases. However, a dilemma was the security of project sites themselves as well as the physical security of the Yemeni project staff seen by destabilizing entities as US government collaborators. As a compromise, YMEP agreed to protect the geodata, but this limited the analysis. At the same time, OTI's caution proved to be prudent as the civil war became more violent.

As Yemen's instability increased, both the State Department and USAID staff and their implementing partners had their 'go bags' ready, but an insufficient plan to secure or destroy all project information in an evacuation. In May 2011, with less than 24 hours' notice, YMEP expatriate staff packed to go but could not telegraph its departure. The conundrum was: how do we dispose of all the project information that had been printed? Cut off access to the database? What if the USAID Mission was returning (there had been several temporary evacuations to Dubai throughout the spring)?[147]

---

[145] Maggie Smith and Nick Starck, "Open-Source Data Is everywhere – Except the Army's Concept of Information Advantage." May 5, 2022, Open-Source Data is Everywhere—Except the Army's Concept of Information Advantage - Modern War Institute (westpoint.edu) (accessed September 30, 2023).

[146] For the purposes of this Lesson, 'stakeholders' is all encompassing (US. civilian and military; implementing partners; NGOs; host country government; civil society organizations; international bodies) while 'implementing partners' specifically refers to NGOs and companies contracted under USAID and other donor country aid agencies. 'Partners' is mission specific.

[147] In Yemen, much of the information security depended on two shredders and the electricity—which would shut down for periods at a time that spring.

While the YMEP Chief of Party (COP) worked with the company headquarters to make evacuation arrangements, the Director of Monitoring and Evaluation, the only other permanent expatriate, hurriedly began shredding documents at such a rate that she burnt out the shredder. She then took the COP's shredder to complete the task, but only by luck, especially when shortly after a mortar landed behind the office and it was time to leave.

The challenge of maximizing information advantage is compounded when there is a level of mistrust between partners regarding the security of information and how it may be used. This leads to the question of how much coordination there can be when there is a need—whether real or perceived—to keep certain data close-hold. It becomes even more complicated when civilian stakeholders may depend on certain information from military actors but do not have the same protocols to protect information the military considers sensitive.

Recommendations. Ultimately, the question is how to strike a balance between operational security and civilian security as well as developed cooperation in partnered engagements. While there are several recommendations to consider, there are three dominant ones:

- Increase cooperation between partners pre-deployment. Not just when a mission or operation is planned, but even earlier through regular training. Implementing partners that operate in conflict areas can incorporate more military-style thinking when it comes to data management.
- Improve evacuation planning to avoid such scenarios as occurred in Yemen. While a burn-pit may be extreme, have established procedures for keeping information—no matter its security level—and a plan to protect information in evacuation or some other emergency such as a natural disaster.
- Increase vetting of local staff when possible. Fortunately, in many stability operations, local candidates had previous work with other USAID projects. Yet someone must be 'first' when hiring a team of local staff. Interviews should include questions to help indicate local staff's interest in and dedication to a program or mission rather than simple attraction to the salary.

Further, the above measures will:

- Enhance trust between partners when it comes to information security and how information is used will enable better decision-making;
- Create more options for influencing perceptions and maintaining a relative advantage over spoilers;
- Establish greater consistency of data between stakeholders; and
- Avoid duplicated or redundant data collection efforts to prevent an unnecessary expenditure of scarce resources) re data collection efforts.

Lesson Author: Sasha Kishinchand served as a Conflict and Stabilization Monitoring and Evaluation analyst with multiple USAID Implementing Partners in locations in the Middle East, Africa, and Afghanistan. She also served as a Presidential appointee to the Iraq Reconstruction and Management Office (IRMO), and a force structure analyst for Naval Special Warfare Command. In addition, she worked in her monitoring and evaluation capacity under the Australian government and the British Foreign Office. She began her career with a BA in International Relations from Tufts University, followed by service as Community Development Peace Corps Volunteer in Cameroon, then earned her MA in Strategic Studies and International Economics from Johns Hopkins School of Advanced International Studies.

Observation. Renown computer scientist, Ivan Sutherland, allegedly said: "Knowledge is a rare thing -- you gain by giving it away."[148] Given his profession, he likely referred to research and design efforts among colleagues. However, the sentiment may be as relevant to information sharing among military and security partners in peace and stability efforts, up to and including intelligence products.[149]

The recently released Department of Defense's *Strategy for Operations in the Information Environment* identifies *Partnerships* as one of its four Lines of Effort (LOEs) to "fully integrate and modernize OIE" (Operations in the Information Environment).[150] In his cover letter to the *Strategy*, Secretary Austin emphasizes partnerships as well. Among the imperatives he outlines for the Defense Department "to gain and sustain information advantages at the times and places of our choosing," he asserts: "It also means bolstering our capacities, *expanding access in allied and partner countries*, and better integration of authorities that help us fulfill our objectives."[151] [Emphasis added] As one military intelligence author posits: "Intelligence sharing is indispensable to modern coalition warfare, but also in numerous other contexts, e.g., peacetime counterterrorism efforts."[152]

In July 2023, Sean Monaghan and Deborah Cheverton, for *War on the Rocks*, note "the allies and partners themselves also have demands of Washington. They want transformational change to Department of Defense [information-sharing] policies and processes that hamper their efforts to support U.S. strategy."[153] So, what information do partners want and how could the US address the needs?

Discussion. The US Department of State proclaims, "Partnerships are key to peacekeeping" and notes the significant financial and training investment the U.S. provides to United Nations (UN) and regional peace operations.[154] Peace operations—and, by extension, many other multinational military missions—are "very much in our national interest," according to a senior U.S. military officer, as well as "far more cost-effective than U.S. boots on the ground."[155]

The July 2023 U.S. Department of Defense's *Strategy for Operations in the Information Environment* reflects the US' interest and intent to continue collaboration with allies and partners in military and security arenas. It notes "the Department will comprehensively consider the informational, physical, and human aspects of the environment…(As) Shared domain awareness, promoting international norms, and building allies and partners are key to establishing and maintaining those advantages."[156] As indicated above, the *Strategy* dedicates one of its four LOEs to *Partnerships* and asserts, in part:

---

[148] "Ivan Sutherland," *A.M. Turning Award*, https://amturing.acm.org/award_winners/sutherland_3467412.cfm (accessed August 10, 2023).
[149] While *information* and *intelligence* have definitions separate and distinct from each other across various professional and multinational applications, this Lesson uses the terms are used as synonyms.
[150] U.S. Department of Defense, *Strategy for Operations in the Information Environment*, July 2023. (Not available online as of this writing.) The other three LOEs are: 1. People & Organizations, 2. Programs, and 3. Policies & Governance. The word *partner* or its variations appear 27 times in the *Strategy*.
[151] Ibid, I.
[152] Marko Milanovic, "Intelligence Sharing in Multinational Military Operations," *The Lieber Institute at West Point*, October 21, 2021, https://lieber.westpoint.edu/intelligence-sharing-multinational-military-operations/ (accessed July 30, 2023).
[153] Sean Monaghan and Deborah Cheverton, "What Allies Want: Delivering the U.S. National Defense Strategy's Ambition on Allies and Partners," War on the Rocks, *Texas National Security Review*, July 24, 2023, https://warontherocks.com/2023/07/what-allies-want-delivering-the-u-s-national-defense-strategys-ambition-on-allies-and-partners/ (accessed July 30, 2023).
[154] Patrick Dolan, "Peacekeeping Possible: The United States Works Worldwide to Build Global Peacekeeping Capacity," Bureau of Political-Military Affairs, *U.S. Department of State*, January 5, 2022, https://www.state.gov/partnerships-make-peacekeeping-possible-the-united-states-works-worldwide-to-build-global-peacekeeping-capacity/ (accessed March 13, 2023).
[155] Jordie Hannum, "Disinformation in a Triple Threat: How Old and New Challenges Make Peacekeeping More Dangerous," *Just Security*, June 13, 2023, https://www.justsecurity.org/86926/disinformation-in-a-triple-threat-how-old-and-new-challenges-make-peacekeeping-more-dangerous/ (accessed August 10, 2023).
[156] U.S. Department of Defense, *Strategy for Operations in the Information Environment*, 8-9.

> The *competition for information advantage* is an inherently global, joint, combined, interagency, and whole-of-society one. The United States military's capability and capacity to operate globally in the IE [information environment] will be contingent on *its ability to establish and maintain situational and enduring partnerships*. *Integration with allies and partners provides a critical warfighting capability*.[157] [Emphasis added]

Monaghan and Cheverton suggest *information sharing* as the "first item on the wish list of US allies and partners," or "NOFORN to YESFORN," and one of three areas "most ripe for reform" in the US government's information environment.[158] They acknowledge that in *information sharing*, "The basic problem is the need to balance two important policy imperatives: protecting classified military information from foreign disclosure vs. 'anchoring our strategy in Allies and partners'" (as described in the NDS).[159] However, they note the NDS also provides the solution to the apparent divergent imperatives. As the disclosure of information policy requires the "disclosure is consistent with U.S. military and security objectives," the authors assert the phrase "anchoring…in Allies and partners" essentially justifies *information sharing*.[160] Still, justification aside, reform in this area "requires modernizing outdated and labor-intensive approaches to foreign intelligence disclosure and information sharing."[161]

Atlantic Council's Transatlantic Security Initiative points out "The difficulties—bureaucratic, cultural, and legal—of sharing information plague not only the intelligence community but also other government agencies and private industry."[162] However, while information sharing challenges may not be a unique issue to US and global defense communities, there may be significant security disadvantages if not addressed. As examples, the authors highlight three themes: the "wide-ranging defense implications" of slowed technological innovation; emerging disruptive technologies like artificial intelligence (AI) and machine learning; and the US' "strategic warning" provision to itself and its allies.[163] Yet, while improved information-sharing between military partners may be laudable for reasons outlined earlier, some authors also offer cautions. Marko Milanovic of *the Leiber Institute at West Point* notes:

> Most states…do not have a domestic legal framework regulating the sharing of intelligence that would satisfy IHRL [International Human Rights Law] requirements in terms of regulatory quality and clarity and effective domestic oversight, and *thus expose themselves to legal liability for violating the privacy of individuals by sharing information* pertaining to them.[164] [Emphasis added]

He highlights two ways states can inadvertently violate IHRL with generous information-sharing policies and processes:

> First, it can be unlawful *as such*, in the sense that a rule of international law may specifically prohibit the sharing of intelligence with a partner, regardless of how the partner intends to use that intelligence.…Second, the sharing or receiving intelligence may be unlawful not because they are prohibited as such, but because they become prohibited due to their connection with an

---

[157] *Strategy for Operations in the Information Environment*, 15. It outlines several Tasks within this LOE, to include: Task A – Establish and Maintain Partnerships within DoD and Among United States Government Interagency Partners, Appropriate Non-United States Government Entities, and International Partners to Enable More Effective Whole-of-Government OIE; and Task B – Foster and Enhance Partnership Capabilities and Capacities.
[158] Monaghan and Cheverton, "What Allies Want: Delivering the U.S. National Defense Strategy's Ambition on Allies and Partners."
[159] Ibid.
[160] Ibid.
[161] Ibid.
[162] Transatlantic Security Initiative, "In Brief: A Ten Step Guide to Transforming Intelligence Sharing with US Allies," *Atlantic Council*, November 3, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/in-brief-a-ten-step-guide-to-transforming-intelligence-sharing-with-us-allies/ (accessed July 30, 2023).
[163] Ibid.
[164] Marko Milanovic, "Intelligence Sharing in Multinational Military Operations."

> unlawful act of a partner. In such cases intelligence sharing is a form of *complicity* in the partner's wrongful act, which the shared intelligence facilitates….[165] [Original emphasis]

The International Committee of the Red Cross (ICRC) echoes these concerns. They emphasize:

> Information may be less reliable when it is shared between actors *with significant differences in terms of intent*, and this can result in escalating the conflict by inadvertently enlarging its scope. Actors should also consider how intelligence will be used by the recipient, in particular the risk that the information shared will contribute to a violation of IHL, for example in relation to the conduct of hostilities…or detention activities.[166] [Emphasis added]

Recommendations. Bram Spoor and Peter de Werd authored a 2023 study of contemporary military intelligence practices through two case studies—a discussion of North Atlantic Treaty Organization (NATO) deployments in Afghanistan and a review of UN missions of recent decades. After their examination, they succinctly recommend "A reevaluation of the nature and value of (open source) information and 'intelligence' is in order, including the function (or limitations) of secrecy."[167] According to Corbett and Danoy of Atlantic Council, this reevaluation needs two critical factors: "sufficient political will and high-level direction to address the issue in an institutional manner," and to "address the issue in a holistic manner, which encompasses policy, process, and mindset."[168] These two factors are further detailed into "ten steps" by *Atlantic Council*'s Transatlantic Security Initiative:

1. Remove the NOFORN caveat for Five Eyes representatives in US agencies.
2. Adopt "Releasable to FVEY" as the default classification for finished intelligence products.
3. Devise a template to define and standardize intelligence sharing classifications.
4. Classify single-source reporting at the NOFORN level on rare occasions and adopt a common referencing system for single-source intelligence reports.
5. Develop joint intelligence requirements with allies.
6. Explore AI and machine learning applications to automate the foreign disclosure process.
7. Maximize the use of open-source intelligence to enable increased sharing with allies without risking sources and methods.
8. Establish and sustain a network of officers committed to facilitating intelligence sharing.
9. Change the risk calculus of intelligence sharing at the analytical level.
10. Undertake a comprehensive review of policy guidance to remove policy constraints, encourage intelligence sharing, and ensure a uniform approach.[169]

In addition to the proscribed "ten steps," the Transatlantic Security Initiative asserts "Intelligence is at its core about *trust*."[170] [Emphasis added] They elaborate:

---

[165] Marko Milanovic, "Intelligence Sharing in Multinational Military Operations."
[166] International Committee of the Red Cross, "Intelligence Support," Understanding Support, Partnered Military Operations, https://sri.icrc.org/understanding-support/forms-support/partnered-military-operations#Intelligencesupport (accessed August 1, 2023).
[167] Bram Spoor and Peter de Werd, "Complexity in Military Intelligence*," International Journal of Intelligence and CounterIntelligence* (2023) 1-21, DOI: https://www.tandfonline.com/doi/full/10.1080/08850607.2023.2209493 (accessed July 30, 2023). In the abstract, the authors note: Intelligence studies missed social science's "complexity turn" more than twenty years ago.…Rather than viewing it as a clearly defined and autonomous field or function embodied by a closed intelligence cycle, military intelligence is best seen as a situated practice.
[168] Sean Corbett and James Danoy, "Beyond NOFORN: Solutions for increased intelligence sharing among allies," *Atlantic Council*, October 31, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/ (accessed July 15, 2023).
[169] Transatlantic Security Initiative, "In Brief: A Ten Step Guide to Transforming Intelligence Sharing with US Allies."
[170] Ibid.

> For the recommendations above to be implemented, both intelligence providers and consumers must prove they can protect the information itself and, even more critically, the sources and methods required to obtain it. A comprehensive counterintelligence strategy, more frequent security training and education, and more consistent protocols will go a long way in ensuring the success of the policies outlined above.[171]

A 2023 study of *trust* and its *role in international intelligence cooperation* confirms this perspective. The authors observe:

> Contrary to the common view that intelligence services are exceptional in their opportunism and rivalry…. the realm of intelligence is instead perhaps the most human of all aspects of government and consists to a large degree of personal relationships. *The universal currency is trust.*[172] [Original emphasis]

They also note, "Known reputations, recognized professional standards, and shared traits socially bind intelligence professionals to their community of practice, enabling them to bridge divides like nationality and even conflicting interests."[173] Finally, Corbett and Danoy conclude their assessment of intelligence sharing solutions for allies and partners with this observation:

> while this paper focused almost exclusively on what needs to be done within the US intelligence establishment, US allies and partners have a similar role to play in optimizing intelligence sharing. They need to reciprocate with their own resources, as well as cohere and adapt their own information management capabilities and mechanisms to accommodate the new model of information exchange, earning the enduring trust of the United States by demonstrating a rigorous process to protect US-derived intelligence in an appropriate manner. In taking a proactive approach to intelligence sharing, the genuine concerns of inadvertent disclosure must be addressed, and the proper protection of critical national capabilities, methods, and sources must be afforded the attention they merit.[174]

.

[171] Transatlantic Security Initiative, "In Brief: A Ten Step Guide to Transforming Intelligence Sharing with US Allies."
[172] Pepijn Tuinier, Thijs Brocades Zaalberg and Sebastiaan Rietjens, "The Social Ties that Bind: Unraveling the Role of Trust in International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* (2023) 36:2, 386-422, https://www.tandfonline.com/doi/full/10.1080/08850607.2022.2079161?src=recsys (accessed August 13, 2023).
[173] Ibid.
[174] Corbett and Danoy, "Beyond NOFORN: Solutions for increased intelligence sharing among allies."

PKSOI Lesson Reports and SOLLIMS Samplers (2013-2023)

2023

- PKSOI Semiannual Lesson Report Protection of Civilians and Civilian Harm Mitigation Response, Volume I and II (March 2023)

2022

- PKSOI Semiannual Lesson Report: Defense Support to Stabilization, Volume I and II (June 2022)

2021

- PKSOI Semiannual Lesson Report Multinational Interoperability Command and Control and Transitions (November 2021)
- PKSOI Semiannual Lesson Report Setting the Stage (May 2021)

2020

- PKSOI Semiannual Lesson Report Multinational Interoperability (November 2020)
- PKSOI Lesson Report Consolidating Gains (March 2020)

2019

- PKSOI Lesson Report Partnering (December 2019)
- PKSOI Lesson Report Strategic Planning (September 2019)
- PKSOI Lesson Report Conflict Prevention (June 2019)
- PKSOI Lesson Report SSR and DDR (January 2019)

2018

- SOLLIMS Sampler Vol 10 Issue 1 Transitional Public Security (December 2018)
- SOLLIMS Sampler Vol 9 Issue 4 Foreign Humanitarian Assistance (September 2018)
- SOLLIMS Sampler Vol 9 Issue 3 PKSO Complexities and Challenges (July 2018)
- PKSOI Lesson Report Right-Sizing and Stage-Setting (July 2018)
- SOLLIMS Sampler Vol 9 Issue 2 Inclusive Peacebuilding (May 2018)
- SOLLIMS Sampler Vol 9 Issue 1 Monitoring and Evaluation (January 2018)

2010-17

- SOLLIMS Sampler Vol 8 Issue 2 Operationalizing WPS (November 2017)
- SOLLIMS Sampler Sp Ed Leadership in Crisis and Complex Operations (May 2017)
- SOLLIMS Sampler Vol 8 Issue 1 Civil Affairs in Stability Operations (March 2017)
- SOLLIMS Sampler Sp Ed Internal Displaced Persons (IDP) (January 2017)
- SOLLIMS Sampler Vol 7 Issue 4 Strategic Communication in PSO (November 2016)
- SOLLIMS Sampler Vol 7 Issue 3 Stabilization and Transition (August 2016)
- SOLLIMS Sampler Vol 1 Issue 2 Investing in Training (June 2016)
- SOLLIMS Sampler Vol 7 Issue 1 Building Stable Governance (March 2016)
- SOLLIMS Sampler Vol 6 Issue 4 Shifts in UN Peacekeeping (February 2016)
- SOLLIMS Sampler Vol 6 Issue 3 FHA Concepts, Principles and Applications (December 2015)
- SOLLIMS Sampler Vol 6 Issue 2 FHA Complexities (September 2015)
- SOLLIMS Sampler Sp Ed Cross Cutting Guidelines for Stability Operations (July 2015)
- SOLLIMS Sampler Sp Ed Lessons from US Army War College Students (May 2015)
- PKSOI Lesson Report MONUSCO Lessons Learned (December 2014)
- SOLLIMS Sampler Vol 5 Issue 4 Reconstruction and Development (November 2014)
- SOLLIMS Sampler Vol 5 Issue 2 Overcoming Spoilers (April 2014)
- SOLLIMS Sampler Vol 5 Issue 1 Host Nation Security (January 2014)

Disclaimer: The views expressed in this publication are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the US Government. All content in this document, to include any publication provided through digital link, is considered unclassified, for open access. This compendium contains no restriction on sharing/distribution within the public domain. Existing research and publishing norms and formats should be used when citing Report content.