Excerpt from InterAgency Journal 16-1
©2026 - Simons Center

Disclaimer: The articles published in the IAJ represent the opinions of the authors and do not reflect the official views of any United States government agency, the Department of War, the Department of the Army, the U.S. Army Command and General Staff College, the Command and General Staff College Foundation and Alumni Association, the Simons Center, or any other non-government, private, public or international organization.

Governing Transformation in Contact

An Ethical Framework for Distributed Decision Making across Interagency Networks

by Babu George

The U.S. Army's Transforming in Contact initiative recognizes a hard truth: The next major conflict will not wait for the force to finish modernizing before it must fight. Units will experiment, adapt, and reorganize while under fire. Ukraine's war since 2022 has provided a real-time demonstration of this reality, as Ukrainian forces used decentralized command structures and commercial off-the-shelf (COTS) technologies to outmaneuver a larger adversary.[1] But what works on a single nation's battlefield becomes far more complicated when the transformation must span not just military echelons but the full interagency apparatus: intelligence, diplomacy, development, law enforcement, and homeland security.

The challenge is not simply operational; it is an ethical one at its root. When authority is pushed to lower echelons, when algorithms assist targeting decisions, when commercial drones are integrated into kill chains within weeks rather than years, the traditional safeguards of civilian control, legal review, and moral accountability come under severe strain. The question for interagency leaders is not whether to embrace distributed decision-making and rapid technological adoption, but how to do so without sacrificing the values that make such power legitimate in the first place.

This article proposes an ethical framework for governing transformation in contact across interagency networks. It draws on a systematic review of fifty peer-reviewed papers spanning organizational theory, network governance, crisis management, and military command, as well as lessons emerging from the Ukraine conflict. The framework is built around five governing principles, each addressing a distinct tension between speed and accountability that interagency leaders must manage.

Babu George, Ph.D., is a full professor of management at Alcorn State University. An experienced academic leader, he has served in various global universities as director, chair, and dean. A prolific scholar, he has authored over 10 books and more than 300 articles in peer-reviewed journals. His research investigates strategic leadership, organizational resilience, and the application of military strategies to modern business contexts. George's broader expertise encompasses crisis management, organizational change, and digital transformation. Through his extensive body of work, he equips modern leaders with actionable frameworks to navigate uncertainty and drive growth amid rapid technological disruption.

Ukraine as a Laboratory for Transformation in Contact

Ukraine's battlefield innovations offer the most vivid contemporary illustration of what transformation in contact looks like in practice. Ukrainian forces did not adopt commercial unmanned aerial systems (UAS), open-source intelligence (OSINT) platforms, and COTS communication tools according to a tidy procurement timeline. They did so under artillery fire, iterating at a pace that traditional acquisition processes would consider reckless.[2] The results were operationally impressive: Small units exploited commercial drones for reconnaissance and strike missions, shared intelligence laterally through ad hoc digital networks, and adapted tactical procedures within days rather than months.[3]

The Ukrainian experience validated a core tenet of mission command–that delegating authority to the point of action enhances operational adaptability in complex, contested environments.[4] Yet, it also exposed serious vulnerabilities. Modeling of distributed decision-making has shown that such approaches can produce information overload and coordination incoherence under stress, findings that the Ukrainian experience confirmed in the field.[5] Scholars have also warned that automating portions of the observe-orient-decide-act (OODA) loop risks marginalizing the human judgment that remains essential for lawful and ethical operations, particularly when targets are identified and engaged at machine speed.[6]

For the interagency, the lessons from Ukraine are both inspiring and cautionary. The speed of Ukrainian adaptation depended on a relatively homogeneous force with shared national purpose operating under existential threat. United States (U.S.) interagency operations, by contrast, involve organizations with different legal authorities, organizational cultures, risk tolerances, and accountability structures. The Department of War operates under Title 10; the Intelligence Community under Title 50; the State Department under Title 22; and law enforcement agencies under yet another set of statutes. Each legal framework carries its own constraints on information sharing, use of force, and operational authorities. When a commercial drone that was procured informally, integrated without full testing, and operated by a newly trained soldier kills an enemy combatant, the legal and moral calculus is already complex. When an analogous tool is deployed across agency boundaries, with ambiguous authority chains and competing classification systems, that complexity compounds.

Ukraine's battlefield innovations offer the most vivid contemporary illustration of what transformation in contact looks like in practice.

Moreover, Ukraine's innovation came at a cost that is often understated in Western analyses. The rapid adoption of commercial systems created supply chain vulnerabilities, operational security gaps, and quality control problems that a more deliberate approach would have mitigated. Ukrainian commanders accepted these risks because the alternative was defeat. U.S. interagency leaders do not face that binary choice, and they should not pretend otherwise. Translating battlefield agility into whole-of-government coordination requires more than enthusiasm for decentralization; it requires ethical architecture.

Structuring Interagency Networks for Ethical Agility

The organizational theory literature provides a useful foundation for thinking about how interagency networks should be structured to support rapid adaptation while preserving

accountability. Three ideal-type governance models for organizational networks have been identified: shared governance, where all participants jointly manage the network; lead-organization governance, where a single dominant member coordinates the network on behalf of the others; and network administrative organization, where a separate entity is created to govern the network.[7] Each model carries different implications for efficiency, legitimacy, and the distribution of power.

This framework has direct implications for interagency transformation. A small, high-trust coalition of agencies working on a specific mission (for instance, a combined counter-UAS task force) may function well under shared governance, with authority distributed broadly and coordination achieved through mutual adjustment. But a large interagency network operating across multiple theaters and functional domains, the more common scenario for whole-of-government operations, will likely require either a lead-organization model or a dedicated administrative body to prevent fragmentation and ensure strategic alignment.[8]

Over-decentralization, where every node acts on its own interpretation of the situation, can undermine the very strategic coherence that distributed networks are supposed to serve.

Research on distributed sensemaking during the Utrecht terrorist attack found that crisis coordination breaks down when participating organizations maintain competing situational pictures without mechanisms for reconciliation.[9] The interagency analogue is clear: when the Department of War, the Intelligence Community, the State Department, and USAID each construct independent assessments of a fast-moving situation, the resulting divergence can paralyze decision-making or produce contradictory actions. Subsequent work has traced how crisis organizations progress from information sharing to genuine distributed decision-making, a transition that requires codified protocols and shared mental models rather than mere connectivity.[10] Without such protocols, more information and faster networks amplify confusion rather than resolve it.

These organizational insights, drawn from both network governance theory and crisis management research, point toward a set of governing principles for interagency transformation. The five principles outlined in the following section address the core tensions that emerge when speed and decentralization meet the accountability requirements of democratic governance.

Five Principles for Ethical Transformation in Contact

Principle 1: Calibrated Authority Delegation

The first principle holds that authority delegation must be calibrated to context, not treated as a blanket policy preference. Research on network governance and military command agrees that delegating authority closer to the point of action enhances adaptability in complex environments.[11] But an important warning emerges from the application of Normal Accidents Theory to networked military operations: the tight coupling and interactive complexity that make networked systems powerful also make them prone to cascading failures that no individual node can anticipate or control.[12] Over-decentralization, where every node acts on its own interpretation of the situation, can undermine the very strategic coherence that distributed networks are supposed to serve.

For interagency operations, calibrated authority delegation means defining decision rights for each type of action and each level of

risk. Routine information sharing and tactical adaptation can be safely delegated to front-line teams. Decisions involving the use of force, the commitment of diplomatic capital, or the disclosure of sensitive intelligence require escalation pathways that are fast but not absent. The goal is not to recreate bureaucratic bottlenecks, but to ensure that the speed of delegation does not outrun the capacity for legal review and policy oversight. Even as AI systems accelerate the OODA loop, human commanders must retain meaningful authority over consequential decisions.[13] This principle applies with equal force across the interagency, where the consequences of an unchecked automated decision can ripple across diplomatic, intelligence, and military channels at once.

Principle 2: Trust Architecture

Trust is the currency that makes distributed decision-making possible. Without it, delegation degenerates into either micromanagement or chaos. Research on threat assessment and decision-making across police, military, ambulance, and fire services has found that effective distributed operations depend on shared frameworks for sensemaking and a baseline of interpersonal and institutional trust that takes deliberate effort to build.[14]

In interagency settings, trust deficits are endemic. Agencies compete for budget share, policy influence, and credit. Classification barriers obstruct information sharing. Organizational cultures differ so sharply that even common terminology can carry different meanings. Building what might be called a "trust architecture" for interagency transformation requires structural investments: joint training exercises, personnel exchange programs, shared operational planning cycles, and, above all, shared accountability for outcomes rather than siloed responsibility for inputs. Network governance effectiveness depends on trust density among participants; where trust is low, more formalized governance mechanisms are needed to compensate.[15] As a result, interagency leaders should audit existing trust conditions before deciding how much authority to distribute, and they should invest in trust-building with the same rigor they bring to technology.

Principle 3: Information Flow Discipline

The Ukrainian experience confirmed what modeling research has demonstrated: distributed decision-making generates enormous volumes of information, and without disciplined management, that information becomes noise rather than signal.[16] Researchers have explored how novel network paradigms, including information-centric networking and software-defined networking, can provide the technical infrastructure for managing information flows in military command and control.[17] Broader surveys of emerging network approaches for military C2 systems have found that architectural choices about how information is routed, filtered, and prioritized have direct operational consequences.[18]

Trust is the currency that makes distributed decision-making possible.

For the interagency, information flow discipline is both a technical and a governance challenge. The technical dimension involves building interoperable data-sharing platforms that can operate across classification levels and organizational boundaries, a persistent gap in U.S. government operations. The governance dimension is harder: Establishing protocols for what information gets pushed versus pulled, who has authority to reclassify or share sensitive material in time-critical situations, and how to prevent the information asymmetries that breed distrust. One promising approach involves heterogeneous network architectures that

link diverse data sources and formats across organizational boundaries to enable coordinated autonomous operations.[19] With appropriate modification, such architectures could serve interagency information-sharing requirements. The ethical imperative is that information flow protocols must be designed not only for speed but for accuracy, context, and the preservation of decision-maker judgment. Flooding a commander or senior civilian with raw data is not empowerment; it is abdication.

...professionals rely on both intuitive, recognition-primed decision processes (fast, pattern-based) and formal, analytical decision processes (slower, deliberate).

Principle 4: Dual-Track Professional Judgment

Research on tactical decision-making in high-risk environments has identified a tension at the heart of practitioner performance: professionals rely on both intuitive, recognition-primed decision processes (fast, pattern-based) and formal, analytical decision processes (slower, deliberate).[20] The most effective operators blend the two, shifting between modes as the situation demands. Training programs that emphasize only one mode produce professionals who are either dangerously impulsive or fatally slow.

This finding has deep implications for how interagency personnel are prepared for transformation in contact. Artificial Intelligence (AI) systems, by their nature, operate in the pattern-recognition mode; they excel at detecting correlations and matching inputs to trained categories, but they lack the contextual moral reasoning and situational judgment that characterize the analytical mode. As AI-enabled decision support tools become embedded in interagency workflows, from intelligence analysis to humanitarian response planning, the risk is that operators will default to algorithmic recommendations without engaging their own professional judgment. Alternatively, they may reject useful machine outputs because they lack the training to evaluate them with care. Research on digital transformation shows that it succeeds only when supported by leadership that understands technology well enough to govern its use wisely, not to adopt it reflexively.[21]

Dual-track professional judgment means training interagency personnel to use AI tools as inputs to their decision-making, not substitutes for it. It means preserving the expectation that human professionals will exercise moral reasoning, legal analysis, and contextual understanding that algorithms cannot replicate. It also means designing AI decision-support systems with transparency mechanisms (explainability, confidence intervals, dissent flagging) that facilitate rather than foreclose human oversight. Leadership development programs should cultivate both transformational and adaptive capacities, since research has shown that leaders who possess both are better equipped to manage digital transformation projects.[22] Interagency training programs should target these qualities.

Principle 5: Accountable Digital Leadership

The final principle addresses a persistent gap in the field: the shortage of leaders who possess both operational expertise and digital fluency. Mastering digital transformation requires leaders who understand the nexus between leadership, organizational agility, and digital strategy.[23] Digital transformational leadership is essential for applying organizational agility in public sector contexts, including in settings where institutional capacity is limited.[24] The evolution of public sector leadership in the digital era points to a clear conclusion: leaders who cannot govern technology will be governed by it.[25] Taken together, these findings underscore that digital

leadership is not a technical specialty but a core governance competency, one that determines whether technology serves institutional purposes or displaces them.

For interagency operations, accountable digital leadership means more than appointing a chief information officer. It means cultivating leaders at every echelon who understand the capabilities and limitations of the technologies being deployed, who can make informed judgments about when to rely on machine outputs and when to override them, and who accept personal accountability for the consequences of technology-assisted decisions. In the context of autonomous systems and AI-enabled information operations, the ethical stakes are high. A leader who authorizes an AI-assisted targeting recommendation without understanding the model's training data, confidence thresholds, or failure modes is not exercising command; they are abdicating it. A comprehensive overview of the challenges facing distributed decision-making in resource-contested and dynamic environments confirms that these difficulties are not theoretical; they are already present in operational settings where leaders must make high-stakes choices with incomplete information and imperfect tools.[26]

Implications for Interagency Transformation Initiatives

Taken together, these five principles suggest that the U.S. government's approach to interagency transformation should differ in kind from the way individual military services adopt new technologies and operating concepts. The military can, within limits, experiment with distributed decision-making within a single chain of command, a shared legal framework, and a common organizational culture. However, the interagency cannot. Whole-of-government transformation in contact requires what researchers in the technical domain have described as the combination of information-centric and software-defined approaches to achieve agility in mobile networks.[27] Applied here as a metaphor for governance design, the interagency needs both flexible, adaptive coordination mechanisms (the information-centric layer) and deliberate, rule-based governance structures (the software-defined layer) operating at the same time.

For interagency operations, accountable digital leadership means more than appointing a chief information officer. It means cultivating leaders at every echelon...

Three practical recommendations follow from this analysis. First, ideally, the National Security Council or a designated interagency body should develop and promulgate explicit governance frameworks for each major transformation initiative, specifying decision rights, escalation protocols, information-sharing rules, and accountability mechanisms before technologies are deployed rather than after failures occur. The governance model should be matched to context: smaller, high-trust coalitions can operate with shared governance, while larger multi-agency initiatives need lead-organization or dedicated administrative governance.[28] This matching process should be explicit and documented, not left to bureaucratic inertia.

Second, interagency training programs should be redesigned to develop dual-track professional judgment, incorporating realistic scenario exercises that require participants to integrate AI outputs with independent analysis under time pressure. These programs should draw from cross-sector research demonstrating that decision-making effectiveness improves when practitioners are trained to shift with intention between intuitive pattern recognition and structured analytical methods.[29] The current

state of interagency exercises, too often scripted and too seldom designed to produce genuine cognitive stress, falls well short of this standard. Exercises should include degraded information environments, contradictory intelligence feeds, and AI recommendations that are sometimes wrong, forcing participants to develop the evaluation skills they will need when real systems fail.

Third, senior leader education should include dedicated digital leadership modules, moving beyond superficial technology overviews to engage with the ethical, legal, and organizational implications of AI-enabled decision support, autonomous systems, and AI-driven information operations. These modules should not be optional enrichment seminars. They should be treated as core competencies for promotion to senior interagency positions, just as joint military experience is now required for general officer advancement. Research has shown that leaders with both transformational and adaptive capacities are better equipped to manage digital transformation projects.[30] Interagency development programs should cultivate both qualities with purpose.

The goal of ethical transformation in contact is not to be as fast as possible but to be as fast as responsible governance permits...

These recommendations may seem cautious compared to the dramatic speed of Ukrainian battlefield innovation. That caution is deliberate. Ukraine's adaptation was driven by existential necessity and accepted risks that a democratic superpower operating across the full spectrum of government functions should not. The goal of ethical transformation in contact is not to be as fast as possible but to be as fast as responsible governance permits, recognizing that the legitimacy and sustainability of interagency operations depend on public trust, legal compliance, and moral accountability that cannot be restored once lost.

Research Gaps and Future Directions

Despite the growing body of literature on distributed decision-making in defense, significant gaps remain. Empirical evaluation of specific network governance designs under real-world stressors, particularly electronic warfare and cyberattack conditions, is scarce.[31] The integration of commercial technologies at scale without loss of strategic control or security remains largely uncharted in peer-reviewed research, even as it proceeds in practice at speed.[32] Cross-sector transferability of lessons, whether models developed in military contexts apply to civilian interagency operations and vice versa, is underexplored.[33] And the long-term cultural impacts of sustained decentralization on organizational identity, cohesion, and institutional knowledge have barely been studied.

Future research should prioritize empirical testing of interagency governance models under contested conditions, including wargames and exercises designed to stress-test information-sharing protocols and authority delegation frameworks. It should explore how commercial technology integration can be governed through scalable frameworks that preserve security and alignment across agencies with different classification standards and risk tolerances. It should also assess whether the leadership development approaches found effective in single-organization studies translate to the more fragmented and politically contested interagency environment.[34]

Conclusion

Transformation in contact is not a choice; it is an emerging condition of interagency operations in the twenty-first century. The pace of technological change, the diffusion of advanced capabilities to state and non-state

actors, and the compression of decision timelines all demand that U.S. government organizations adapt while operating, not before. Ukraine has demonstrated that distributed decision-making and mission command, supported by commercial technology and adaptive leadership, can produce remarkable operational results.[35]

But operational results are not the only measure of success for a democratic government. The ethical framework proposed here, built on calibrated authority delegation, trust architecture, information flow discipline, dual-track professional judgment, and accountable digital leadership, is intended to ensure that the speed of transformation does not outstrip the capacity for responsible governance. Each principle addresses a specific tension between agility and accountability, and each requires deliberate investment in organizational design, training, and leadership development rather than mere technological adoption.

The interagency faces a choice that is more consequential than any particular technology decision. It can pursue speed for its own sake, treating ethical constraints as friction to be minimized. Or it can recognize that those constraints (civilian control, legal compliance, professional judgment, moral responsibility) are not obstacles to effective transformation but the foundations of legitimate authority without which no transformation is sustainable.

History offers a relevant lesson. The most durable military and governmental innovations have not been those that moved fastest, but those that paired operational innovation with institutional adaptation. The Prussian adoption of mission command in the nineteenth century succeeded not because it was quick, but because it was accompanied by systematic reforms in officer education, doctrinal development, and organizational culture that gave decentralized authority a coherent intellectual foundation.[36] The interagency equivalent of that foundation is ethical governance, and the time to build it is now, before the next crisis forces transformation upon organizations that have not prepared the ethical infrastructure to sustain it. The framework offered here stakes a clear position: Ethical governance is not the enemy of agility. It is the condition that makes agility worth having. ***IAJ***

Notes

1 Petro Tudorache and Mircea Constantinescu, "Enhancing Decision-Making Resilience through Mission Command: The Particular Case of Ukraine," *Vojenské rozhledy* 33, no. 4 (2024), https://doi.org/10.3849/2336-2995.33.2024.04.020-036; Karim Crombé and John Nagl, "A Call to Action: Lessons from Ukraine for the Future Force," *The US Army War College Quarterly: Parameters* (2023), https://doi.org/10.55540/0031-1723.3233.

2 Crombé and Nagl, "A Call to Action"; Tudorache and Constantinescu, "Enhancing Decision-Making Resilience."

3 *The Russia-Ukraine War: Security Lessons* (2025), https://doi.org/10.3726/b21757.

4 K. G. Provan and P. Kenis, "Modes of Network Governance: Structure, Management, and Effectiveness," *Journal of Public Administration Research and Theory* 18, no. 2 (2007): 229-252, https://doi.org/10.1093/jopart/mum015; B. Van Bezooijen and E. Kramer, "Mission Command in the Information Age: A Normal Accidents Perspective on Networked Military Operations," *Journal of Strategic Studies* 38, no. 4 (2015): 445–466, https://doi.org/10.1080/01402390.2013.844127; J. Gomes et al., "Surveying Emerging Network Approaches for Military Command and Control Systems," *ACM Computing Surveys* 56 (2023): 1–38, https://doi.org/10.1145/3626090.

5 A. Kalloniatis, T. McLennan-Smith, and D. Roberts, "Modelling Distributed Decision-Making in Command and Control Using Stochastic Network Synchronisation," *European Journal of Operational Research* 284, no. 2 (2020): 588-603, https://doi.org/10.1016/j.ejor.2019.12.033.

6 J. Johnson, "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age," *Defence Studies* 23, no. 1 (2022): 43-67, https://doi.org/10.1080/14702436.2022.2102486.

7 Provan and Kenis, "Modes of Network Governance."

8 Provan and Kenis, "Modes of Network Governance"; J. Wolbers, "Understanding Distributed Sensemaking in Crisis Management: The Case of the Utrecht Terrorist Attack," *Journal of Contingencies and Crisis Management* (2021), https://doi.org/10.1111/1468-5973.12382.

9 Wolbers, "Understanding Distributed Sensemaking."

10 W. Treurniet and J. Wolbers, "Codifying a Crisis: Progressing from Information Sharing to Distributed Decision-Making," *Journal of Contingencies and Crisis Management* (2020), https://doi.org/10.1111/1468-5973.12323.

11 Provan and Kenis, "Modes of Network Governance"; Van Bezooijen and Kramer, "Mission Command in the Information Age"; Gomes et al., "Surveying Emerging Network Approaches."

12 Van Bezooijen and Kramer, "Mission Command in the Information Age."

13 Johnson, "Automating the OODA Loop."

14 G. Penney, D. Launder, J. Cuthbertson, and M. Thompson, "Threat Assessment, Sense Making, and Critical Decision-Making in Police, Military, Ambulance, and Fire Services," *Cognition, Technology and Work* 24 (2022): 423–439, https://doi.org/10.1007/s10111-022-00694-3.

15 Provan and Kenis, "Modes of Network Governance."

16 Kalloniatis, McLennan-Smith, and Roberts, "Modelling Distributed Decision-Making."

17 J. Stocchero, C. Da Silva, L. De Souza Silva, M. Lawisch, J. Anjos, and E. De Freitas, "Secure Command and Control for Internet of Battle Things Using Novel Network Paradigms," *IEEE Communications Magazine* 61 (2023): 166-172, https://doi.org/10.1109/mcom.001.2101072; G. Leal, I. Zacarias, J. Stocchero, and E. De Freitas, "Empowering Command and Control through a Combination of Information-Centric Networking and Software Defined Networking," *IEEE Communications Magazine* 57 (2019): 48–55, https://doi.org/10.1109/mcom.2019.1800288.

18 Gomes et al., "Surveying Emerging Network Approaches."

19 M. Hawkins et al., "Heterogeneous Network-Driven Data Fabrics to Enable Multi-Mission Autonomy," MILCOM 2022 (2022): 259-264, https://doi.org/10.1109/milcom55135.2022.10017623.

20 Penney et al., "Threat Assessment, Sense Making, and Critical Decision-Making"; D. Launder and G. Penney, "Towards a Common Framework to Support Decision-Making in High-Risk, Low-Time Environments," *Journal of Contingencies and Crisis Management* (2023), https://doi.org/10.1111/1468-5973.12487.

21 B. AlNuaimi and K. Singh, "Mastering Digital Transformation: The Nexus between Leadership, Agility, and Digital Strategy," *Journal of Business Research,* 145 (2022), https://doi.org/10.1016/j.jbusres.2022.03.038; H. Sugiyanto, "Evolution of Public Sector Leadership in the Era of Digital

Transformation," *International Journal of Public Administration and Policy* (2025), https://doi.org/10.58290/ijpap.v1i1.14.

22 J. Huang, R. Jiang, and J. Chang, "The Effects of Transformational and Adaptive Leadership on Dynamic Capabilities: Digital Transformation Projects," *Project Management Journal* 54 (2023): 428-446, https://doi.org/10.1177/87569728231165896.

23 AlNuaimi and Singh, "Mastering Digital Transformation."

24 B. Ly, "Leveraging Leadership and Digital Transformation for Sustainable Development: Insights from Cambodia's Public Sector," *Sustainable Futures* (2025), https://doi.org/10.1016/j.sftr.2025.100545; B. Ly, "The Interplay of Digital Transformational Leadership, Organizational Agility, and Digital Transformation," *Journal of the Knowledge Economy* (2023): 1–20, https://doi.org/10.1007/s13132-023-01377-8.

25 Sugiyanto, "Evolution of Public Sector Leadership."

26 C. Szabo, R. Baker, G. Pearce, E. Teffera, and A. Perry, "Overview and Challenges of Distributed Decision Making in Resource Contested and Dynamic Environments," *ACM Computing Surveys* 57 (2025): 1-34, https://doi.org/10.1145/3719001.

27 J. Stocchero, A. Carneiro, I. Zacarias, and E. Freitas, "Combining Information Centric and Software Defined Networking to Support Command and Control Agility in Military Mobile Networks," *Peer-to-Peer Networking and Applications* 16 (2023): 765-784, https://doi.org/10.1007/s12083-022-01443-z.

28 Provan and Kenis, "Modes of Network Governance."

29 Penney et al., "Threat Assessment, Sense Making, and Critical Decision-Making"; Launder and Penney, "Towards a Common Framework."

30 Huang, Jiang, and Chang, "The Effects of Transformational and Adaptive Leadership."

31 Kalloniatis, McLennan-Smith, and Roberts, "Modelling Distributed Decision-Making"; Johnson, "Automating the OODA Loop."

32 Crombé and Nagl, "A Call to Action."

33 Treurniet and Wolbers, "Codifying a Crisis"; Wolbers, "Understanding Distributed Sensemaking"; Launder and Penney, "Towards a Common Framework."

34 AlNuaimi and Singh, "Mastering Digital Transformation"; Huang, Jiang, and Chang, "The Effects of Transformational and Adaptive Leadership"; Sugiyanto, "Evolution of Public Sector Leadership"; Ly, "Leveraging Leadership and Digital Transformation"; Ly, "The Interplay of Digital Transformational Leadership."

35 Tudorache and Constantinescu, "Enhancing Decision-Making Resilience"; Crombé and Nagl, "A Call to Action"; *The Russia-Ukraine War: Security Lessons* (2025).

36 See generally Daniel J. Hughes, ed., Moltke on the Art of War: Selected Writings (Novato, CA: Presidio Press, 1993); and Martin Samuels, Command or Control? Command, Training, and Tactics in the British and German Armies, 1888-1918 (London: Frank Cass, 1995).