Restrategizing Digitalization in the Military

Paul C. van Fenema
Pieter Soldaat

Digital innovation could lack relevance on the battlefield of the future due to challenges including realism, coherence, and effectiveness. Because the current paradigm is ineffectual, digitalization of the military requires a categorical reframing process. Military leaders must revisit digitalization and its role as a paradigm in enabling military organizations and operations. Three process phases are useful to reframe and reinstitutionalize the digitalization of the military: (1) reflection on the problem; (2) shifting of the framing categories; and (3) construction of the frame. As part of the third phase, four design paradigms will enhance digitalization in military processes: (1) establishing the primacy of nonpermissive ecosystem practices (the operational theater); (2) separating permissive and nonpermissive ecosystem practices; (3) paradoxical coupling of nonpermissive and permissive practices; and (4) investing in communication between humans first with strictly prioritized technological investments.

Military organizations have been investing in innovative concepts and digital technologies since the 1990s.*[1] Military organizations do this because they think they will gain an advantage in reference in terms of temporal and/or capability advantages to an enemy or gain a budgetary advantage for political reasons, basically gaining "more bang for the buck"—or at least the same bang for less bucks. The Dutch Ministry of Defense has already invested substantial amounts of money in digitalization and automatization. It recently published its *Defence Vision 2035*, detailing its move toward an even more data-driven organization.[2] As a result, billions of euros will flow to further digitalization. This trend is happening not only in the Netherlands but also elsewhere in the world.[3]

Dr. Paul van Fenema is a professor of military logistics and associate professor of organizational science at the Netherlands Defence Academy.

Lieutenant Colonel Pieter Soldaat, the liaison officer of the NATO Very High Readiness Joint Task Force brigade, holds a master in military history from the University of Amsterdam.

*The authors want to thank Tim Grant, the editors, and reviewers for their advice and support. We are also grateful to the Future of War Conference 2022 organizers and participants: https://faculteitmilitaireweten schappen.nl/.

1. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed., rev. (Washington, DC: C4ISR Cooperative Research Program, 2000).

2. Ministerie van Defensie, *Defence Vision 2035: Fighting for a Safer Future* (The Hague, Netherlands: Ministerie van Defensie, 2020), https://english.defensie.nl/.

3. "Chief Digital and Artificial Intelligence Office (CDAO)," CDAO, n. d., accessed March 27, 2023, https://www.ai.mil/.

Digitalization, requiring digital transformation, concerns the phenomenon that "work processes are increasingly intertwined with information technologies, enabling organizations to process large data sets and intelligently subtract and manage information, providing decision-makers with (supposedly) improved knowledge to support analysis and decisionmaking."[4] This article interprets digitalization in the military as a broad concept, affecting strategic processes such as dashboards, business processes such as 3-D printing and digital twins for maintenance and logistics, as well as operational processes such as command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) command and control, and targeting.

These investments are driven by notions like network-centric warfare or the sixth revolution of military affairs.[5] The underlying line of thinking builds on insights like networked military operations, investments in artificial intelligence (AI), and a belief in efficiency, and it resonates with similar ideas in the commercial world—such as Industry 4.0 and its digital transformation and servitization—relying on data, AI, control towers, and cross-organizational interactions.[6]

Specifically, AI has been defined as "scientific discipline, technologies used to realize AI, and AI capabilities."[7] It is also "the frontier of computational advancements that references human intelligence in addressing ever more complex decision-making problems," encompassing facets such as autonomy, learning, and inscrutability.[8] The assumptions undergirding these concepts and technologies tend to promise a novel type of digitalized military organization, preferably with ever fewer soldiers and more combat effectiveness.

But an important conceptual and empirical-professional problem emerges when relating these promises to the actual experiences regarding military digital innovation thus far and the characteristics of military operations in general. It has proven incredibly difficult, especially in the operational theater, to build digital and networked innovation in military organizations that would seamlessly connect enabling and operational processes.[9]

---

4. Therese Heltberg, " 'I Cannot Feel Your Print.' How Military Strategic Knowledge Planners Respond to Digitalization," *Journal of Strategy and Management* 15, no. 2 (April 2022): 220, https://doi.org/10.1108/JSMA-12-2020-0344.

5. Michael Raska, "The Sixth RMA Wave: Disruption in Military Affairs?," *Journal of Strategic Studies* 44, no. 4 (2021), https://doi.org/.

6. Catherine Bucaniec, "Russian Military to Develop Weapons Using Artificial Intelligence," C4ISRNET, August 17, 2022, https://www.c4isrnet.com/; and Johannes W. Veile, Marie-Christian Schmidt, and Kai-Ingo Voight, "Toward a New Era of Cooperation: How Industrial Digital Platforms Transform Business Models in Industry 4.0," *Journal of Business Research* 143 (April 2022), https://doi.org/.

7. Ida Merete Enholm et al., "Artificial Intelligence and Business Value: A Literature Review," *Information Systems Frontiers* 24, no. 6 (2022): 1712; and see also Greg Allen, *Understanding AI Technology* (Washington, DC: Joint Artificial Intelligence Center, Department of Defense, 2020), https://apps.dtic.mil/.

8. Nicholas Berente et al., "Managing Artificial Intelligence," *MIS Quarterly* 45, no. 3 (2021): 1435, 1437, https://misq.umn.edu/.

9. Mikayla Easley, "Skeptics of Services' JADC2 Plans Emerge," *National Defense*, August 15, 2022, https://www.nationaldefensemagazine.org/.

Since the early days of network-centric warfare in the late 1990s, major investments in comprehensive systems for both intra- and extra-theater processes have often been unsuccessful, with limited "power to the edge."[10] After 30 years, progress has been problematic, as shown by Dutch examples including Enterprise Resource Management's Systems Analysis Program Development (SAP), the weapon-storage system COLOR, and operational situational awareness systems such as the Battle Management System (BMS).[11] Even the long-promised paperless office has not materialized.

While such issues have been evident on a national-societal level, no interoperability has occurred on the joint combined interagency level, regardless of the huge investments that have been made. Digital disconnects experienced during international military operations have been reported repeatedly.[12] The build-up and teardown of modern-day command posts takes days, even weeks—much longer than the "analog" command posts of the Cold War. This extensive time commitment was witnessed during the NATO corps exercise Cougar Sword in Wildflecken, Germany, October 7–18, 2022. Indeed, modern military operations require an integrated set of complex digital and energy-providing technologies.[13]

Two questions emerge, one perhaps unpopular: Has the digitalization of the military concerning business and operational practices become trapped in blind optimism? Or has its realization turned into a modern version of the emperor's-new-clothes fairytale? At the very least, the current situation implies that military organizations face a major puzzle with respect to their strategies for digitalization. This is experienced first in the organizations responsible for nonoperational sustainment processes, such as the procurement and maintenance-sustainment organizations. Second, the operational organization at the front line experiences the ramifications of, for instance, choices for products, services, and companies that do not sufficiently lead to operational success.

And at the front line, a vivid concern is the introduction of future technologies that may only function under specific circumstances, with fixed processes and stable infrastructure, and that may collapse when energy, communications, or other vital infrastructure is destroyed.[14]

---

10. Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress*, RL32411 (Washington, DC: Congressional Research Service [CRS], 2007), https://apps.dtic.mil/.

11. Merel Vertegaal, "Development of a Battlefield Management System: How to Use the User" (The Hague, Netherlands: TNO Defense Research, June 1, 2001), https://apps.dtic.mil/; and Jan-Bert Maas, Paul C. van Fenema, and Joseph Soeters, "Post-Implementation ERP Usage: A Longitudinal Study of the Impact of Control and Empowerment," *Information Systems Management* 35, no. 4 (2018), https://www.tandfonline.com/.

12. Erik J. de Waard et al., "Learning in Complex Public Systems: The Case of MINUSMA's Intelligence Organization," *Public Management Review,* November 17, 2021, https://doi.org/.

13. Hind Benbya et al., "Complexity and Information Systems Research in the Emerging Digital World," *MIS Quarterly* 44, no. 1 (2020), https://papers.ssrn.com/; and Paul C. van Fenema et al., "Sustaining Relevance: Repositioning Strategic Logistics Innovation in the Military," *Joint Forces Quarterly* 101 (April 2021).

14. Sebastian Sprenger, "30 Years: Future Combat Systems – Acquisition Gone Wrong, *Defense News*, October 25, 2016, https://www.defensenews.com/.

Concerns about digital communications, digital signatures, and undesirable electromagnetic "presence" abound.[15]

So far, digital innovation as well as digitalization trajectories in military organizations are continuing in an uncoordinated fashion and without awareness of integration challenges.[16] A naive and civilian business-like vision seems to emerge that appears to advocate a mantra of substitution: new digitalized business will replace old business.[17] Moreover, digital innovation proves challenging to materialize cross-level integration, that is, how to relay information across hierarchical levels in and beyond the theater.

This is not to say that military innovations are not necessary. On the contrary, digital innovation runs the risk of lacking relevance in the battlefield of the future due to problems of realism, coherence, and effectiveness. The current paradigm does not work, due not only to practical problems but also for philosophical reasons. Digitalization of the military thus requires a categorical reframing process. This is especially important because given current international affairs, defense budgets will increase substantially in many countries. Such a reframing calls for a revisitation of digitalization and its role as a paradigm in enabling military organizations.

Restrategizing, like any strategic process, involves a process outlining steps to be undertaken and a content side indicating the gist of the strategy's direction.[18] Different views on strategic processes exist, including linear steps and "wayfinding"; this paper adopts the former view to provide an accessible argument.[19] Hence, upon setting the scene, this article proposes processual phases to guide the restrategizing process in terms of reframing. This article then offers design philosophies that operationalize the content side of a new strategy for digitalization in the military. It concludes with implications for research and practice.

Setting the Scene

"Ants and bees can also work together in huge numbers, but they do so in a very rigid manner and only with close relatives. Wolves and chimpanzees cooperate far more flexibly than ants, but they can do so only with small numbers of other individuals that they know intimately.

15. Andrew Eversden, "The Army Wants to Reduce Electronic Signatures of Its Command Posts," C4ISRNET, August 11, 2020, https://www.c4isrnet.com/.

16. van Fenema et al., "Sustaining Relevance."

17. Stella Pachidi et al., "Make Way for the Algorithms: Symbolic Actions and Change in a Regime of Knowing," *Organization Science* 32, no. 1 (2020), https://doi.org/.

18. Robert M. Grant, "Corporate Strategy: Managing Scope and Strategy Content," in *Handbook of Strategy and Management*, ed. Andrew Pettigrew, Howard Thomas, and Richard Whittington (London: Sage Publications, 2006).

19. Robert Chia, "A Process-Philosophical Understanding of Organizational Learning as "Wayfinding": Process, Practices and Sensitivity to Environmental Affordances," *The Learning Organization* 24, no. 2 (2017), https://doi.org/.

> *Sapiens can cooperate in extremely flexible ways with countless numbers of strangers. That's why Sapiens rule the world, whereas ants eat our leftovers and chimps are locked up in zoos and research laboratories."*
>
> Yuval Noah Harari[20]

Since the fall of the Berlin Wall, all militaries have cashed in on the peace dividend, as smaller armies became accustomed to outsourcing and relying on commercial innovation and technologies.[21] For many reasons, military organizations were treated increasingly as if they resembled commercial firms, becoming estranged from the harsh realities of the battlefield and engendering a lack of focus on the psychological and social domains. Assumptions undergirding commercial firms' digitalization then must be reflected upon in terms of how these assumptions apply to military organizations. These assumptions include engineerability; permissiveness of the context in which technology is used; a singular data reality such as shared, single-truth databases; and unidirectional or substitutive transformation toward digitalization.

Engineerability, recognizable in packaged software and business process projects, seems much less feasible in the military. This problem might not have been noticed earlier since many officers and civilian employees working for materiel commands and defense ministries are foremost educated as technicians and/or business managers, as is the case with the Netherlands Defence Academy. This has resulted in a growing tendency to depict the world as a system of systems, where humans are increasingly replaced by digitalization and where they structure their organizations and environment accordingly (fig. 1).

Figure 1 shows from top to bottom an analytics continuum ranging from descriptive use of technologies up to prescriptive use. Human input—light green—gets reduced, for example, shifting to merely checking technology or even being entirely removed from decision-making and action loops. One could also interpret this model using the OODA concept.[22] This is represented as a digital transformation paradigm that assumes an organization is changing at its core unidirectionally and in a substitutive sense toward a digital future (top to bottom in fig. 1).

20. "Yuval Noah Harari: Why We Dominate the Earth," *Farnam Street* [*fs*] (blog), accessed March 13, 2023, https://fs.blog/.

21. Ann Markusen, "How We Lost the Peace Dividend," *American Prospect*, December 19, 2001, https://prospect.org/.

22. James 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," *Defense Studies* 23, no. 1 (2023), https://www.tandfonline.com/.

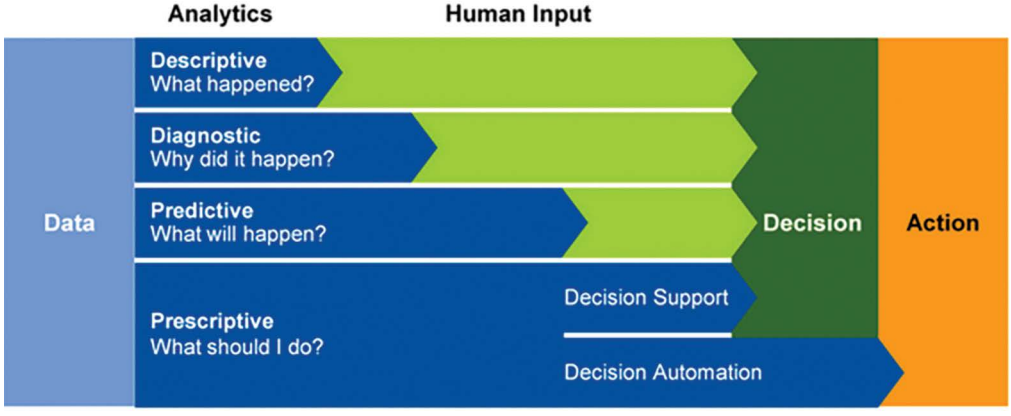

Figure 1. Analytics continuum[23]

This may work for born-digital and incumbent commercial and nonmilitary public organizations. But with a military confronted with real war, assumptions such as one data reality—wherein commercial firms tend to integrate their dispersed operations and rely on shared data and information technology, availability of data, and across-the-board transitioning toward digitalization—are too simplistic.[24] Optimism with respect to advanced digital technologies' capabilities and ignorance of the role of humans require critical reconsideration to avoid building a new military organization that could fail the test of future battle. Digitalization obviously plays a role in the targeting cycle, but this article rejects the ambition of an Internet of Things/Industry 4.0 vision for military operations.

This vision ultimately implies "autonomous decision-making within major functions in an organization. . . . The IT systems within the organization should completely support all the organization processes and they should be fully integrated."[25] After all, many digital technologies come with severe rigidities of routines, built on single-trust data lakes and unlimited connectivity that are rarely possible in operational circumstances.

At the same time, leveraging emerging digital technologies is still important. Military organizations must combine routine business operations with unpredictable theater operations. Therefore, the focus of technology differs across permissive and nonpermissive environments, where the military may or may not have the control or capability to support

23. Gertjan Hendriks and Rick Bouter, "The Analytics Continuum – Data Driven Decisions & Actions," *My Thoughts on Emerging Technology* (blog), February 27, 2018, https://rickbouter.com/.

24. Mary Zhang, "Data Lake: A Single Source of Truth in the Cloud," Dgtl Infra: Real Estate 2.0 (website), November 14, 2022, https://dgtlinfra.com/.

25. Michael Sony and Subhash Naik, "Key Ingredients for Evaluating Industry 4.0 Readiness for Organizations: A Literature Review," *Benchmarking: An International Journal* 27, no. 7 (2020): 10, DOI 10.1108/BIJ-09-2018-0284.

operations. Determining exactly how it differs addresses the challenge of restrategizing digitalization in the military.

A Categorical Reframing Process

Assumptions that apply to commercial firms are inadequate when considering digitalization as it concerns the military, but this can only be understood through a process of reframing.[26] If realities of war are incorporated, consultants, civilian IT professionals in the military, and military leadership can still join forces to digitalize the military but under an altered paradigm. Three process phases are useful to reframe and reinstitutionalize the digitalization of the military: (1) reflection on the problem; (2) shifting of the framing categories; and (3) construction of the frame.

Reflection on the Problem

The first phase reflects on the problem itself. With an increasing reliance on commercial digital innovation, the military has been mirroring in part the civilian need for process optimization, or efficiency, assuming its relevance in the theater. In the civilian world, process optimization might give competitors an advantage, but only because this world is stable, bound by laws and regulations, and therefore almost predictable. Even humans are thought to be dependable and predictable, perceived as cogs in the machinery, as evidenced in their job descriptions.

Yet process optimization supported by digitalization leads to ever more concentration of knowledge of the entire process to ever fewer people. Once digitalized, it will become harder to alter or change the "hardcoded" software for these optimized processes, because too few people know how to adapt these processes and their accompanying software. In fact, advanced digitalization increasingly introduces a paradox and vulnerability for adaptive military operations: pervasive use makes everyone depend on digital technologies, while in-depth expertise is restricted to a limited number of experts. A digital paradigm therefore requires a different view of supply chain logistics and reliability.

Moreover, the upkeep and maintenance of computer systems and especially databases are labor-intensive and require an elevated level of accuracy. Changes are often difficult to make, which is why databases frequently contain old data. This situation can be aggravated because often there is no benefit to the person who enters the data the first time—the data is only reused further up the chain. Feedback loops with the originator are frequently nonexistent, so the data originator does not know how far their input is processed in the chain or what is done with the input.

---

26. Barbara Gray, Jill M. Purdy, and Shahzad Ansari, "From Interactions to Institutions: Microprocesses of Framing and Mechanisms for the Structuring of Institutional Fields," *Academy of Management Review* 40, no. 1 (2015), https://www.jstor.org/.

User interfaces are also often difficult to design and implement, and even the underlying data model does not contain all the possibilities of the real world. Regarding the latter, in the military world, the data model of the NATO Multi-Lateral Interoperability Program (MIP) does not cover all military eventualities that can occur on the battlefield.[27] Moreover, standards for data exchange are often not adhered to, programmers make mistakes, interfaces are faulty, and national military organizations tend to prefer their own national digital technologies at the expense of interorganizational cooperation.[28]

Thus a computer network or a digitalized process can be prone to failure. While technical performance in a permissive environment has been extremely high, the military must increasingly consider kinetic and/or cyber attacks both within the theater and critical data infrastructures outside of the theater.[29] When it fails in practice, it is not uncommon that the user will start to work around these technologies to remedy the problem. For critical issues, a user will find alternative means to achieve a task, such as interpersonal, face-to-face, or remote communications using a repertoire of available technologies—telephone, WhatsApp, or commercial satellite communications. Sometimes users will do this because they know the person on the other end of the line/message. When this happens, the system is lost and will never recover and catch up with reality.

The implementation of digitalized processes already proves difficult in the civilian world, but it is much more so in the military world. For a number of practical reasons digitalization in an operational environment is not so easy. Just-in-time supply chain management—moving materials just prior to needing them for production—will not work because a military environment requires resiliency and redundancy.[30] Another civilian innovation, centralized inventory—with all stock kept in a centralized location—will provide juicy targets for an enemy. Moreover, the end user asking for resupply will have a tough time from a longer distance, since they often can formulate their demands only at an extremely late stage with little time left for supplies to be sent.

In a civilian context, an Amazon.com-style of e-commerce logistics has been extremely successful. It relies on data sharing, analytics, and fast inventory movement based on a flexible, partially outsourced network of individuals and companies. This will not work in the military. However fanciful or nice it would be to have something similar on the battlefield—for example, counting in realtime the ammunition expenditure of a vehicle and sending this in the network—this type of logistics is not necessary and

27. Eddie Lasschuyt et al., *How to Make an Effective Information Exchange Data Model, or The Good and Bad Aspects of the NATO JC3IEDM* (The Hague, Netherlands: NATO/OTAN, September 2, 2004).

28. Sebastiaan Rietjens, Erik de Waard, and Paul C. van Fenema, "Employing Comprehensive Intelligence: The UN Experience in Mali," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, ed. Paul A. L. Ducheine and Frans P. B. Osinga (The Hague, NL: Asser, 2017).

29. Christian Bueger, Tobias Liebetrau, and Jonas Franken, *Security Threats to Undersea Communications Cables and Infrastructure - Consequences for the EU*, In-Depth Analysis (Brussels: European Parliament, Directorate General for External Policies, Policy Department, April 2022), https://www.europarl.europa.eu.

30. Sandeep Phogat, "The Trouble with JIT in Military Operations: A Review," Line of Sight (Government of Canada), January 26, 2022, https://www.canada.ca/.

more importantly not robust enough. It might equate to giving a fool enough rope to hang themselves.

Digitalization of military operations will need a guaranteed communication layer, but this layer cannot be guaranteed. Furthermore, the improvised nature of this communications layer will require many technicians laying and sustaining the necessary mobile infrastructure. For this reason, numerous supporting communications support—vehicles and personnel—will be visible in the vicinity of command posts, which in itself paradoxically increases the vulnerability of the command posts.[31]

Digitalization also involves physical security demands, ungovernable roll-based access databases due to the high rate of personnel changes in a military outpost, crypto concerns, incompatible software, hardware problems, and significant downtime, so much so that the number of people and amount of effort needed to make this system work will possibly far exceed the advantages, assuming it would ever work. Furthermore, such digitalized processes are vulnerable to enemy action like counterintelligence, surveillance, and reconnaissance or information warfare.[32]

For more philosophical reasons, digitalization in an operational environment will prove difficult as well. The military world finds itself working under a set of paradoxes that is exactly the opposite of what applies to the civilian world.[33] Whereas in commercial firms, success, when repeated, will bring more success, in the military world the enemy learns from their adversary's previous successes, and if a solution is repeated, the enemy expects it, and thus it will likely fail.

The same applies for military solutions in general; the short road—hardcoded processes—to success will prove to be the bloodiest, just because an enemy will also expect this. Every hardcoded process will be watched by the enemy, making the organization vulnerable to enemy intrusion. Thus, it may be better to take the difficult road, which the enemy does not expect. This also calls for flexible and adaptable processes. Due to enemy action, such processes must and will change, and military organizations should therefore steer clear from digital-only and hardcoded process management.

For practical and philosophical reasons, organizations must be incredibly careful with process optimization and digitalization in the military. When the military implicitly mirrors civilian process optimization, it may end up with technologies that are out of touch with its situational needs, as illustrated in the Army's Future Combat Systems Program.[34]

---

31. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985).

32. David Hambling, "GPS Cyberattack Falsely Placed UK Warship near Russian Naval Base," *New Scientist*, June 24, 2021, https://www.newscientist.com/.

33. Edward N. Luttwak, *Strategy: The Logic of War and Peace*, 2nd ed. (Cambridge, MA: Belknap Press, 2002).

34. Christopher G. Pernin et. al., *Lessons from the Army's Future Combat System* (Santa Monica, CA: RAND Corporation, 2012), https://www.jstor.org/.

Shifting Framing Categories

The second phase in the process to reframe the digitalization of military operations concerns the shifting of one category of frames toward another one. A frame is defined as a " 'schemata of interpretation' . . . that actors use to affect the interpretation of events among different audiences"; frames "simplify and condense the 'world out there' by selectively punctuating and encoding events in order to render them meaningful . . . keeping some elements in view while hiding others."[35]

Categories matter as they structure frames people use.[36] Instead of business digitalization as a category, military operations should be an alternative starting point. This resembles a similar shift in military logistics and asset management.[37] The theater poses unpredictable challenges to the military across multiple domains.[38] Engineerability, artifacts, and a systems world—the conceptualization of reality—give way to the harsh reality and experience of warfare.

This argument resonates with the rejection of systemic operational design. Instead, this article advocates a holistic and primarily linear process of designing and planning operations and a preference for improvisational thinking over technical thinking.[39] According to this view, "Military design has particularly emphasized the value of creativity for waging war . . . [and it] connects to longstanding debates in military theory, and particularly to the work of Carl von Clausewitz, who is considered the first to have emphasized chance and creativity as essential characteristics of warfare."[40]

The belief in a "mechanical" worldview was officially abolished in the US military by then Commander, US Joint Forces Command General James N. Mattis (later the US Secretary of Defense) in 2008.[41] He noted the system-of-systems approach led to ever-growing command posts and multiple layers of staff and maintenance personnel yet ultimately produced nothing but "overextension and confusion."[42] He also proposed a return to the

35. Peer C. Fiss and E. Zajac, "The Symbolic Management of Strategic Change: Sensegiving via Framing and Decoupling," *Academy of Management Journal* 49, no. 6 (2017): 1774, https://doi.org/.

36. W. Ocasio, J. Loewenstein, and A. Nigam, "How Streams of Communication Reproduce and Change Institutional Logics: The Role of Categories," *Academy of Management Review* 40, no. 1 (2015).

37. van Fenema et al., "Sustaining Relevance."

38. Bradley Cooper, "Precision Logistics: Sustainment for Multi-Domain Operations," *ILW* [Institute of Land Warfare, Department of the Army] *Spotlight* 19-4 (September 2019), https://www.ausa.org/.

39. Milan N. Vego, "A Case against Systematic Operational Design," *Joint Force Quarterly* 53 (2009).

40. Dan Öberg, "Warfare as Design: Transgressive Creativity and Reductive Operational Planning," *Security Dialogue* 49, no. 6 (2018): 494, https://doi.org/.

41. James N. Mattis, "USJFCOM Commander's Guidance for Effects-Based Operations," *Parameters* 38, no. 3 (Autumn 2008), https://apps.dtic.mil/; and see also Mattis, Memorandum for US Joint Forces Command, Subject: Assessment of Effects Based Operations, August 14, 2008, https://smallwarsjournal.com/.

42. Mattis, "Effects-Based Operations," 19.

acceptance of a more complex and chaotic worldview described by von Clausewitz, where people react to people.[43]

New thoughts on military operations include warfare principles and concepts such as surprise, complexity, and nonroutine exploitation of opportunities. Threats can come from any dimension in unpredictably ordered patterns. Successful action depends on breaking patterns and surprising and seeking the unknown, rather than on enacting scripts. Taking military operations as the anchor, military organizations should not advocate only incremental innovations. In fact, disruptive technologies include weapons never envisioned in a linear process, such as atomic bombs and helicopters.[44]

If military operations is a foundational category for framing and designing digital innovation, an open-minded approach is of paramount importance. This starts with strategic mental versatility. This is not surprising given the extreme context of military operations that requires major versatility.[45] Military organizations must have redundancy and holographic modes of organizing to keep functioning under any conditions and avoid easily detectable centers of vulnerability, for example, a single point of failure.[46] That is, organizational modules have their own comprehensive functionality enabling replacement and combination.[47]

This structural redundancy necessitates organizational simplicity. Reflection on framing implies distancing from an institutionalized way of thinking that does not serve the military, specifically the normalized yet problematic crossover between business-type digitalization and the military.[48] This process requires that military organizations "complicate" themselves, rejecting known thought patterns based on previous categories.[49]

Frame Construction

Taking military operations as the category, frame construction becomes the third phase in the process of reframing military operational digitalization. This provides a new take on the interplay of human and technology agency.[50] Starting points are realistic assumptions, such as the unavailability of data, fake data, and lack of energy resources.

---

43. Antoine Bousquet, "Chaoplexic Warfare or the Future of Military Organization," *International Affairs* 84, no. 5 (2008).

44. We thank one of our reviewers for this insight.

45. Theo Farrell, Frans Osinga, and James A. Russell, eds., *Military Adaptation in Afghanistan* (Redwood City, CA: Stanford University Press, 2013).

46. de Waard et al., "Complex Public Systems."

47. Gene I. Rochlin, Todd R. La Porte, and Karlene H. Roberts, "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea," *Naval War College Review* 51, no. 3 (1998).

48. Satish Nambisan, Mike Wright, and Maryann Feldman, "The Digital Transformation of Innovation and Entrepreneurship: Progress, Challenges and Key Themes," *Research Policy* 48, no. 8 (2019).

49. Eric-Hans Kramer, *Organizing Doubt: Grounded Theory, Army Units and Dealing with Dynamic Complexity* (Copenhagen: Liber/Copenhagen Business School Press, 2007).

50. Alex Murray, Jen Rhymer, and David G. Sirmon, "Humans and Technology: Forms of Conjoined Agency in Organizations," *Academy of Management Review* 46, no. 3 (2021).

Priority is given to reliable and secure communications and to providing situational awareness to human actors at all levels within and beyond a theater. All humans at all levels are to be capable of thinking for themselves.

In 2022, for the first time, a communication layer was established on which the digitalization of the battlefield could take place. Thousands of Starlink terminals made by SpaceX were deployed over Ukraine in order "to help Ukrainian troops operate drones, receive vital intelligence updates, and communicate with each other in areas where there [were] no other secure networks."[51] Yet widespread outages were reported, leading to "catastrophic" losses of communication in liberated areas and along the front line.[52] Until then, Starlink had proven relatively robust and secure, although it also had to be made jamming-resistant.

With a communication layer established, humans should be able to communicate with each other with whatever digital means are available. Only a connected ring of people working under mission command can adapt and improvise continuously to encountered problems or enemy interference. This idea resonates with literature on high reliable organizations, which stresses, for instance, "heedful interrelating" to understand the context of an evolving crisis and cooperating parties.[53] This should be the orientation of digital innovations and a norm for critically (re)considering efforts in the military to improve or fix automated processes, whether logistical, decision-making, or tactical.

Design Paradigms Starting from Military Theater Operations

As part of the third phase, four design paradigms will help successful digitalization in military processes: (1) establishing the primacy of nonpermissive ecosystem practices (the operational theater); (2) separating permissive and nonpermissive ecosystem practices; (3) paradoxical coupling of nonpermissive and permissive practices; and (4) investing in humans first.

Primacy of Nonpermissive Ecosystem Practices

A first approach acknowledges that while a strategic intent for an operation is likely to be relatively stable, materializing this intent is unpredictable, as the current war in the Ukraine illustrates.

The operational world is chaotic, inducing new forms of military operations. This concept is also referred to as chaoplexity—which acknowledges the order inherent within

51. Mehul Srivastava et al., "Ukrainian Forces Report Starlink Outages during Push against Russia," *Financial Times*, October 7, 2022, https://www.ft.com/.

52. Srivastava et al., "Starlink Outages."

53. Karl E. Weick and Karlene Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* 38, no. 3 (September 1993): 357, https://www.jstor.org/.

chaos and complexity—as a sequel to networked operations.[54] Military operations in the theater do not rely on process optimization but on unpredictability, asymmetry, secrecy, and obtaining advantage across domains. People will try to outsmart each other, including through electronic warfare and information warfare.[55] Ukraine blows up bridges; Russia will use pontoons. Ukraine destroys ammunition depots with HIMARS rockets; Russia will spread its depots in attempts at decentralization.

In order to be able to adapt and improvise, military operations must prioritize communication between humans. For instance, the authors experienced remote communication challenges during an exercise in Norway, which demonstrated the key role of human-to-human communication. The satellites were just at the horizon, resulting in the satellite dishes pointing into the ground. Military radio signals were dampened by the thick, wet forests, and civil 4G networks had no coverage. Command posts thus had to fall back on military personnel using motorcycles to deliver messages on USB sticks. This manner of communication may seem outdated, but such a measure may be required in the overall repertoire of operations as the situation demands it.

Separating Permissive and Nonpermissive Ecosystem Practices

Civilian corporate resources are mostly prohibited from nonpermissive environments. Their concepts of networked digital services are not likely to play a useful role in such unstable, uncertain environments. First and foremost, under the law of armed conflict, civilians may become legitimate combatants and therefore targets if they assist one side over another.[56] Moreover, commercial sources may also be considered fair game, as indicated by the argument that SpaceX satellites are now a legitimate military target.[57] This article proposes a separation between extra- and intra-theater paradigms, each with their own set of problems. The split is likely to occur between the operational theater supply chain and extra-theater defense industrial base, implying a novel focus for digital innovation: not a highly mature digital network, but a network that keeps working.[58]

This separation between permissive—extra theater—and nonpermissive—intra-theater—applies also to high-tech assets used in military operations in the theater. These technolo-

54. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009).

55. Farrell et al., *Military Adaptation*; and Mykhaylo Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," Royal United Services Institute for Defence and Security Studies (RUSI) (website), November 30, 2022, https://rusi.org/.

56. "The Practical Guide to Humanitarian Law," Medicins Sans Frontieres [Doctors without Borders] (website), accessed March 13, 2023, https://guide-humanitarian-law.org/.

57. Tara Brown, "Can Starlink Satellites Be Lawfully Targeted?," Lieber Institute, West Point (website), August 5, 2022, https://lieber.westpoint.edu/.

58. Raffaele Della Croce et al., *Building Resilience: New Strategies For Strengthening Infrastructure Resilience and Maintenance* (Paris, France: Organisation for Economic Cooperation and Development, 2021), https://www.oecd.org/.

gies increasingly rely on advanced servitization, data-driven analytics pertaining to assets and service logistics, and constant fleet-level learning, such as Tesla's practice of leveraging its large fleet of cars for machine learning. These digitalization trends exemplify the unidirectional and comprehensive transition toward the "cognitive enterprise," relying heavily on integrated computing platforms for operating. Concepts such as platforms, standardization, and visibility optimize multiple business processes outside of the theater. But they must be put on hold in a nonpermissive context.

Artificial intelligence may support units if sufficient data is available, with units flexibly reverting to non-AI modes when deemed beneficial or necessary. This implies a transition in mindset and a check-in/check-out process when units move toward or out of a nonpermissive environment. Their systems may have only partial data collection leaving the nonpermissive environment. This requires the optimization-oriented organization to pick up the pieces and "recharge" advanced technologies in cooperation with industry, as the challenges with standards based on models such as NATO's Joint Command, Control, and Consultation Information Exchange Data Model (JC3IEDM) and earlier Army Tactical Command and Control Information System (ATCCIS) illustrate.

Yet limited maintenance and update facilities are available in the theater. Moreover, relying on data sharing across networks for remote support is risky and often impossible. Hence, to serve military operations, the digital innovations remain concentrated in the asset—such as a weapons system—and on hold until the asset reappears in the permissive environment. Moreover, sustaining capabilities to deal with old technologies remains relevant, as the Ukraine conflict illustrates.

Paradoxical Coupling of Nonpermissive and Permissive Practices

Coupling implies that design is geared toward operations dominating, but it needs to provide room for another type of design.[59] Intra- and extra-theater practices of the digital ecosystem coexist yet not in an equal manner. In addition, they depend on inter-human communications to ensure mutual understanding. Such coupling is paradoxical because the diversity of the two ecosystems—intra-theater versus extra-theater—implies contradictory requirements and paradox management.[60] Figure 2 shows a split between permissive and nonpermissive environments.

As an exception, cyberspace, according to Joint Publication 3-12, *Cyberspace Operations*, is a recognized nonpermissive environment.[61] On the left, efficiency (low stocks), concepts like just-in-time management, and comprehensive technologies rule the game; on the

59. Öberg, "Warfare as Design."

60. Wendy K. Smith, and Marianne W. Lewis, "Toward a Theory of Paradox: A Dynamic Equilibrium Model of Organizing," *Academy of Management Review* 36, no. 2 (2011).

61. Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: CJCS, June 8, 2018), https://irp.fas.org/.

right, redundancy (just-in-case stock management—the storage of large inventories to prevent shortages) and resilience rule.

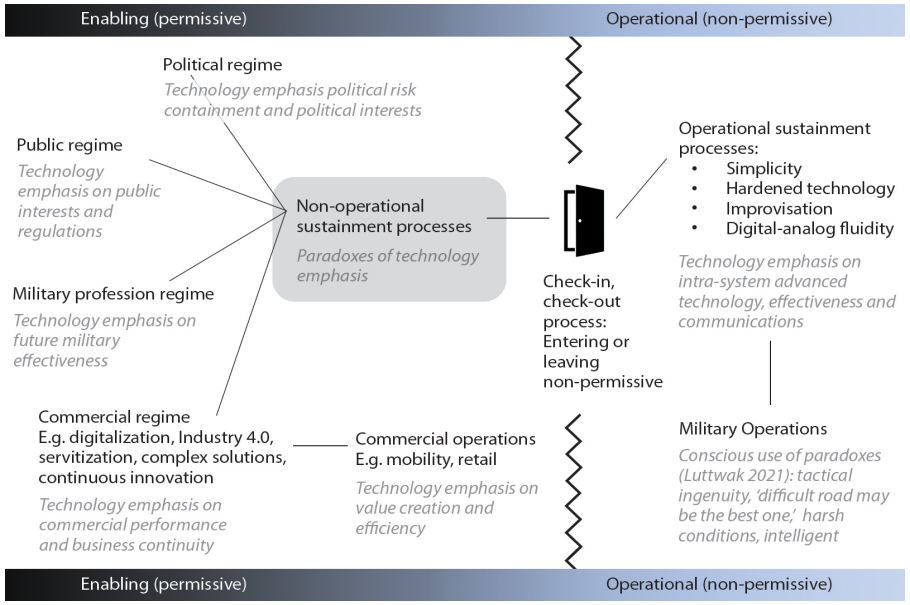

Figure 2. Digitalization in the military

The paradox also applies to complexity-simplicity: in the permissive environment, technical complexity prevails to optimize processes. The coupling is different from coexistence since military operations dominate the overall ecosystem in nonpermissive environments. For instance, this could mean that in the permissive environment, decisions are made that differ from regular business.

Where possible, communications from inside to outside the theater offer chunks of information to be analyzed using digital capabilities outside of the theater. Incomplete information is a starting point rather than a nuisance to a model, assuming single-truth data sets that are complete.

Humans First

In a highly automated world, people are both the problem and the solution. They are the problem because they are forced to improvise in unpredictable ways and they make mistakes, such as software engineers creating faulty software, military units forced to use unreliable equipment due to political/industrial machinations, or maintenance personnel and operators typing errors. At the same time, humans are also the solution. Whereas a computer will signal a system error and halt operations when a mistake or issue is encountered, humans will talk to each other and will attempt to resolve the issue by improvisation, and the process does not stop.

Therefore, militaries must invest in human interaction first in a chaoplexic environment. For example, in 2006, a simple chat program, J-chat, proved to be the most useful and most-used program of all computer systems in the International Security Assistance Force (ISAF) domain in Afghanistan, and it continues to be so in modern-day command posts. Even radio broadcasts were transcribed into written chats so that everyone in theater could subscribe to and read what was happening with platoons operating in other sectors that were normally out of range. Additionally, people would chat to each other when an icon on a screen was distrusted, because, for example, it had not moved for awhile. This interpersonal communication also gave a form of feedback and acknowledgement.

In chaotic environments, only humans can adapt. There is no room for integrated cross-process automation. In the operational environment, processes should be as short as possible and connected to each other by humans. Humans ( ) must interlink multiple processes so that these processes can quickly be rearranged ( ):[62]

Instead of striving for all-encompassing automated systems, then, one should divide the process into smaller components where humans can intervene, interrelate, and improvise. While humans interlink processes using technologies, this article acknowledges the demarcated usefulness of autonomous data flows. This approach creates overdependence on humans and leverages humans' higher cognitive capabilities. Therefore, the approach has to be nuanced with the idea that AI and automatization can or even must be implemented for short-term processes where the reaction time of human operators may prove to be too long, such as with air-defense systems on ships and Iron Dome-type settings.

In any case, every computer system or automated process should be highly accessible and understandable.[63] These should also be equipped with a manual override button, figuratively speaking. The notion of conceptualized workflows as common in business process design and packaged software does not fit in a nonpermissive operational environment.

There are three final thoughts on process aggregation and AI: On one hand, within demarcated subprocesses, AI may increasingly speed up decision-making and leverage vast amounts of data, if these are available. On the other hand, for aggregated-composed series of subprocesses, military organizations run the risk of AI combining processes in an inaccessible, incomprehensible, and possibly undesirable fashion. Also, thought should be given to how susceptible computer AI is to deception, as compared to humans. At the same time, in the future, they may be able to control interlinked subprocesses and rely on

62. Clay Bartels, Tim Tormey, and Jon Hendrickson, "Multidomain Operations and Close Air Support: A Fresh Perspective," *Military Review* (March–April 2017), https://www.armyupress.army.mil/.

63. Peter Svenmarck et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications," in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting* (Bordeaux, France, May-June 2018), https://www.foi.se/.

AI. This applies in particular to theaters combining absence of noncombatants and urgent pressure to transition to extreme levels of warfare speed and span of control. As US Secretary of the Air Force Frank Kendall mentioned in 2021:

> This year, the [Air Force's] chief architect's office deployed AI algorithms for the first time to a live operational kill-chain at the Distributed Common Ground System [DCGS] and an air operations center for automated target recognition. In this case, moving from experimentation to real military capability in the hands of operational warfighters significantly reduced the manpower-intensive tasks of manually identifying targets—shortening the kill chain and accelerating the speed of decision-making.[64]

Conclusion

A categorical shift in strategizing digital innovation for military organizations is needed. This opens space for four design paradigms applicable to service ecosystems, which when combined offer a novel approach to digitalization in the military. Starting from chaoplexity, this article seeks a new mode of engaging multiple specialists in a concurrent fashion with innovative objectives derived from the operational context and future technologies.

Military operations—within an operational theater—represent the primary subecosystem driving design efforts. Such design is separated from extra-theater ecosystems but still (paradoxically) coupled. This research has implications in four areas.

Digitalization in the Theater

Rejecting transposition of commercial concepts as a primary move, future research can start with properties of military operations, both generic ones informed by history and those emanating from the current and upcoming era of partial digital and multidomain warfare. Considering electronic warfare awareness and how to remain unnoticed are starting points for design rather than afterthoughts. Communication is reduced and secrecy is enhanced when units are logistically independent and have a certain number of their own supplies, not needing to ask or communicate a logistical need.

Controlling Networks within and beyond the Theater

Conceptualization has evolved quite separately in different communities of practice such as military academics and nonmilitary business studies orienting toward commercial firms and permissive environments. How is the chaoplexity of the theater coupled with supply chains that operate in a more routine fashion? A gradual transition from nonmilitary business value chains towards boundary spanning military(-ish) supply chain

64. AutoNorms WebAdmin, "Shortening the Kill Chain with Artificial Intelligence," AutoNorms (website), November 28, 2021, https://www.autonorms.eu/.

organizations and onwards to the military operation deserves more research. This includes possibly inevitable public-private frictions.[65]

Moreover, organizations assuming they operate in a permissive environment may have to consider risks in a total-war situation, including cyber attacks and espionage.[66] Digital technologies such as meta and digital twins may overlayer permissive and nonpermissive operations and support conflict resolution across the entire chain. To achieve network control, more insights in the interplay of formal command chains and informal, often lateral, communications are needed.[67]

Human and AI Interplay in the Military Context

Strong military operational validation is paramount; this concerns testing concepts, technologies, processes, and people under nonpermissive circumstances. New insights are needed to enable fluidity of shifting between advanced digital and simple analog ways of working, while acknowledging the importance of simplicity and improvisation.[68] Instead of opting for one digital transformation strategy, as is common for businesses, the military may need many or all of them in the theater, maybe even being "proud to be analog."[69]

Diversity of Communications

Finally, more than process automatization, militaries should prioritize the ability to communicate between human operators with a diversity of means. This effort entails ensuring fall-back options under any circumstances that can deal with complexity and fragmentation and allow for improvisation and adaptation.[70] Accordingly, this article encourages communication technology, but it is hesitant with respect to automation technology, especially in a nonpermissive context. As Yuval Harari noted above, homo

65. Peter Tatham, "An Exploration of Trust and Shared Values in UK Defence Supply Networks," *International Journal of Physical Distribution & Logistics Management* 43, no. 2 (2013).

66. Elad Bengigi et al., *Logistics in Contested Environments* (doctoral dissertation, Naval Postgraduate School, 2020), https://www.academia.

67. Rob Sinterniklaas, "Future of Command Relationships: Lessons from an Ancient Land" (conference paper, The Future of War Conference, Amsterdam, October 5–7, 2022).

68. Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1984).

69. Zeljko Tekic and Dmitry Koroteev, "From Disruptively Digital to Proudly Analog: A Holistic Typology of Digital Transformation Strategies," *Business Horizons* 62, no. 6 (2019).

70. Jeroen Wolbers, Peter Groenewegen, and Kees Boersma, "Introducing a Fragmentation Perspective on Coordination in Crisis Management," *Organization Studies* 39, no. 11 (2018).

sapiens won the race because they communicated. Therefore, digitalization should support the flexible cooperation of strangers relying on swift trust, including technological actors such as AI and robots.[71] ✈

71. Steve Curnin et al., "Role Clarity, Swift Trust, and Multi-Agency Coordination," *Journal of Contingencies and Crisis Management* 23, no. 1 (March 2015), https://doi.org/.