Influencing Populations on the Strategic Battlefield

Concepts of Warfare in Operational Environments of the Future

by Martin Nilsson

Resumé

För att vi ska kunna genomföra gemensamma operationer i framtidens operationsmiljö måste vi nogsamt analysera bedömda och önskade militära förmågebehov samt därtill planera vilka förändringar vi behöver genomföra. Med utgångspunkt i koncepten *Multi Domain Operations* och *New Generation Warfare* analyseras den framtida militära krigföringsförmågan. Artikeln framhåller bland annat befolkningens roll i den framtida krigföringen. Informationsdomänen får ökat fokus eftersom det är en operationsmiljö där fler intressenter befinner sig. Tempot och mängden av informationshantering ställer stora krav på de kombattanter som befinner sig däri vilket medför ett stort behov av en tydlig ledningsfilosofi. Tydlighet kommer även vara en faktor när det kommer till att avgöra vilka som är kombattanter eller inte i operationsmiljön, vilket kan göra icke-kombattanter extra utsatta i ett cyberkrig som troligtvis bedrivs både under lång tid och på djupet. Andra tunga framgångsfaktorer är kulturell förståelse och förmågan att utrycka sig på ett koncist och tydligt sätt i multilaterala sammanhang för att bibehålla handlingsfrihet och initiativ i framtidens operationsmiljö vid genomförandet av parallella gemensamma operationer mellan domänerna i hög hastighet. Vi måste tidigt identifiera och avbryta antagonistiska hot att störa bi- och multilaterala överenskommelser eller försök att förstöra suveräna stater.

IF YOU WANT peace, prepare for war.[1] Edward Luttwak's paradox is logical to a certain degree, but what type of war should nations prepare for? One certainty is not to prepare for anything that has already taken place. History shows that the nature of war will remain unchanged, and acts simultaneously as a roadmap during uncertainty.

To understand future conflict, a qualified assessment of current and future contexts must be conducted.[2] Regardless of the quality of contextual assessment, each war is a unique case with its own logic.[3] Consequently, well-recognized military theories for analyzing future conflicts combined with contextual assessments should indicate how to be victorious in 2035 and onwards. The theories of Isserson and Douhet could serve as guides to the battlefields of the future.

Current and future societies are increasingly connected via the "new" cognitive/human/information domain, which gives civilian populations a prominent role in future conflicts, and makes civilians "unaware" combatants in the conflict. Thus, it follows that future conflicts will likely see adversaries attempt a deep offensive battle that aims to influence the willingness of a population to defend themselves against foreign actors. This paper will lay out an explanation on how deep battle with non-military measures

could affect the human will deep beyond our area of operations.

The central military theories used in this paper entail concepts like maneuver warfare, deep battle, and mission command as command philosophy, but also theories concerning a population's role in war. Furthermore, focal points for the analysis will be the Multi Domain Operations (MDO) and New Generation Warfare (NGW) concepts. This article does not focus on contemporary or futuristic innovations, but instead the timeless catalyst off all action – humans. Furthermore, this paper is written from a Swedish perspective although the greatest ambition is a global perspective--a perspective for the future.

Defining the Operational Environment of Future Conflicts

To analyze the Operational Environment (OE) comprehensively, political, military, economic, social, infrastructure, and information (PMESII) factors are considered.

First, regarding political factors, sovereign states hold absolute monopolized power over the use of violence and acts of aggression. Furthermore, no common absolute definition of war exists as the acts of aggression defining an armed conflict refer only to physical kinetic acts. Consequently, this enables information and cyber operations to proceed with abundant freedom of action and impunity. Therefore, numerous actors can currently achieve their objectives under the threshold of armed conflict.[4]

Second, regarding military factors, the world's leading superpowers hold similar kinetic capabilities and are evenly matched on the current battlefield. While a quantitative focus on non-military methods now and in the future is vital, military methods must simultaneously stay vigilant and agile to protect all assets and infrastructure in all domains. The range of security tasks is wide from physical protection of webservers to electronic countermeasures built into satellites. The nuclear weapon threat will be excluded in this analysis due to its main goal being a strategic method for deterrence more so than a tactical/operational weapon system, for as long as a global balance in means and ways exists, the ends will stay the same.

Third, for economic factors, global trade is likely to increase in complexity and integration with new technical innovation in the service, transportation, and manufacturing sectors. Global trade will consequently be more vulnerable to disturbances which can cause severe consequences for a population and their resilience to withstand pressure from foreign actors. Over time economic pressure from foreign powers can manipulate a population's willingness to defend themselves in favor of the foreign power.

Fourth, social factors like culture and history have naturally had, and will continue to significantly shape how various sovereign states act. Furthermore, these factors will influence how each nation prioritizes the aforementioned factors (PMES), including their approach to new innovation and/or adopting/emulating others' experiences or methods. Aside from these factors, because an adversary can conduct operations below the threshold of armed aggression, the population becomes a key actor in future conflicts, or as General (ret.) Mattis recognizes, a nation's population is a key terrain.[5]

Fifth, discussing infrastructure, both physical and non-physical factors must be accounted for. Space will be the main domain which will see the greatest physical change in the future. Super-constellations of small satellites will enhance the communication,

weather forecasting, surveillance, positioning, and timing capabilities, drastically improving all situation awareness.[6] The future challenges lay more in bandwidth than the physical space available. Another challenge is to find a solution to rapidly replace satellites in space using a flexible, concealed, and affordable system.

Sixth, information factors include how transparent the world is becoming. Enormous amounts of data are collected from e.g. satellites. Today humans cannot manage all the crude data. To match the tempo of future conflicts, initially machines or artificial intelligence (AI), rather than humans, will exploit data.[7] The challenges therein include receiving information that is accurate regarding time, space, and force. Additionally, too much information, inaccurate, or partly inaccurate information will severely impair the decision-making process.

Last, the infrastructure of the future, especially in space, will lead to complete transparency. Non-linear warfighting means a shift in focus to non-kinetic warfare. The cyber domain constantly changes, which is why a long-term concept must be endeavored, regardless of technological innovation. The worldwide governance in cyber law must be developed in order to prevent power projection under the threshold of armed conflict. Collateral damage as a result of offensive cyber operations must have legal consequences. Also, future technology will make the environment, or battlefield, non-linear and unpredictable.[8]

Analytical tool

To analyze and discuss future warfare the "Warfighting Capabilities-temple," used in the Swedish military strategy doctrine, will be used. The warfighting capabilities rest on three pillars: physical factors, conceptual factors, and moral factors. Each pillar highlights crucial factors that collectively provide a balanced and effective warfighting military. The analysis starts with the conceptual perspective, followed by the physical and moral perspectives.

Conceptual perspective

The MDO concept, covering a global battlefield, is based on simultaneous operations across all domains, presenting many potential threats to the adversary and thereby overloading the decision cycle and allowing the joint force to seize and retain the initiative.[9] In order to master simultaneous, multi-domain influence and manage massive amounts of information at high speed, humans will certainly need AI support.

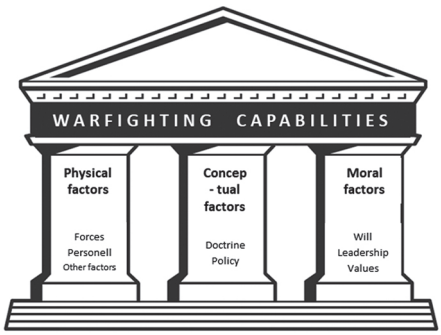

Figure 1. Warfighting capabilities, Swedish military strategy doctrine.

William S. Lind discusses maneuver warfare in his handbook, highlighting decentralized command & control (C2). The decentralization makes the decision-making process more effective by out-speeding the enemy who will eventually lose its unity of forces. Subsequently, the ability to fight effectively and in an organized manner is terminated.[10] Considering this, the MDO concept can be seen as a type of maneuver warfare with focus on C2, more so than fire and maneuver.

Furthermore, how AI is trained to "understand" the commander's intent and act accordingly should be considered. In order to mass one's combat power in time and space, and present the enemy with multiple dilemmas, the force must have a well-established multi-domain integration in addition to multilateral integration.[11] The organization must act in a complex, nonlinear, yet uncomplicated manner in order to preserve freedom of action. C2 methods that worked in early 21th century for NATO might not be appropriate for the new MDO-concept.[12]

Clearly, the MDO concept relies on a multilateral endeavor. For future alliances to be formed among sovereign states, the alliances' strategic goals must align with each individual, sovereign state's strategic goals; otherwise, the alliance is inefficient and less effective in the high tempo cyber battlefield. Lastly, the more integrated and complex a warfighting machine becomes, the more integrated the alliance's strategic goals must be, which can be troublesome regarding divergent relations to e.g. China.

In his book, Jonsson discusses different views on NGW, which he defines as the main battlespace, namely the mind, consciousness, perception, and strategic calculus of the adversary that are influenced by information and psychological warfare.[13] This corresponds to Col. Connor, who argues that perception is the main battlespace, and that kinetic operations will support the desired end state when necessary.[14]

Russian leadership has set an approximation regarding the relation between military/non-military measures. Based on what has previously been discussed, it can be assumed that the most effective way to reach your strategic objectives in the future is though non-military methods. This reminds us and again validates Sun-Tzu's words about the skilled strategist and victory without bloodshed.[15]

As Russian methods focus on expanding information operations and subversion, they concurrently isolate their own societies from supposed western influence. Allen & Moore states that subversion, as a general rule, cannot create political divisions, but merely exploit existing divisions within a population.[16] Again, the population is becoming an actor, or an indirect tool, to shape political opposition.

Along with the argument about shaping an adversarial population, Deep Battle architected by G. s Isserson, must be highlighted. The theory is defined as "simultaneous containment and suppression of the enemy's entire tactical depth", and traditionally refers to conventional kinetic warfare.[17] Isserson warns about "[the] strong points in the depth of the enemy position… [to] form the backbone of a new defensive position".[18] It can be argued that deep battle has been further developed from tactical-[operational] to strategic level and applied in asymmetric warfare using information operations in the entire depth of the enemy where the population is the backbone of the enemy's defensive positions.

Regarding asymmetric warfare, or rather the fixation on hybrid warfare, it can be said that it is not representative of the broader military development in Russia.[19] Bartles notes that hybrid war refers to a much narrower scope of activities than the term "indirect and asymmetric" methods.[20] Additionally, Bartles argues that Russian practice of hybrid warfare is one of the most misunderstood aspects of Gerasimov's article.

Physical perspective

At the strategic level, the MDO concept needs to effectively compete below the threshold

of armed conflict, deterring an escalation. Should deterrence fail, the capability to prevail in the next phase must be maintained. Considering long-term strategies, the capability to defeat two peer-level adversaries simultaneously must also be developed.[21] At the operational level, there must be a base plate for all MDO-allies. Capabilities like JISR, JTGT, JFS, and JSA[22] should be considered areas for implementation with high level of integration and interoperability.

Considering Gerasimov's ratio in military versus non-military measures with methods like "formation of the political opposition" in the initial phases of a conflict, it is remarkable that Perkins' drafted battlefield model fails to address the non-military threat.[23] Considering that fact, Perkins' model focuses far too much on the physical and kinetic types of warfare, and far too little on information operations where the population is the central target. Furthermore, Perkins' model is based on a comparison to air-land battle concept, naturally centering conventional warfare. In contrast to Perkins' conventional warfare focus, McFate writes that no one fights conventional war anymore, and that it has such a strong dogma that all other warfare is called unconventional.[24] Everything we know about the nature of future kinetic war is its characteristics: chance, luck, friction, and some additional principles of war. Context, ends, ways, and means will always differ. Consequently, excluding any type of warfare could have serious consequences for the future war fighting capability.

The NGW concept still calls for a robust military. The main focus of Russian kinetic fighting powers are merely offensive and defensive operations using brute force, maneuver warfare and operational deep battle in increasingly integrated joint operations. Nuclear weapons, although mainly seen as a strategic weapon for deterrence remain an agile means, and together with the conventional forces, represent important means in national power to achieve a state's ends. Regardless of the measures and ratio, the adversaries will be impacted with simultaneous effect throughout the entire depth of its territories.[25]

Russian anti-access – area denial (A2AD) capability has been frequently discussed with divergent conclusions. It can be understood, similar to the hybrid warfare concept, that A2AD capability is not representative for Russian strategy outside its territory, due to the A2AD's defensive nature. Kofman argues in a likely manner saying that A2AD doctrine does not exist, and that contemporary capabilities or components are organized differently. Kofman indicates that the western world's misunderstanding is a result of technological fetishism combined with threat inflationism, thus overrating actual Russian organization and A2AD strategy.[26]

Moral perspective

The MDO concept relies on interoperability, i.e. common standards, doctrines, and procedures. To achieve and maintain the required level of interoperability there are numerous variations in technological aspect. Human factors, conversely, are applicable to all nations. Interoperability requires the understanding of cultural differences and is central in the end result. For military contexts, an excellent way to be exposed to other cultures is through exchange in professional military education (PME).[27] Besides knowledge of cultural differences, one learns other states' strengths and weaknesses and expertise areas which is imperative in operations.[28] Besides PME, a well-recognized and integrated training program is required to operate efficiently.

The training programs must include operating in complex environments where mission command can be maximized. The OE will overflow the commander with information, rendering AI crucial to maintain a fast-paced tempo. Commanding and fighting alongside AI needs extensive training to understand not only the human variations in culture, but also the AI's. Additionally, the training must teach the commander to think across the domains to identify and exploit opportunities, and most essentially, to rethink the whole battlespace itself with innumerable new maneuver options.[29]

Regardless of the proficiency and efficiency in the fight, the US and its democratic allies will always have a disadvantage in information operations. Consequently, the US focus must be to fortify itself and its allies against disinformation without undermining western values and subverting its own population.[30] The openness and the high degree of interconnectedness citizens enjoy makes the population simultaneously fragile and tangible, but also informed and critical. The openness is obviously a security risk which all societies have different strategies to mitigate. Today, western offensive cyber operations on adversarial populations are less effective due to e.g. quantitatively few globally connected citizens, or citizens protected behind government firewalls. Instead, focus must be on infrastructural or other governmental targets.

The main purpose with the NGW information operations is to shape and affect the receiving party in a predetermined matter. To achieve this, reflexive control can be used. Reflexive control is when an object is manipulated to think and act in a way that the opponent intends to indirectly force the adversary to make a desirable decision.[31] Methods such as strategic deception, diplomatic pressure, rumor, false narratives, and possible harassment, all aim to deplete the willingness of an adversarial population to fight,[32] and are ways to achieve reflexive control.

Another military theorist that centralized the will of the people was Douhet. His methods for achieving total submission of a population are not applicable in the 21th century information warfare. Nevertheless, central to his argument is to influence and impact the population in such a manner that there will be a decisive end, preferably before the war even started. The decisive point was to make the people suffer, and consequently the population, due to self-preservation would demand surrender from their government.[33] To summarize the non-military measures, ideas from Isserson and Douhet seem greatly applicable in contemporary and future warfare, in targeting adversarial populations and their will to fight.

Analysis of future approaches

Using DOTMLPF-I,[34] focusing on doctrine, leadership, and interoperability, three areas from the analysis will be summarized for future operations.

Defensive Cyber Operations (DCO): The willingness of the people to defend themselves is crucial to preserve an independent sovereign state. Therefore, as a population is considered key terrain or a strategic backbone, the population needs to be actively involved as a defense mechanism, consequently raising the threshold for actions under armed conflict. Additionally, the population must learn the adversary's view of war, and their strategic and tactical behavior regarding informational warfare. Furthermore, to protect the will of the people, DCO must include protecting important infrastructure and industry like power plants, fresh water wells, and an increasingly connected farming in-

dustry including manufacturing and transportation of food from producer to retailer. Interruption, disruption, or destruction must be prevented and protected.

Future leadership must be highly proficient in commanding with enormous amounts of information. Yesterday's fog of war meant little to no information. Tomorrow's fog of war entails abundant amounts of information, where it takes a certain skill to sort and find accurate and qualitative information. Simultaneously, although AI can assist in this endeavor, mankind needs to build up trust in machines/software to the level where high-risk decisions concerning lives can be delegated. Additionally, future commanders need to have a better strategic overarching mindset and good understanding of international relations; hence the actions executed by the junior officer in the cyber domain, will have far greater consequences than for the old famous strategic corporal.

Cultural understanding is key in the process of interoperability in this aspect of integrating multilateral capabilities and executing operations together, across domains quickly. To preserve freedom of action and maneuverability, the same operational language must be spoken, and the understanding of values, strengths and weaknesses must be vital. By accepting and understanding mutual differences, an amplified and complex threat is projected to the adversary. Together we are strong, and possess the capability to meet and de-escalate any adversary, and if necessary, destroy them. From a small state perspective, operations center around DCO, offensive cyber operations (OCO), and technological innovation e.g. quantum computers or efficient transport systems of space domain infrastructure and/or information.

Conclusions

Presently and for the foreseeable future, nations face perhaps radical changes which will demand a new level of thinking and executing and require working simultaneously across domains at high speeds. Consequently, this calls for decentralized command structures and clear understandings of mandate and a commander's intent.

This article shows that the role of, and the influence on, a population is crucial in a future conflict. If societies are not aware of the level of adversarial influence on them, the population within that society may in the worst case call for an end to the war before it even begins, as Douhet sought.

To combat the enemy in 2035, a primary focus should be to hide and/or protect one's weaknesses by displaying a complex and non-linear cyber domain. Simultaneously, a boundless human network of cognitive integration is required to fight seamlessly, cooperatively, and with contemporary technology, to find and destroy any adversarial attempt to disrupt allied alliances or destroy allied sovereign states.

The author is major, serving at the Swedish army staff.

Notes

1. Luttwak, Edward N.: *Strategy: The Logic of War and Peace*, 2nd edition, Belknap Press, an Imprint of Harvard University Press, Cambridge, MA 2002, p. 1.
2. Perkins, David G.: "Multi-Domain Battle The Advent of Twenty-First Century War", *Military Review,* November-December 2017, p. 11, *https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/Multi-Domain-Battle-The-Advent-of-Twenty-First-Century-War/*, (2020-05-08).
3. Gerasimov, Valery: "The Value of Science Is in the Foresight", *Military Review*, January-February 2016, p. 29, *https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf*, (2020-05-08).
4. Perkins, David G.: "Multi-Domain Battle Driving Change to Win in the Future", *Military Review,* July-August 2017, p. 9, *https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2017/Perkins-Multi-Domain-Battle/,* (2020-05-08); McFate, Sean: *The New Rules of War: Victory in the Age of Durable Disorder,* First edition, William Morrow, an Imprint of HarperCollins Publishers, New York, NY 2019, pp. 64-66.
5. Waitling, Jack and Roper, Daniel: "European Allies in US Multi-Domain Operations", *RUSI Occasional Paper,* October 2019, p. 24, *https://rusi.org/sites/default/files/20190923_european_allies_in_us_multi-domain_operations_web.pdf,* (2020-05-08).
6. "Challenges to security in space", *Defense Intelligence Agency*, January 2019, p. 33, *https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf,* (2020-05-08).
7. Kemp, Herbert C.: "Rethinking the information Paradigm: The future of intelligence, Surveillance, and Reconnaissance in Contested Environments", *The Mitchell Forum,* no. 18, February 2018, p. 6, *https://defense.info/partners-corner/2018/04/rethinking-the-information-paradigm/,* (2020-05-08).
8. Ibid., p. 5.
9. Op cit., Perkins, David G., see note 2, p. 13; Atkins, Sean A.: "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace", *Air and Space Power Journal*, Fall 2018, p. 29, *https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-3/F-Atkins.pdf,* (2020-05-08).
10. Lind, William S.: *Handbok i manöverkrigföring*, Förkortad och kommenterad upplaga, Försvarshögskolan, Stockholm 2006, pp. 17-18.
11. Op. cit., Perkins, David G., see note 2, p. 11; Kukkola, Juha; Nikkarila, Juha-Pekka and Ristolainen, Mari: "Asymmetric frontlines of cyber battlefields", *MILCOM 2017 IEEE*, 2017, p. 21.
12. Alberts, Davis S.: "Multi-Domain Operations: What's New, Whats's Not, and the Implications for Command and Control", *Institute for Defense Analysis*, 26 March 2018, p. 6, *https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/5bf59e15f950b77783c11f4e/1542823446013/23rd_ICCRTS_paper_51.pdf,* (2020-05-08).
13. Jonsson, Oscar: *The Russian Understanding of War: Blurring the Lines between War and Peace,* Georgetown University Press, Washington 2019, pp. 12-14.
14. Connor, Sidney A.: "Military operations in the information age: putting the cognitive domain on top", *U.S Air War College*, Air University [Research report], 2017, *https://apps.dtic.mil/dtic/tr/fulltext/u2/1038189.pdf*, (2020-05-08).
15. Op. cit., Gerasimov, Valery, see note 3, p. 28, p. 34; Zi, Sun: *Sun Zis krigskonst*, Santérus, Stockholm 2015, pp. 39-40.
16. Allen, T.S and Moore A. J.: "Victory without Casualities – Russias Information Operations", *Parameters*, vol. 48, nr. 1, Spring 2018, p. 70, *https://publications.armywarcollege.edu/pubs/3544.pdf,* (2020-05-08).
17. Harrison, Richard W.: *Architect of Soviet victory in World War II: the life and theories of G.S. Isserson,* McFarland & Co., Jefferson, NC 2010, p. 86.
18. Ibid., p. 86.
19. Friis, Karsten and Garberg Bredesen, Maren: "Strike first and strike hard?: Russian military modernization and strategy of active defence", Frivärld, 2 december 2019, *https://frivarld.se/rapporter/strike-first-and-strike-hard-russian-*

military-modernization-and-strategy-of-active-defence/, (2020-05-08).
20. Bartles, Charles K.: "Getting Gerasimov Right", *Military Review*, January-February 2016, p. 34, *https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Military Review_20160228_art009.pdf,* (2020-05-08).
21. Op. cit., Waitling, Jack and Roper, Daniel, see note 5, p. 23, p. 30.
22. Joint Intelligence Surveillance and Reconnaissance, Joint Targeting, Joint Fire Support, Joint Situation Awareness.
23. Op. cit., Gerasimov, Valery, see note 3, p. 28; Op. cit., Perkins, David G., see note 4, p. 10.
24. Op. cit., McFate, Sean, see note 4, pp. 28-30.
25. Op. cit., Bartles, Charles K., see note 20, p. 34, p. 36.
26. Kofman, Michael: "Russian A2/AD: It is not overrated, just poorly understood", *Russia Military Analysis: A blog on the Russian military*, January 25 2020, *https://russianmilitaryanalysis.wordpress.com/2020/01/25/russian-a2-ad-it-is-not-overrated-just-poorly-understood/*, (2020-05-08).
27. Paget, Steven: "Interoperability of the mind", *The RUSI Journal,* September 29 2016, p. 48, *https://rusi.org/publication/rusi-journal/%E2%80%98interoperability-mind%E2%80%99-professional-military-education-and-development?qt-related=1&page=114*, (2020-05-08).
28. Op. cit., Waitling, Jack and Roper, Daniel, see note 5, p. VI.
29. Op. cit., Atkins, Sean A., see note 9, pp. 30-33.
30. Op. cit., Allen, T.S and Moore A. J., see note 16, p. 70.
31. Ibid., p. 61.
32. Op. cit., McFate, Sean, see note 4, p. 66.
33. Douhet, Giulio: *The Command of the Air,* The University of Alabama, Tuscaloosa, AL 2009, p. 20, p. 51 and p. 58.
34. Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability.