Journal of Strategic Security

Volume 15 | Number 4 Article 9

Technology, Data, & The Future of Warfare: A Review Essay by James Torrence

James Torrence, DSS
U.S. Army, HQDA Data Operations Division

pp. 133-141

Recommended Citation
Torrence,, James DSS. "Technology, Data, & The Future of Warfare: A Review Essay by James Torrence." *Journal of Strategic Security* 15, no. 4 (2022) : 133-141.
DOI: https://doi.org/10.5038/1944-0472.15.4.2087
Available at: https://digitalcommons.usf.edu/jss/vol15/iss4/9

Technology, Data, & The Future of Warfare: A Review Essay by James Torrence

***Future War and the Defence of Europe*. By John R. Allen, Frederick Ben Hodges, & Julian Lindley-French. Oxford, United Kingdom: Oxford University Press, 2021. ISBN: 9780198855835. Bibliography. Index. Pp. 30, 217, 219, 267. $34.64**

***Radical War: Data, Attention and Control in the 21st Century*. By Matthew Ford & Andrew Hoskins. Oxford, United Kingdom: Oxford University Press, 2022. ISBN: 9780197656549. Diagrams. Appendices. Notes. Bibliography. Index. Pp. 5, 11, 58, 60, 85, 111, 113, 149. $27.95.**

***The New Art of War: The Origins, Theory, and Future of Conflict*. By Geoffrey F. Weiss. Cambridge, United Kingdom: Cambridge University Press. ISBN:9781108837644. Figures. Appendix. Notes. Bibliography. Index. Pp. 324. $34.99**

***War Transformed: The Future of Twenty-First-Century Great Power Competition and Conflict*. By Mick Ryan. Annapolis, MD: Naval Institute Press. ISBN:97882477427. Tables. Notes. Bibliography. Index. Pp. 42, 82, 104, 324. $39.95**

James Torrence, Doctor of Strategic Security
U.S. Army, HQDA Data Operations Division

Future War, *Radical War, The New Art of War,* and *War Transformed,* are all recent books in which the authors look at the future of warfare and account for emerging technologies. All four of these books are must-reads for leaders interested in understanding how emerging technology will impact both the theory of warfare and the future of warfare. The boldest, and most informative of these four books is *Radical War*. Ford and Hoskins write the rare book that takes big chances, introduces new concepts (i.e., considering the conversion rate of actions at the operational level of war and the need to move faster than the speed of narrative), and goes beyond generic descriptions of what data and tech-centric warfare may look like.

Though these books discussed how future technology will influence the battlefield, there was a clear lack of discussion on the risks associated with

the transition to a data-centric decision model where humans are replaced by machines.[1] The lack of risk discussion leaves the reader with the impression that the authors did not want to wade into the challenges of discussing risk in a complex, tech-saturated environment that is still evolving. The two important themes that emerged after reading these four books are the importance of understanding emerging technology and its impact on the future battlefield, and the challenges of knowledge management and information archiving.

Emerging Technology

Though each book takes a different approach to the analysis on how technology shapes the future of warfare, a consensus emerged on the types of technology about which leaders must learn. Weiss asserts that "AI [Artificial Intelligence], autonomous, and semi-autonomous weapons (e.g., "robots" or "drones") will undoubtedly influence future war." [2] Ryan expands on the technologies listed by Weiss and claims that "eight specific technologies – artificial intelligence, robotics, quantum technology, biotechnology, energy weapons, hypersonics, space technology, and additive manufacturing – are likely to have the greatest impact on twenty-first century military affairs."[3] Hodges, Allen, and Lindley-French further expand the impact of AI and argue that

> AI would not be a stand-alone technology, but act in concert with machine-learning [ML], human enhancement, genetic manipulation, data analytics, simulation, behavioural science, drone technologies, quantum-based sensors that can reveal the ocean depths and whatever is sailing within it, cyber warfare, synthetic technologies and nano-technologies linked to 3D printing, hypersonic weapons, smart weapons, unmanned combat aerial vehicles that form part of attack swarms, and the use of big data to create synthetic reality to better inform often-automated decision making.[4]

The authors capture the important technologies that are making or on the verge of making significant impacts on the battlefield. The only aspect of emerging technology that Weiss, Ryan, Hodges, Allen, and Lindley-French failed to mention was the continued increase of mobile, connected devices on the battlefield. Though mobile devices are not new, the ubiquity and

https://digitalcommons.usf.edu/jss/vol15/iss4/9
DOI: https://doi.org/10.5038/1944-0472.15.4.2087

continued advances in processing power of connected systems on the battlefield increases the number of people who participate in and influence conflict. Ford and Hoskins recognize that smart devices "remove the bystander from war" which makes the "distinctions between audience and actor, soldier and civilian, media and weapon become meaningless."[5] In addition to removing the bystander from war, smart devices also influence the way in which military forces prepare for operations.

Ford and Hoskins argue that "mobile connected devices are revolutionising how armed forces organise for warfighting."[6] Additionally, Ford and Hoskins assert that "cloud-enabled, networked and handheld digital systems" change the way military "forces think through the necessary steps needed to go from collecting targeting information to taking a decision and dropping a bomb."[7] It is important to include mobile devices as part of emerging technology because of how they impact participation and planning in war. The continued augmentation of human thought with technology coupled with the amount of data consumed and produced from individuals, corporations, NGOs, and governments, creates an unprecedented environment in which war moves at a relentless pace.

Technology & The Speed of War

There is consensus amongst all the authors that the speed of war will increase exponentially as emerging technology becomes part of the military decision-making cycle. Hodges, Allen, and Lindley-French claim that "another major war in Europe would be hyperwar" which is "ultra-fast warfare that combines a myriad of systems to wreak havoc in an instant."[8] They think that "hyperwar will exponentially accelerate the speed of war across multi-domain warfare conducted via air, at sea, on land, in space, in cyber space, and increasingly via information and deep, destructive human and machine generated 'knowledge.'"[9] Ford and Hoskins propose their own definition: radical warfare. They argue that "radical war is the immediate and ongoing interaction between connected technologies, human participants, and the politics of violence."[10] Hyperwar and radical warfare both focus on the combination of the speed of warfare, technology (including machines), and people. However, the future of warfare is defined (the term warfare can also suffice without always trying to make a new definition), leaders must be prepared for a speed of violence, information, and decision-cycles never-before-seen.

Ryan acknowledges that "the speed of planning, decision-making, and action is increasing due to hypersonic weapons, faster media cycles impacting political decisions, and the potential for AI to speed up decision-making at many levels."[11] Ford and Hoskins assert that "armed forces must have the capacity to fight at the speed of data transfer" which "allow[s] them to be ahead of the media narrative, shaping stories even before journalists have had chance to broadcast."[12] Ford and Hoskins expand on the idea of fighting at the speed of data transfer and ask the question: "if military operations have to keep up with the speed of information as it is spread across civilian information data networks, then when does war stop?"[13] The future speed of warfare, information, and decision-cycles will result in a complex ecosystem of inputs and outputs in which militaries must make operational decisions not only to defeat the enemy, but also to create rather than be a victim of a narrative. The speed of warfare also necessitates a change to a top-down decision-cycle which means decisions must be further delegated to subordinate chains of command or to machines.

Ryan says that the "the application of AI and its accelerating influence in war means that there must be wholesale reexamination of current chain of command approaches and of the degree of delegation provided to subordinate commanders"[14] Allen, Hodges, and Lindley-French argue that "given the speed of future war, demonstrable speed of command will be central to both credible deterrence and warfighting."[15] Weiss also recognizes that "improvements in AI algorithms and machine learning will enable some weapons (including cyber weapons) to complete more complex missions and perhaps even surpass human decision-making abilities for select purposes."[16] Additionally, Ryan argues that "computer-based decisions are unlikely to have the requisite flexibility or discretion to make humans irrelevant, particularly for real-time circumstances."[17]

The furthest any of the books goes in discussing the delegation of decision-making is *Future War and the Defence of Europe* (the authors argue that the Supreme Allied Commander Europe (SACEUR) should have more delegated authority and that the NATO command structure is insufficient to deal with the rapid changes in warfare).[18] The other books discuss the importance of delegating decisions to people and/or machines, but never provide an example or model for what that looks like in practice.

https://digitalcommons.usf.edu/jss/vol15/iss4/9
DOI: https://doi.org/10.5038/1944-0472.15.4.2087

It was disappointing that none of the four books laid out a model or framework for what the delegation of decisions looks like (machine-only loop, human-machine loop, human-only loop) in a future warfare environment comprised of various technologies and the need to account for and outpace adversary decision cycles. A framework focused on decision delegation would quickly result in a requirement to develop risk acceptance criteria for the delegation of decisions (another topic not discussed in any of these books). It is easy to talk about how AI, ML, and future technology will hypothetically speed up decision-cycles, but much more challenging to talk about how risk is assessed and accepted prior to new decision models being implemented. Any future decision-model will depend on data access and data analysis. Ford and Hoskins discuss the challenges associated with knowledge management (including data sources and data governance) in *Radical War*.

Knowledge Management and Information Archiving

The most important topic discussed across all four books is that of knowledge management. Ford and Hoskins argue that "identifying military weaknesses and optimising performance through engagement in history depends on information management and record-keeping."[19] Furthermore, the combination of an increase of information (and disinformation) mixed with a push to digitize records leaves militaries "reliant on the production of partial histories based on selected readings of the public record combined with interviews of officers who understand that these exercises have both career advancing and limiting effects."[20] The effect of an inability to maintain a factual archive can "delegitimize official histories of war" and limit a military's future effectiveness if it cannot learn from its last engagement.[21]

Ford and Hoskins argue that "audiences today are more like nodes in a network, part of a hyperconnected ecology of war, that constantly create and consume media but are not reliant on traditional broadcasters" which leads to "relentless churning of different opinions and images of war, such that consensus about what war is becomes much harder to construct and maintain."[22] Additionally, they contend that "data decays, files get deleted, hyperlinks break, cyberattacks corrupt code, [and] criminals use ransomware to prevent access to material" which "adds to the sense of

doubt that comes from working in a new war ecology where false information spreads more quickly than truthful content."[23]

Ford and Hoskins were the only authors to discuss the challenges of maintaining an official record in an environment with misinformation, restriction to data sources, echo chambers, and competing narratives. Militaries depend upon official records from which to learn and drive future changes to avoid becoming obsolete. Ford and Hoskins summed up the fundamental challenge of technology and record-keeping as follows: "technology consequently facilitates and constrains the digital individual as they find ways to contribute towards and break the mainstream consensus over what constitutes knowledge and what ought to form part of the received historical record."[24]

Technology will continue to increase the speed of both decision-cycles and warfare on the future battlefield. Leaders cannot forget the importance of record-keeping (including the source and access to data that informs records) as they are bombarded with more and more information that makes it challenging to decipher what really happened. All four books covered the emergence of future technology, but none of them contained a discussion of the risks associated with moving towards a data-centric decision-model with machines in the loop.

The Risks Associated with Data & Tech-Centric Warfare

Military leaders must have a process to identify and accept risk during both training and conflict. None of the four books put forth a framework to discuss the risks associated with adding a machine into the decision cycle during military operations. As the authors of each of the four books discussed machines being part of the decision cycle, they skipped over discussion about how military leaders should approach the risk associated with this data-centric approach to warfare. A basic framework centered on decision integrity should include the following categories: internal data, external data, algorithmic, position, navigation, and timing (PNT), and transport.[25]

Internal data is the data produced, governed, stored, and distributed within an organization (in the case of the future of warfare, the military or government). Leaders must understand if they have the right data

https://digitalcommons.usf.edu/jss/vol15/iss4/9
DOI: https://doi.org/10.5038/1944-0472.15.4.2087

required to feed their AI and ML models and if that data is secure. The first question for any military or organization looking to become data-centric is whether the organization has the right data. The best data governance and data products in the world are irrelevant if they don't use the right data inputs. Concurrent with the need to ensure an organization captures the right data is the need to validate that its internal data is secure. It is unlikely that any organization will ever have complete internal data or data that is completely secure which necessitates understanding the risk associated with decision outputs derived from internal data.

AI and ML models will also ingest external data as part of algorithms designed to enhance decision-making. External data is any data that is produced outside of the organization. External models (whether from open-source or data shared from industry or military partners) must also have a percentage of confidence related to data integrity measured against the data production, data governance model, and data security from the data source.

AI and ML models will have a variety of algorithms used to ingest and analyze internal and external data. Organizations will put a heavy emphasis on algorithmic security to ensure that a threat actor does not try and manipulate the algorithms or the data that feeds the algorithms to influence decision-outputs. Threat actors will also employ their own AI and ML models to analyze outputs of a military or national data-centric decision model to try and approximate the factors that influence an algorithm. Algorithmic integrity must be captured during ongoing risk identification.

PNT can fit in either internal or external data (depending on the source), but it is worth mentioning as its own because of its importance. In a large-scale conflict, military personnel from multiple armies will be scattered across the air, land, sea domains conducting operations. The integrity of PNT inputs is critical to any decision-model. If PNT is not correct (or if there is an unacceptable level of risk associated with the integrity of ingested PNT data), then the output of the model will lead to decisions based on the wrong data. Decisions based on the wrong data will lead to disastrous consequences in a conflict.

Transport is the medium through which data is accessed by the AI and ML models. If transport is disrupted, degraded, or denied, then the data feeding the AI and ML algorithms will be incomplete. In a near-peer conflict, it is inevitable that there will be long periods during which data from multiple sources will be inaccessible. The amount of data received in a decision-model compared to the amount of data the model identifies as being accessible must be analyzed to identify the level of risk from a recommended decision based on incomplete data.

The integrity of a data-centric decision model with a machine in the loop is important for identifying the risk (at any given time) associated with outputs from the model. A data-centric decision model with a machine in the loop must assess the integrity of internal data, external data, algorithmic, PNT, and transport to understand how much risk is associated with each decision output.

Conclusion

Future War, *Radical War, The New Art of War,* and *War Transformed,* show that authors from multiple countries with varying levels of military and strategic experience agree that warfare will be fast, integrate myriad new technologies, and will have machines as part of the decision cycle. *Radical War* adds to the discussion by including the importance of knowledge management to enable militaries to learn from the past to shape the future. Each of the books discussed contain lessons from which readers must learn when thinking about warfare in the future. *Radical War* stands out amongst these four books for pushing the boundaries of the existing literature and proposing new models, frameworks, and theories of warfare to account for emerging technology.

As authors continue to address technology and the future of warfare, they must discuss the risk management associated with adopting new technologies, adding machines into the decision-cycle, and militaries moving faster to try and create rather than be a part of someone else's narrative. Any discussion of risk should include the integrity related to data inputs and the algorithms that use and analyze those inputs to produce decision outputs.

https://digitalcommons.usf.edu/jss/vol15/iss4/9
DOI: https://doi.org/10.5038/1944-0472.15.4.2087

Endnotes

[1] *Radical War* talks about risk specific to information management and accessibility, but not in a broader model.
[2] Weiss, *The New Art of War*, 324.
[3] Ryan, *War Transformed*, 42.
[4] Allen et. al, *Future War*, 217.
[5] Ford & Hoskins, *Radical War,* 11.
[6] Ibid., 5.
[7] Ibid.
[8] Allen et. al, *Future War*, 217.
[9] Ibid., 219.
[10] Ford & Hoskins, *Radical War,* 11.
[11] Ryan, *War Transformed*, 82.
[12] Ford & Hoskins, *Radical War,* 85.
[13] Ibid., 85.
[14] Ryan, *War Transformed*, 104.
[15] Allen et. al, *Future War*, 30.
[16] Weiss, *New Art of War*, 324
[17] Ryan, *War Transformed*, 324.
[18] Allen et. al, *Future War*, 267.
[19] Ford & Hoskins, *Radical War,* 111.
[20] Ibid., 111.
[21] Ibid., 113.
[22] Ibid., 60.
[23] Ibid., 149.
[24] Ibid., 58.
[25] A longer paper showing how this model fits with the 7-layer OSI model would be beneficial.