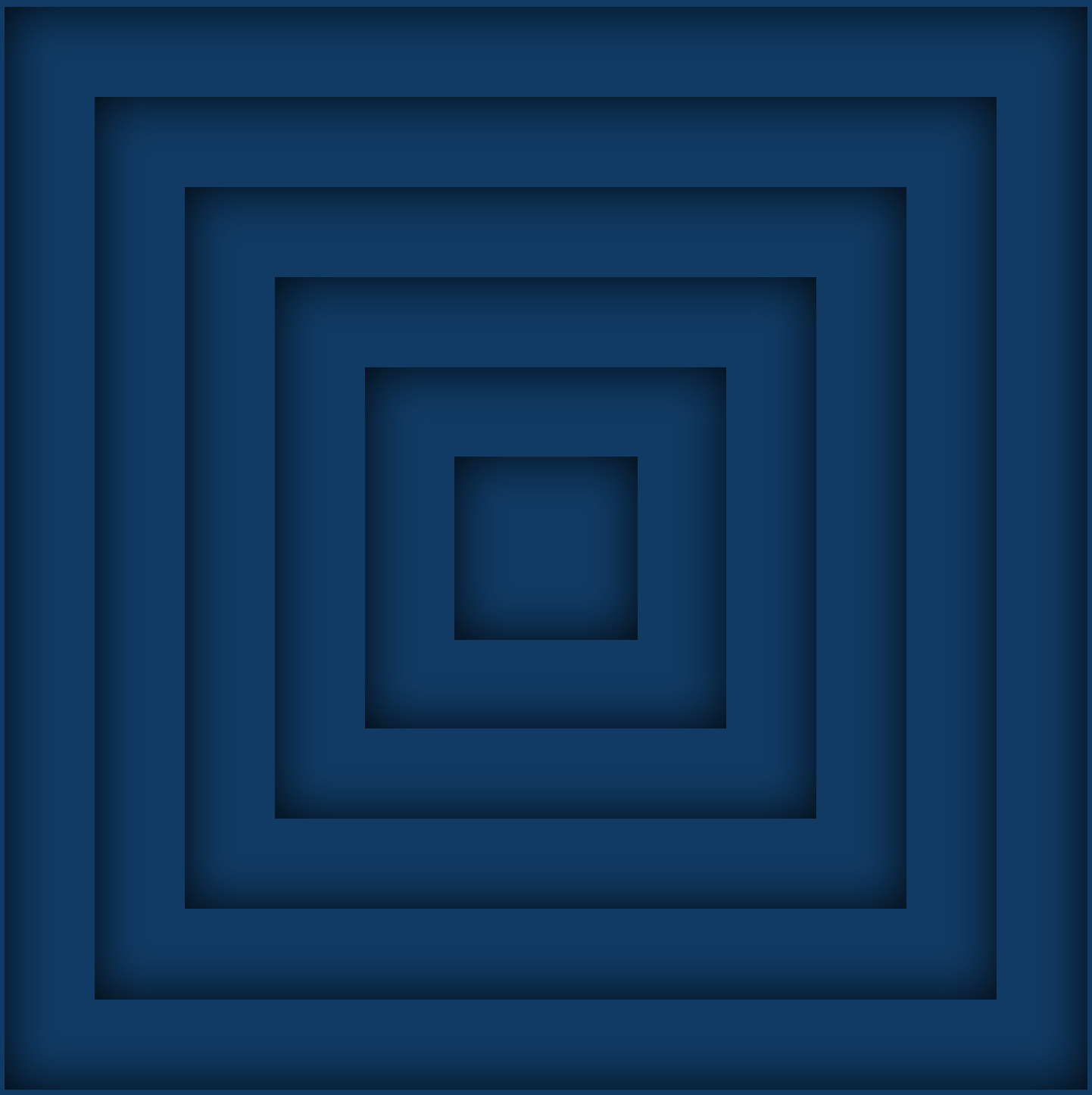
The Hague Centre
for Strategic Studies

Guest Contribution

The Promise and Peril of Emerging Disruptive Technologies for Joint and Combined Multi-Domain Operations

Nina Kollars, United States Naval War College

November 2023



The Hague Centre
for Strategic Studies

The Promise and Peril of Emerging Disruptive Technologies for Joint and Combined Multi-Domain Operations

Author:
Nina Kollars, United States Naval War College

November 2023

This paper has been developed within the context of the "HCSS-NATO HQ SACT Symposium on Rethinking Fire and Manoeuvre across physical and non-physical aspects of domains". The views are those of the author and do not represent those of HQ SACT, NATO, the US government, the Naval War College or of HCSS as an institution.

There is promise and peril in adopting emerging disruptive technologies (EDTs) as the centerpiece of how modern militaries intend to conduct multi-domain operations (MDO). As a cyber and innovation scholar I hope what I have to say is distinct from my practitioner brothers and sisters. There is so much that they have in their wheelhouses as we attempt to pierce the veil of the future. Mine will not be an entirely happy story. Because the object of our inquiry is how we *want* to fight rather than how we *already* fight, we have an obligation to be critical and highly skeptical. My concern is compounded further anytime one marries together two heavily jargonized and bloated terms such as EDT and MDO. At a minimum, we should all take pause, and question our sense of integrity.

Between Two Acronyms

Military forces face a number of hurdles that are timeless and nearly universal across all attempts at technological change. Whether the question is acquisitions at an industrial scale, or the next iteration of a ship, the challenge of technological change is a longstanding puzzle for militaries. In a joint and combined environment, the complexity only increases. Whether it is planning, acquisition, or interoperability with our allies, there are ongoing challenges to technological change.[1] But what is unique, specifically to MDO and EDT?

From my view, the problem unique to EDT and MDO is one of who are the majority developers of the technology, the owners of the infrastructure and the majority users of the system. This is to say that development is nearly entirely the private sector; ownership is largely held by global firms; and users are largely not military users.

Insofar as this is the case, the primary factors shaping the successful integration of EDTs into military operations are as follows:

First, EDTs (as currently produced) are developed in a marketplace where government money, even those as large as US military dollars, are still the marginal investment. Militaries cannot and never will have the monopoly on them, and therefore will not be able to shape them to their preferences. All that is left is partnerships, and that is hard. More complex still, the systems upon which these EDTs will be leveraged will be through existing public/private infrastructure that is already fully leveraged for its own peacetime purposes.

Second, EDTs leveraged in the context of warfighting will not occur in a vacuum. Instead, they will occur in an already congested corporate and human context that is already using EDTs for their own purposes.

And third, EDT changes very quickly. As an effect of the first and second factors EDTs tend to be designed for the market and public's pace for change, not at the pace of military technological change.

Given these factors, I anticipate that the successful incorporation or failure of EDTs in MDO is seated firmly outside the control of militaries...even powerful ones. But this is not reason for despair. Instead, I'm here to talk about managing our expectations, and seizing opportunities where they will yield the most military utility, particularly in a joint and combined environment.

But first, as academics do, definitions and scoping.

1 See for instance the literature on military technological innovation: Grissom, Adam. "The future of military innovation studies." *Journal of strategic studies* 29, no. 5 (2006): 905-934. Horowitz, Michael C., and Shira Pindyck. «What is a military innovation and why it matters.» *Journal of Strategic Studies* 46, no. 1 (2023): 85-114.

Which EDTs?

What is an EDT? By emerging, we are referring to that which is becoming apparent but is not quite fully realized. It is in the early stages of development and adoption. We have some guesses of what the utility is, but we don't know for certain all of the uses. And quite often, our guesses are wrong. By disruptive, we tend to mean something that has the potential to re-order or fundamentally shift how things are done. The internet is a tremendous example of a disruptive technology. Not only did it displace most paper letter writing, but when combined with social media platforms, the internet upended most facets of human social life for those who operate on it. From dating, to writing and sending pictures to our families, to making phone calls, the internet generated a paradigm shift in how humans behave.

There are all kinds of EDTs from quantum computing to CRISPR genome manipulation, but for our purposes, I am scoping this manuscript specifically to the realm of changes in data/information production and processing.[2] I am doing so largely because the majority of things we tend to refer to as EDTS for military applications are, with very few exceptions, adjustments in the production of data and the processing of information.[3] The time we are living in given these emerging data production and processing change is a very volatile one.[4] The development has taken decades of work, but we are reaping the effects of centuries of engineering and science right now.

Within this digital data and processing scope I am referring to the full landscape of inputs to computer processing systems. Those inputs can be imagery, audio, conventional messaging, or sensors (be they motion, pressure, proximity, or photoelectric) that are fed into processors be it wired or wireless. No matter the signal, it is data. And data is ripe for mining. On the other end is the processing of the data, be that the human brain, a cellular telephone, Amazon's cloud, or Open AI's ChatGPT systems. When mixed, this complex component-filled stew is how I think of EDTs—they are the systemic output of the organic and synthetic organism the world has created.[5] We are yet in the first quarter of this century, but already it is clear that this century will be marked by the maturation of a revolution in data—how it is produced and who or what consumes it—enabled to choose and act. We can see more, discover more, do more through our data systems than ever before.

As it turns out, a fundamental and curious feature of being human appears to be the continued creation of data production machines, data conversion machines, and data ingestion machines that enable and enhance the scope of human understanding and human action.[6] Whether we are talking about the printing press, the microscope, or computers, data is at its core. Data is, to quote James Gleick in his book "The Information"...the blood and the fuel, the vital principle" of the world.[7]

2 Zhu, Haocheng, Chao Li, and Caixia Gao. «Applications of CRISPR–Cas in agriculture and plant biotechnology.» Nature Reviews Molecular Cell Biology 21, no. 11 (2020): 661-677.

3 See for instance the Nato website: Emerging and Disruptive Technologies, June 22, 2023 https://www.nato.int/cps/en/natohq/topics_184303.htm

4 My scoping doesn't narrow the playing field too aggressively since even by NATO's STO report, only two of the categories are left out, biotechnology and advanced materials. See: "Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains NATO Science & Technology Organization." https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

5 Note here that I am borrowing heavily from social construction of technology thinkers such as Bruno Latour, Langdon Winner, Weibe Bieker and so many others who drawing no strong distinction between humans and the machines they use. See: Bruno Latour, *Reassembling the Social: Actor Network Theory* (Oxford: Clarendon, 2005); Langdon Winner, *Autonomous Technology : Technics-out-of-Control as a Theme in Political Thought* (Cambridge, Mass.: MIT Press, 1977); Wiebe E. Bijker, *Of Bicycles, Bakelites, and Bulbs : Toward a Theory of Sociotechnical Change* (Cambridge, Mass.: MIT Press, 1995).

6 Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. Computer: A history of the information machine. Taylor & Francis, 2023.

7 Gleick, James. The information: A history, a theory, a flood. Vintage, 2011.

What is MDO?

As for what is meant by, or what I think we mean by MDO, we have a little bit of an endogeneity problem in drawing a distinction between it and EDTs. By this I mean that MDO appears to have been generated with an eye toward the capabilities that data-centric EDTs would generate. MDO implies EDTs that can expand awareness, coordination across forces, and anticipation of adversary moves. As a matter of advocacy—which new concepts like this invariably need—MDO is often described in all too rosy terms, promising to create real-time omniscience and control...As if, somehow, everything, everywhere, could be understood and actioned at the blink of an automated eye.

As an innovation scholar and a technology skeptic I want to reassure the reader of two things. First, in spite of the labyrinthine processes of the Department of Defense, and the painful jargonized processes we must undergo to change, multi domain operations are very real.[8] Underspecified perhaps, and only slowly being operationalized in the modern context, certainly, but the concept that sea, ground, and air assets would be leveraged collaboratively through enhanced data capabilities...has existed for over a century. What is new is the sheer amount of data production, the digital infrastructures to carry it, and the massive amount of computing power that generates action and new insights.

Since the early conversations by Army General David Perkins of MDB—multidomain battle—evolved steadily into MDO. At that time, the keenest interest was how to incorporate cyberspace and information warfare capabilities to enhance the employment of military assets in conflict.[9] Over time, additional data production and processing capabilities have come to the foreground, namely machine learning, big data processing, and autonomous capabilities.[10] It is the promise and peril of these amplified new methods of data production and data processing bring to combined arms conflict that we must wrap our heads around.

Together MDO and EDT sees the promise of leveraging these systems, this global systemic shift to data and data processing that have rendered real-time persistent surveillance a reality not just as an exercise in intelligence, but as a global reality for the maritime cargo shipping industry, emergency response organizations, and even families. From this view, great power militaries can ride the wave of innovation as the marketplace bursts with cheap new methods of sensing, collecting, and processing data. For example, the fact that refrigerators can assess nutrition levels, then program, and ultimately purchase foods for a family is interesting.[11] That a military could do so also is intriguing but much harder to do from a sustainment and logistics perspective. How can it scale? What data systems must be replaced? Can we simply bolt this solution onto existing systems? Thus, while there is promise, there is massive complexity and uncertainty as well.

8 Townsend, Stephen J. "Accelerating Multi-Domain Operations." *Military Review* (2018): 4-7.

9 Perkins, Gen David G. "Multi-Domain Battle." *Military Review* (2017).

10 Watling, Jack, and Daniel Roper. *European Allies in US Multi-Domain Operations*. Royal United Services Institute for Defence and Security Studies, 2019. Pg 8-10

11 A. -D. Floarea and V. Sgârciu, «Smart refrigerator: A next generation refrigerator connected to the IoT,» 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Ploiesti, Romania, 2016, pp. 1-6, doi: 10.1109/ECAI.2016.7861170.

Peril 1: Relying on Private Sector Infrastructure

One of the standing jokes about the virulently powerful development of AI chatbots like ChatGPT is that success breeds even greater success. The more we feed the algorithm, the more interested people become in it, the more we feed it. There can be no substitute for the sheer hoard rush of public behavior that helps these systems get smarter, and faster. The more the tendency to use these data systems occurs in everyday life and in the corporate world, the stronger the infrastructure that feeds these systems becomes. This massive global data generating and gulping system is built to churn out new products and ideas daily. The same is also sadly true for our reliance upon computing power. Corporations like Microsoft and Amazon Web Services own much of the computing power that enables all the data processing these hungry algorithms need.

For a great power military to leverage the power of these systems as we see them in the private sector, militaries must tap in. But tapping in isn't as easy as it might seem. There are easily four decades now of academic literature on "public private partnerships," in which well-meaning scholars offer that there are opportunities for government and defense to latch onto private sector innovation, and to "fast-follow" the development and acquisition of data technologies.[12] The reality is that while companies are interested in making money from governments, they are much less interested in being controlled by them, particularly during a conflict.

In peacetime, the upside of cutting deals with Google, Amazon Web Services or Starlink, is militaries can lean into all the most exquisite real-time data that the open-source world can offer. During conflict, this is another question entirely. As the Elon Musk case continues to evolve wherein Starlink's data appears to have been throttled over Ukraine, the reliability of globally footprinted companies and their willingness to cooperate during war is one that deserves serious consideration.[13] When it isn't your infrastructure, you aren't guaranteed access.

We can see some of these attempts to leverage deterrence by detection by the Biden administration's use of intelligence to announce Russian and North Korean intent. For these instances, the private sector is more than happy to have their infrastructure and resources featured as part of the show. What hasn't been addressed well in any of the extant research is the degree to which firms that provide access to data lakes and data processing are interested in cutting deals to Allied militaries in a time of war. If this is to be considered as a serious element of a future warfight, then those discussions must begin now. Among the concerns about leveraging private infrastructure in war time is the flow of data.

12 I too was one of these optimistic scholars. Kollars, Nina A., and Andrew Sellers. "Trust and information sharing: ISACs and US Policy." *Journal of Cyber Policy* 1, no. 2 (2016): 265-277. But see also: Lu, Qingchang, Muhammad Umar Farooq, Xiaoyu Ma, and Robina Iram. «Assessing the combining role of public-private investment as a green finance and renewable energy in carbon neutrality target.» *Renewable Energy* 196 (2022): 1357-1365. Hodge, Graeme A., and Carsten Greve. «Public–private partnerships: an international performance review.» *Public administration review* 67, no. 3 (2007): 545-558.

13 Lilly, Bilyana, Kenneth Geers, Greg Rattray, and Robert Koch. "Business@ War: The IT Companies Helping to Defend Ukraine." In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, pp. 71-83. IEEE, 2023.

Peril 2: You're Here with Everybody Else in a Congested Use Environment.

When Elon Musk and Volodymyr Zelensky trade barbs on X, and when ship tracker H.I. Sutton, and Tanker Trackers can find the global position of navies, and when the Marine Corps solicits help from citizen observers to find their lost F-35. Something is afoot in skill spaces normally reserved for intelligence and military action.

EDTs leveraged in conflict, will be competing for an already crowded data and user environment. For example, EDTs that are easily applied to social media platforms, or as additions to the ubiquitous mobile phone application environments are giving rise to enhanced opportunities to influence human behavior and belief. Software that can generate deep fakes—whether photographs, phone, or video—open users to the opportunity to leverage deep fakes to mislead and shape the information environment. While militaries would like to use these systems as well, they will be doing so in an already saturated and potentially more volatile space during conflict. Similarly, image and language processing software, combined with open-source data, can help track and identify persons and asset movement. Industry already readily uses these monitoring systems and will increasingly rely upon advanced computing to greater effect. Militaries will also want to tap into these systems. The problem is, everyone else is here with you, and they're adopting the systems to their own purposes faster than militaries can, and once again, likely on private sector infrastructure (see Peril 1)

Peril 3: Scaling EDT With Yesterday's Technology

In spite of the continued and unoriginal harangue of policy makers and innovation organizations like the Defense Innovation Unit, there are real economic reasons why militaries cannot change at the pace of consumer technological shifts. These reasons are not the familiar small politics ones like bureaucratic lethargy, perpetual ruggedization schemes, or pork barrel political schemes for re-election. But less obviously So, what if a great power military simply decided that it will slap the table and invest in a singular military-only infrastructure that can operate without using civilian data infrastructure? This is one pathway that could be pursued. On this path, we simply shoot for 'good enough' and commit to being outdated. After all, given the structure of the EDT electronics marketplace that is made up of disposable short-lived whiz-bangs, a military could not possibly man, train, and equip at the cutting edge. That would be a terrible idea, and a horrifying pathway to outrunning our allies and partners in nearly every way. And yet, very few people caught up in the innovation churn of Silicon Valley's critique of US Department of Defense acquisitions woes ever offer this up. But it could be a solution. The promise here is to invest in minimal data sipping systems that operate only on data that is necessary for operations. The upside of going this route is the reverse of the prior point. It is likely systems that are simpler will work better in the melee of war fighting. Data sipping semi-rugged networked systems could be vaguely dumb, rather than supremely smart, vastly simplifying the complexity of the computing systems and limiting the appetite of leadership to try and see everything everywhere. Seeking the anti-exquisite path is to give up on the fancy dream of MDO, but to design for something far more familiar with just a little more data and coordination. Systems like this are likely to be cheaper, and more useful on the battlefield with fewer bells and whistles, but also less complex maintenance, and fewer dependencies.

Bonus Peril: Knowing is Not Enough.

Finally, a sore and sad truth remains. While leveraging peacetime smart data assets to discover new behaviors, for discerning new indicators and warnings, or in the service of deterrence by detection, a massive kinetic war aided by a bespoke JADC2 still suffers from the weakness of any military, its supply chain. Ultimately, victory in a general war will require a massive munitions stockpile and defense industrial base. It isn't enough to have the data systems and sensors. Knowing what is happening is not the same as doing something about it. Data moves very quickly but military assets—the resupply and sustainment move at the speed of humanity. Even the fastest physical assets require an industrial base to mass produce the necessary munitions to accompany these networked systems. Perhaps at first, in a kinetic fight, the data and the kinetics will match pace, if we are lucky. But then, at some point, likely in a few days to a week or so, we will go Winchester. We will run out of things to hurl at each other. At that point, it really doesn't matter how exquisite your data systems are in a high-end fight. The re-supply will bottom out, and we could be stuck watching slow moving cargo ships at sea on high resolution giant screens powered by billion-dollar software and networks toddling across the ocean. And war will look like it always has, grindingly slow, and sad.

In sum, the promise of data-centric EDTs to a warfighting force must be tempered with the knowledge of the infrastructure and developers who provide it. It is my guess—whichever capabilities are purchased and leveraged for military use, will be used within the larger melee that is the existing context of use by literally, everyone else. Thus, it is likely that data-centric EDTs will yield more utility in peace and the period leading up to conflict than in a kinetic fight. Thus, my guess is that optimized usage of data and data processing machines will remain elusive to modern military forces as a centerpiece to victory. An ancillary story perhaps, but not the centerpiece. For all those who hope to realize the visions laid out in so many OV1s I sincerely hope that I am wrong. And one of the reasons I am encouraged to write about this is that the debate should begin immediately of the effect of these three factors on the de-risking, and right-sizing of MDO.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl