Modelling Multi-Domain Conflict – Conceptualizing 'War 2.0'

Dr. K. Scott
De Montfort University
Leicester LE1 9BH
UNITED KINGDOM

jklscott@dmu.ac.uk

ABSTRACT

"World War III is a guerrilla information war with no division between military and civilian participation." – McLuhan [1].

In the current conflict in the Ukraine, it has been claimed that Russian information warfare has been poorly-conducted and largely ineffective. However, as *Dan Milmo and Pjotr Sauer have observed [2], this is only true if we neglect the influence campaigns being conducted beyond Europe and the Anglophone sphere. In a world of global communication, we need to adopt a global perspective and look beyond the immediate confines of any theatre of conflict. Similarly, the concept of 'unrestricted warfare' requires us to adopt a model of 'warfare' which goes far beyond the traditional idea of the exercise of kinetic and military force. This paper will present a framework for the analysis and modelling of conflict which will better enable all participants/stakeholders (military and civilian) to prepare for and respond to 'unrestricted warfare', and which offers an initial system for wargaming such conflict. 'Multi-domain' warfare must consider not just the 5 domains of land/maritime/air/space/Cyber and Electro-magnetic, but the intersections between civil and military spheres within these domains, and the requirement to think beyond conventional spheres of responsibility. True cognitive superiority can only be achieved by transcending traditional divisions; the model advanced in this paper offers a first step towards this.*

1.0 DEFINING FUTURE CONFLICT

"Prediction is very difficult, especially if it's about the future." (Niels Bohr)

What follows is an attempt to devise a working hypothesis about the possible nature of forms of future conflict (referred to from now on by the shorthand term 'War 2.0'), drawing on and seeking to synergise the opinions seen in a wide range of source texts (*inter alia* [3] – [10]). In attempting to determine what war in the near (let alone distant) future may be, we must first accept that any predictions will be at best partial, in both senses of the word (incomplete and prejudiced). While we can hypothesise based on historical experience, knowledge of current capabilities and technical and geopolitical trends, much of what we do will inevitably be at best educated guesswork. That said, a consideration of the current threat landscape suggests that when planning for future conflict, we should bear in mind two guiding principles, both coined by Marshall McLuhan. The first is the epigraph to this article [1], and the second comes from *War and Peace in the Global Village*: [11] "Every new technology necessitates a new war". The technological tools at our disposal will inevitably shape all levels of warfare, from the operational to doctrine. In his study of what he terms the 'scientific way of warfare' Bousquet [12] maps out the connection between technology, scientific theory, and forms of conflict:

Table 1: The four regimes of the scientific way of warfare ([8], p. 30).

	Mechanism	Thermodynamics	Cybernetics	Chaoplexity
Key Technology	Clock	Engine	Computer	Network
Scientific concepts	• Force • matter in action • linearity • geometry	• Energy • entropy • probability	• Information • negentropy • negative feedback • homeostasis	• Information • non-linearity • positive feedback • self-organization • emergence
Form of Warfare	• close order drill • rigid tactical deployments	• mass-mobilization • motorisation • industrialisation	• command and control • automation	• decentralisation • swarming

He argues that we have entered the age of 'chaoplexity' (a blend of 'chaos' and 'complex'), characterised by non-linearity and non-hierarchical, self-governing systems, and a near-total absence of traditional command and control structures. John Robb [13] provides an excellent study of how what he terms 'open source warfare' works out in practice, while Adam Roberts [14] presents a fascinating piece of speculative fiction, in his depiction of a private military contractor operating as a truly self-sustaining, anarchic (in the true sense of the term) combat network. Central to all these visions of future is *information*, as both weapon and essential in gaining and maintaining advantage. It is not going too far to say that the development and proliferation of IT and AI are the essential elements that shape all future potential conflict; the implications for combat, command and control and planning are huge [15]. From potential autonomous weapons systems to human-machine teaming [16] and AI-driven analysis [17], these technologies will inevitably generate 'new war'.

The concepts of Multi-Domain Integration and Operations have become central to modern defence [18], [19], and it is vital to note that full spectrum dominance in a multi-domain battlespace requires an awareness that the 5 key domains (land, maritime, air, space and cyber/electromagnetic; the UK links Electronic and Information Warfare in its conception of the 5th domain) are not discrete realms, but inextricably interlinked and interdependent. More than that, the cyber/informational domain is the spine that runs through all other domains; without an informational network, C4ISTAR collapses.

Where much thinking on MDI proves deficient is that it restricts itself to the martial realm; we plan Multi-domain operations in terms of military force (kinetic and non-kinetic), and fail to remember McLuhan's dictum that future war makes "no division between military and civilian participation." [1] The idea that war is a purely military concern has never been true, and as will be discussed below, it is central to one key model for conflicts to come. The UK model of MDI does place the 5 domain structure within a wider network of relationships with allies and home government actors/stakeholders, but this still fails to grasp the full complexity (or chaoplexity) faced.

In 1999, Qiao Liang and Wang Xiangsui published 超限戰, translated as *Unrestricted Warfare China's Master Plan to Destroy America* [20]. In this work, they outline a model for conflict which "which transcends all boundaries and limits" ([20], Introduction), and "all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed" ([20], Introduction.) They declare:

> *(O)nly if we break through the various kinds of boundaries in the models of our line of thought, take the various domains which are so completely affected by warfare and turn them into playing cards deftly shuffled in our skilled hands, and thus use beyond-limits strategy and tactics to combine all the resource is of war, can there be the possibility that we will be confident of victory. ([20], pp. 200-1).*

Such, then, is the challenge; a world of chaoplexic conflict, enabled by IT and AI, where power projection across the informational domain can damage an opponent without a shot being fired, and where attribution can be next to impossible. The use of proxy forces and private military contractors add further complexity. Tactically, the rise of non-linear, hybrid, open source warfare poses huge challenges for conventional military forces and governments, as shown by the West's response to Russian actions [21] before the recent and much less effective return to conventional tactics in Ukraine. We are severely challenged by the current state of play; attempting to work out how to mitigate against future unknown threats seems next to impossible. As Rosa Brooks puts it:

> *It's time to accept that "war" and "peace" are not binary opposites, but rather the outer limits of a continuum. Indeed, add in cyber, individualized weapons, and various nonlethal forms of coercion and control and a two-dimensional continuum may not be enough: we may need to conceptualize warfare in three dimensions, or even more [22].*

What follows is a first step towards such a model.

2.0 MODELLING FUTURE CONFLICT

"All models are wrong, but some are useful" [23].

How may we develop a model that will allow us to conceptualise, analyse, and model the phase space of 'War 2.0'? What follows sketches an initial framework which is scalable and flexible from city to country to international, and which allows us to consider multi- and cross-domain actions and results, aiming to, as General Sir Nick Carter put it, 'move beyond jointery' [24]. More than that that, it seeks to be portable; given the porosity (if not actual non-existence of boundaries between the domains of warfare and the military and civilian realms, our model must be accessible and usable by all potential targets of 'unrestricted warfare'.

The following model is adapted from one that was used to construct a conceptual framework for understanding and designing Influence Operations [25]: this is an attempt to broaden the span of investigation and application. If we accept that the future conficts will not respect the 'war/peace' boundary, then we need to be able to develop an abstraction that does the same. The basis of this model is a matrix formed of the intersection of the categories used in the PMESII and ASCOPE analytical techniques, creating a 6x6 matrix, defining target areas as variables (PMESII) within the dimensions offered by ASCOPE (Table 2 below).

This matrix is already used by, *inter alia*, NATO's Civil-Military Cooperation Centre of Excellence, and provides a sure foundation for the next level of information, namely moving the 2-dimensional matrix into a 3-dimensional form, by adding a layer for each of the five domains of warfare (Land, Maritime, Air, Space, Cyber/ElectroMagnetic). This then creates a form composed of 6x6x5 = 180 cells, allowing us a high degree of precision in defining the origin, target, and spread of an attack (Figure 1). More than this, it also offers a taxonomy of locations and and actors which is meaningful in contexts beyond the purely military. It also allows the logging of incidents/attacks from the perspective of attacker, defender, or neutral party.

Table 2: The PMESII/ASCOPE matrix [26].

	P Political	M Military	E Economic	S Social	I Information	I Infrastructure
A Areas	Areas - Political (District Boundary, Party affiliation areas)	Areas - Military (Coalition / LN bases, historic ambush/IED sites)	Areas - Economic (bazaars, shops, markets)	Areas - Social (parks and other meeting areas)	Areas –Information (Radio/TV/newspapers /where people gather for word-of-mouth)	Areas – Infrastructure (Irrigation networks, water tables, medical coverage)
S Structures	Structures - Political (town halls, government offices)	Structures - Military / Police (police HQ, Military HHQ locations)	Structures - Economic (banks, markets, storage facilities)	Structures - Social (Churches, restaurants, bars, etc.)	Structures - Information (Cell / Radio / TV towers, print shops)	Structures - Infrastructure (roads, bridges, power lines, walls, dams)
C Capabilities	Capabilities - Political (Dispute resolution, Insurgent capabilities)	Capabilities - Military (security posture, strengths and weaknesses)	Capabilities - Economic (access to banks, ability to withstand natural disasters)	Capabilities - Social (Strength of local & national ties)	Capabilities - Info (Literacy rate, availability of media / phone service)	Capabilities - Infrastructure (Ability to build / maintain roads, walls, dams)
O Organizations	Organizations - Political (Political parties and other power brokers, UN,)	Organizations - Military (What units of military, police, insurgent are present)	Organizations - Economic (Banks, large land holders, big businesses)	Organizations - Social (tribes, clans, families, youth groups, NGOs / IGOs)	Organizations - Info (NEWS groups, influential people who pass word)	Organizations - Infrastructure (Government ministries, construction companies)
P People	People - Political (Governors, councils, elders)	People - Military (Leaders from coalition, LN and insurgent forces)	People - Economic (Bankers, landholders, merchants)	People - Social (Religious leaders, influential families	People - Info (Media owners, mullahs, heads of powerful families)	People - Infrastructure Builders, contractors, development councils)
E Events	Events - Political (elections, council meetings)	Events - Military (lethal/nonlethal events, loss of leadership, operations, anniversaries)	Events - Economic (drought, harvest, business open/close)	Events - Social (holidays, weddings, religious days)	Events - Info (IO campaigns, project openings, CIVCAS events)	Events - Infrastructure (road / bridge construction, well digging, scheduled maintenance)

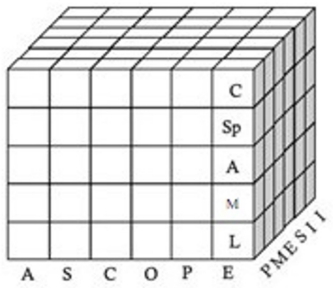

Figure 1: The 3-D model of the multi-domain 'unrestricted' battlespace, ASCOPExPMESIIx5 domains of warfare (land, maritime, air, space, and cyber/electro-magnetic).

This basic model lends itself easily to tailoring and/or refinement. In its original form, the 3-D matrix was composed of a 6x6x4 framework, corresponding to PMESII+ASCOPE+DIME (Diplomacy, Information, Military, Economy). A further level of detail was added by giving each of the component blocks one of three 'spins' (analogous to quarks) to correspond to the strategic, tactical, and operational levels. Each layer of the basic framework could also be used as the base for a new 3-D 5x5x5 matrix, with the Z-axis representing the 5 ways of responding to an attack (or indeed the 5 forms an information attack may itself take): *disrupt*, *deny*, *degrade*, destroy, or *deceive*.

One important feature of this model is that it moves away from focusing on protagonists' action on any one element or domain of the battlespace, and to adopt a holistic perception of the multi-domain system. It enables analysts to plot actions moving across domain boundaries, mapping the possible cross-domain repercussions of a particular act: such a model allows us to think more clearly about the identification of *Systempunkts* (those points in a network which if attacked lead to a cascade failure [27]). Similarly, as we move towards a fully integrated 'Internet of Battlefield Things', generating a vastly increased and unceasing stream of data across the domains, we can posit an AI-enabled monitoring of the state of the system, and highlighting changes in specific cells which are indicative of likely hostile action; each of the 180 cells of the model becomes a unit of information, any change in its status acting as 'a difference which makes a difference' (Bateson's definition of the 'bit' [28]). To return to the idea of constructing a better controlling narrative for engaging with modern conflict, what this gives us is a mapping tool for specific landscapes, and a mechanism for generating actions which can be tracked as they pass through the domains. It is both setting and plot generator. It does not suggest who might populate this landscape, but it allows population by any and all of the possible threat actors we see emerging in the present. Above all, it is designed to focus on event and repercussions; while knowledge of *who* our adversaries are (or might be) is vital (identity, individual and cultural, predisposes to certain actions), we must concentrate on *what* they do.

If we accept that this model is effective in allowing us to map multi-domain unrestricted conflict, then the next step to examine how it could be used in a wider context; how can we use this model in a dynamic, experiential process of experimentation and analysis? How, in short, can we place it at the centre of a ('serious') game?

As with the Influence gaming project discussed earlier [24], for this to work, it must seek to consider as many inhabitants of the attacks surface as possible – involvement of military, governmental, academia, and private sector subject matter experts will be required. Combatting unrestricted warfare requires an unrestricted series of inputs. The author's previous experience confirms him in his belief that such an exercise is possible; what is needed is a group of individuals prepared to look beyond the walls of their specialist silos and collaborate. As Wiener [29] says, 'There is no Maginot Line of the brain'; our opponents look beyond traditional boundaries, and so must we. This is, then, an invitation to any and all who see the merit of the ideas advanced here, and who would wish to be involved in such a project. In his previous work, the author was part of a truly multidisciplinary, international team, and an exercise such as is proposed here will require an even greater range of expertise; NATO offers the perfect environment to build such a project. The author welcomes all expressions of interest, and hopes that the end of this paper will mark the beginning of an innovative and worthwhile endeavour.

3.0 REFERENCES

[1] McLuhan, M. (1970). *Culture Is Our Business*. New York, NY: Ballantine Books, p.66.

[2] Milmo, D. and Sauer, P. (2022)." Deepfakes v pre-bunking: is Russia losing the infowar?", in *The Guardian*, 19 March, [Online]. Available: https://www.theguardian.com/world/2022/mar/19/russia-ukraine-infowar-deepfakes

[3] Cohen, R. S. *et al*. (2020). *The Future of Warfare in 2030: Project Overview and Conclusions*, Santa Monica, Calif Ministry of Defence Strategic Trends Programme. (2015).

[4] *Future Operating Environment 2035*, Shrivenham: Development, Concepts and Doctrine Centre: RAND Corporation.

[5] Gaub, F. (ed.). (2020). *Conflicts to Come: 15 Scenarios for 2030*, Paris: European Union Institute for Security Studies.

[6] Valasek, T. (ed.). (2019). *New Perspectives on Shared Security: NATO's Next 70 Years*, Washington DC: Carnegie Endowment for International Peace.

[7] Ministry of Defence Strategic Trends Programme. (2015). *Future Operating Environment 2035*, Shrivenham: Development, Concepts and Doctrine Centre.

[8] Johnson, R. A. (2014). "Predicting Future War," *Parameters* 44, no. 1, pp. 65-76.

[9] Roberts, P. (ed.). (2019). *The Future Operating Environment Out to 2030*, London: Royal United Services Institute.

[10] Amerson, K. and Meredith S.B. (2016). 'The Future Operating Environment 2050: Chaos, Complexity and Competition,' *Small Wars Journal* [online], 31 July, https://smallwarsjournal.com/jrnl/art/the-future-operating-environment-2050-chaos-complexity-and-competition

[11] McLuhan,, M. and Fiore, Q. (1968). *War and Peace in the Global Village*. San Francisco, CA: Hardwired, p. 98.

[12] Bousquet, R. (2008). *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, London: Hurst, UK.

[13] Robb, J. (2017). *Brave New War: The Next Stage of Terrorism and the End of Globalization*. New York, NY: John Wiley & Sons.

[14] Roberts, A. (2011). *New Model Army.* London, UK: Gollancz.

[15] Scott, K. (2022). "Reith, Russell, and the Robots: AI, Warfare, and Shaping the Debate," in *Proc 21st Eur. Conf. on Cyber Warfare and Security*, pp. 443-9.

[16] Ministry of Defence. (2018). *Human-Machine Teaming: Joint Concept Note (JCN) 1/18*, Shrivenham: Development, Concepts and Doctrine Centre, UK.

[17] Layton, P. (2021). "The Artificial Intelligence Battlespace." RUSI.org. https://rusi.org/explore-our-research/publications/commentary/artificial-intelligence-battlespace. (accessed July 5, 2022).

[18] Ministry of Defence. (2020). *Joint Concept Note 1/20: Multi-Domain Integration,* Shrivenham: Development, Concepts and Doctrine Centre, UK.

[19] Gov.uk. (2022). "Guidance: Multi-Domain Integration". Gov.uk. https://www.gov.uk/guidance/multi-domain-integration. (accessed July 5, 2022).

[20] Qiao, L., and Wang, X. (2020). *Unrestricted Warfare: China's Master Plan To Destroy America*, Lambertville, NJ: Shadow Lawn Press. [Kindle Edition].

[21] Pomerantsev, P. (2014). "How Putin is Reinventing Warfare," *Foreign Policy,* 5 May. [Online]. Available: https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/

[22] Brooks, R. (2016). *How Everything Became War and The Military Became Everything: Tales From The Pentagon*, New York, NY: Simon and Schuster, p.6.

[23] Box, George E. P.; Norman R. Draper (1987). *Empirical Model-Building and Response Surfaces*, New York, NY: Wiley, p. 424.

[24] Carter, N. (2019). "Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019"" rusi. Org. [Online]. Available: https://rusi.org/event/annual-chief-defence-staff-lecture-and-rusi-christmas-party-2019

[25] Kodalle, T., Ormrod, D., Scott, K., and Sample, C. (2019) "Thoughts about a General Theory of Influence in a DIME/PMESII/ASCOP/IRC2 Model". *Journal of Information Warfare,* vol. 19, no. 2. [Online]. Available: https://www.jinfowar.com/journal/volume-19-issue-2/general-theory-influence-dimepmesiiascopirc2-model

[26] Adopted from an open source planning template: https://www.trngcmd.marines.mil/Portals/207/Docs/wtbn/MCCMOS/Planning%20Templates%20Oct%202017.pdf?ver=2017-10-19-131249-187 last visited on 17. March 2019.

[27] Shachtman, N. (2007). "Inside the *Brave New War*, Part 2," wired.com, 17 May. [Online]. Available: https://www.wired.com/2007/05/q-tell-me-more-/

[28] Bateson, G.W. (1972). *Steps to an Ecology of Mind*. New York: Ballantine Books, p.315.

[29] Wiener, N. (1989). *The Human Use of Human Beings: Cybernetics and Society.* London: Free Association Books, UK, p. 122. First published 1950.