‘Out Beyond Jointery’: Developing a Model for Gaming Multi-Domain Warfare

Keith Scott

De Montfort University, Leicester, UK

jklscott@dmu.ac.uk

Abstract:

Play is battle and battle is play. [Huizinga, Homo Ludens]

What Huizinga is saying here is not that conflict is *playful*, but rather, it is a *game*, following set rules of conduct and occurs within a defined zone of action. Elsewhere in *Homo ludens*, he argues that modern warfare operates without the ritualised, rule-based structure of, for example, the mediaeval tourney. The purpose of this paper is to consider the ways in which a model based on the structure of games may help us better engage with the challenges of Multi-Domain Conflict. We are all familiar with the concept of Cyber as the 5th Domain of warfare, but we need to consider it not as a discrete zone, but as running through and interpenetrating the other 4 (Earth, Sea, Air, Space), the informational spine that enables all other forms of conflict. This paper will: 1. Discuss the developing concept of Multi-Domain Conflict as a move ‘beyond jointery’ (as General Sir Nick Carter put it) into a truly integrated form of warfare, blurring and collapsing boundaries between kinetic and non-kinetic, between the services, and between military and civilian authority; 2. Outline a theoretical model for conceptualising Multi-Domain Conflict as gamelike in form, with environments of operation (‘boards’), protagonists (‘players’), and possible forms of action (‘moves’). As befits a conference on Cyber and Information Warfare, it will argue that the D5 model of IW (Deny, Disrupt, Degrade, Deceive and Destroy) is portable and scalable across the other 4 domains (Land, Sea, Air, Space); 3. Show how this theoretical model can be employed both to model and simulate Multi-Domain Conflict; wargames have been a key element of military planning and training for at least a century – this paper argues that we need to develop a new *Kriegspiel* to better understand coming conflicts.

[...] theories are only made to die in the war of time. Like military units, they must be sent into battle at the right moment; and whatever their merits or insufficiencies, they can only be used if they are on hand when they’re needed. [Debord 1978, p.10]

Keywords: Multi-Domain Conflict; Serious Gaming; Information Warfare; Cyber Warfare

1. Introduction

In 2013, Thomas Rid published a work which claims categorically that *Cyber War Will Not Take Place*. This declaration is, I argue, fundamentally wrong, based as it is on a definition of ‘war’ which, as will be shown, is inadequate for understanding the complex and proteiform nature of present and future conflict. It is not simply the case that cyber warfare *does* exist as a discrete and developing form of warfare, where cyber ‘munitions’ blur the traditional division between kinetic and non-kinetic effects (Stone 2013; Farwell & Rozhinski 2011; Collins & McCombie 2012; Zetter 2014), but that conflict within the Cyber domain is an inevitable and necessary element of warfare. This paper will present three themes related to contemporary and future warfare:

1. an analysis of ‘war’ (arguably a highly contested term) in its actuality, moving away from the traditional Clausewitzian model towards a conception of a much broader and complex form of interlinked and interacting multi-domain conflict;
2. an attempt to develop an initial conceptual model for mapping, modelling and analysing multi-domain conflict;
3. a discussion of how such a conceptual model may form the basis for future wargame-based modelling and simulation exercises for all stakeholders (not merely the military) in an era of ‘unrestricted warfare’.

We begin with an apparently straightforward question: what *is* War? Thomas Rid argues that, within his definition of the term, ‘cyber warfare’ is not a true concept, as it does not automatically imply the use of *force*:

An act of war is always instrumental, and to be instrumental there has to be a means and an end: physical violence or the threat of force is the means; forcing the enemy to accept the offender’s will is the end.

[Rid: 2]

While he accepts that cyber actions can cause damage equivalent to that of kinetic weapons, he states that they do not cause physical harm on a scale equivalent to that of conventional ordinance’s ‘shock and awe’:

The use of cyber weapons that could inflict damage and pain comparable to the pummeling of Dresden, London, Belgrade, or Beirut at the receiving end of devastating airpower is, at present, too unrealistic even for a bad science fiction plot. [19]

Thirdly, he argues that war always ultimately requires a declaration of hostilities, and cannot be fought *sub rosa*, because 'History does not know of acts of war without eventual attribution' [2].

Ultimately, he contends that the very concept of 'cyber war' is an impossibility:

cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future. [xiv]

Rid's argument is clear, meticulously structured and well-informed, and to a certain extent true, but only within the frame of reference he uses, which rests on a very narrow definition of what 'war' is. His model is essentially Clausewitzian, and this, I contend, is an inadequate model to understand conflict in our era, and indeed in considering conflict in general. Clausewitz died in 1831, in an era which was overwhelmingly pre-Industrial, where limitations of military technology (single-shot muskets, cannon with limited range and slow rate of fire, poorly armoured and slow cavalry...) restricted combat to overwhelmingly large-scale, close-range massed set-piece battles, where the objective was to destroy the enemy's forces and conquer the physical terrain. Moreover, warfare in Clausewitz's era was limited to two domains (land and sea; air warfare truly begins in the 1850s with the use of balloons for reconnaissance and limited offensive action); we now operate in five (land, sea, air, space, and cyber (including both information space and the electromagnetic spectrum). To employ the terminology employed by Lind et al (1989) and Hammes (2006), Clausewitz was fighting 1st-Generation warfare; we are now facing 4th Generation conflict.

It should not be thought, however, that my objection to Rid's use of a Clausewitzian standpoint is due to the latter's position as a historical figure; indeed, a figure from a much earlier period in the history of the development of strategic theory seems to offer a set of ideas which map closely onto the modern era. Living about 2000 years before Clausewitz, Sun Tzu presents a model of warfare which runs explicitly counter to Rid's. Where Rid argues that attribution is central to war, Sun Tzu prefigures the doctrine of maskirovka when he declares 'All warfare is based on deception' (*The Art of War*, p.3). Where Rid states that the employment of overwhelming physical force is an essential element of warfare, Sun Tzu that victory can be achieved in many ways: 'to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting' (*The Art of War*, p.8).

My main concerns with Rid's contention are twofold. Firstly, he does not seem to see that cyber actions can have effects that are as physically and psychologically devastating as kinetic warfare. We know that the SCADA systems which control much of our critical national infrastructure are hugely vulnerable to cyber attack (Shaw 2004; Yadav and Paul 2019; Trend Micro 2019). Any IT-controlled system is potentially vulnerable to attack and disruption, with potentially catastrophic results; consider for example the likely outcome of a coordinated series of attacks on the air traffic control systems at major airports (Tamimi, Hahn, and Roy. 2020; Hird 2020). Add to this the challenges posed by attacks to the financial system, and the opportunities for Information Warfare offered by social media, and the possibilities of cyber-created 'shock and awe' are all too evident. Just because we have (apparently) not yet seen such a large-scale attack does not mean that it could not or will not happen, nor that we should not prepare for it. Thinking the unthinkable is a key element of effective security. We must also consider that a networked society, where all zones of human activity – civil and military, private and public sector, individual and collective – are intimately and inevitably interconnected leads to a vastly increased attack surface. One of the fundamental principles behind this paper is that conflict is now inherently *multi-domain*, and that actions in one domain can and must be evaluated for their possible effects in other domains. The cyber domain in effect forms an informational spine which runs through (and in many cases runs) actions in all the other domains, and effective cyber security must draw on the expert knowledge of those who work in all other spheres of human activity. Put crudely, 'what happens in cyber does not stay in cyber'.

My second objection to Rid's conception of warfare is more wide-ranging; it rests on a very simple question, the answer to which is highly complex: what *is* war? There is in fact no single definition in international law of the term; we have codes of conduct concerning behaviour during war (most notably the Geneva Conventions), but no official summation of what war actually consists of. If it is a large-scale open conflict between nation states,

then the 'War on Terror' is not a war (neither Al-Qaeda nor ISIS/ISIL/Daesh are nation states). If an official declaration of war is required, then the UK has not been at war since 1942, when it declared war on Siam; similarly, the last declaration of war by the United States was also in 1942, against Bulgaria, Hungary, and Romania. Hence, the 'wars' in Vietnam, Korea, the Falklands, and Iraq cannot be officially named as such; this is clearly ludicrous. Consider the wikipedia entry for 'Outline of war'; there is no single overarching definition, merely a quasi-fractal proliferation of subcategories. There are *wars* (asymmetric, network-centric, unconventional, psychological...) but no *war*.

Jason Rivera (2014) maps out a taxonomy of forms of conflict, marking a clear delineation between 'war' and 'not-war' (Figure 1 below); such a neat division is arguably illusory.

Figure 1: a mapping of 'war' and 'not-war' (Rivera 2014).

Examine a selection of the recent work on grey zone conflict (Carment and Belo 2020; Hoffman 2018; Morris *et al* 2019; Raine 2019 *inter alia*) and what becomes clear is that this hybrid, liminal form of 'warfare' is becoming ever-more common, posing a profound challenge to existing models of the war/peace division. As Rosa Brooks (2016) observes, it is perhaps time that we

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.

The conceptual basis for such conflict has been advanced by Qiao and Wang, in the work translated as *Unrestricted Warfare*. These two officers of the PLA argue that war can be fought in many ways, kinetic and non-kinetic, mentally and physically, across all spheres of activity:

all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will, it means that all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed

Coleman (2009; 2006) lays out what he terms the '15 modalities of Unrestricted Warfare' as

1. Cultural warfare
2. Economic warfare
3. Environmental warfare
4. Financial warfare
5. Illegal drugs warfare
6. International law warfare
7. Information and media warfare

8. Telecommunications and network warfare
9. Political warfare
10. Psychological warfare
11. Resource warfare
12. Smuggling warfare
13. Technology warfare
14. Terrorist warfare
15. Gang warfare

(he sees modalities 7, 8, and 13 as the ambit of Cyber warfare; 9 and 10 should surely also be considered as falling within its domain).

Rid, with his narrow neo-Clausewitzian conception of war, has no adequate way of responding to Qiao and Wang's infinitely wider and more open vision of how conflict can be conducted in many different ways in many different arenas. If we imagine combat between forces driven by these two opposed mindsets, it seems hard to see that Rid's side would emerge victorious. Qiao and Wang display a willingness to work across traditional barriers, and to embrace as wide a range as possible of strategies and tactics:

only 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 resources of war, can there be the possibility that we will be confident of victory. [200-01]

War has always been a complex, proteiform entity; what changes is our belief as to what falls within the class of 'acceptable forms of war'. If, however, we do as Rid does, and seek to deny the existence of forms which lie beyond those of which we approve, then we will inevitably fail. The model of Unrestricted Warfare gives us the 'what' and 'how' of modern warfare; to understand the 'where' we must consider the growing interest in Multi-Domain warfare.

2. Multi-Domain Conflict

In 2019, the then Chief of the UK Defence Staff, General Sir Nick Carter, delivered a speech in which he made many of the same points outlined above, arguing that the traditional idea of 'war' and 'peace' as discrete states is illusory. He discussed certain (unnamed) nation states, and quoted Edward Lucas (2019), saying:

these regimes [...] view the strategic landscape as characterised by a continuous and never-ending struggle that encompasses everything from what the West calls 'peace' to nuclear war. When they consider conflict along this spectrum, the primary change from one end to the other is the relative weighting that is given to non-military and military instruments. These regimes believe that they are already engaged in an intense form of warfare, but it is political conflict and not kinetic warfare. Their primary operational focus is on employing a range of mainly non-military instruments in non-traditional ways below the threshold of large scale conventional military operations to achieve strategic gains [Carter 2019].

We should note that in Lucas' original article, he actually names the states involved; it should come as no surprise that one of them is the state whence comes the theory of unrestricted warfare. Carter and Lucas are making precisely the point made throughout this paper, that 'war' and 'peace' occupy opposite poles on a continuum, or a cycle:

The linear depiction of peace to war and back again must be revised to reflect the cyclical nature of war where there are only positions of relative advantage. The continuum of conflict is defined by competition short of conflict, conflict itself, and the return to competition (Perkins 2017)

This conception of war as cyclic, rather than linear, shifting constantly and endlessly from high- to low-intensity and back again, is matched by the appearance in recent years of a model of military operations which is truly holistic, and collapses the traditional divisions between different services' domains of activity; we are, it is

argued, in the age of ‘multi-domain warfare’. A review of some of the most recent work in this field¹ shows an attempt to, in Carter’s words, ‘move beyond jointery’ and develop fighting forces which can operate in a truly integrated manner, going far beyond the idea of ‘combined operations’ (the logical extension of the idea of multi-domain conflict, namely abandoning the tradition divisions between the various branches of the armed services, has not as yet truly been engaged with, for reasons it is not hard to determine). The UK Ministry of Defence’s *Joint Concept note 1/20* depicts the way in which the multi-domain model sees the 5 domains of conflict operating (Fig.2 below); through a series of overlapping zones of effect, Air wraps around Land and Sea, Space wraps around these, and the fifth domain (here defined as ‘Cyber and electromagnetic’) surrounds them all. This is a fair first step at conceptualising the multi-domain environment, but it is flawed, for 2 key reasons:

1. **Conceptual Incompleteness:** this model still suggests that the domains are discrete, if overlapping, zones, whereas a truly multi-domain conflict will operate through and within multiple domains simultaneously, and the boundaries between the zones are at best a matter of convention, rather than reality (for example, which domain does a UAV controlled by a land unit launching an attack from the air on a maritime target ‘belong’ to?). Secondly, and crucially, this model fails to grasp the full complexity of the relationship between the ‘cyber’ domain and all the others; it does not simply envelop the others, it runs through them, penetrating and connecting them, the informational skeleton or nervous system without which none of the others can operate. Any map, of course, is a reductive model of reality, a 2-D depiction of a 3-D environment, but multi-domain warfare requires a ‘map’ which can better present the interconnection and interpenetration of actions and effects (kinetic and non-kinetic).
2. **Limitation of Scope:** It is perhaps unsurprising that a model devised by the Ministry of Defence should consider multi-domain conflict as a purely military affair; however, it is inadequate for examining war as it truly is (and arguably always has been). Firstly, war has always affected civilian populations, either as victims caught in the crossfire, or as deliberate targets. Secondly, warfare in its ‘unrestricted’ form is ‘fought’, not just by soldiers in a combat environment, but non-kinetically, in the economic, political, and sociocultural domains. If we cannot include the non-military in our model, we fail to grasp the true nature of the situation, and our attempts to achieve true full-spectrum dominance are doomed to failure before we begin. Multi-domain conflict is by its essential nature multi-agency and multi-stakeholder, and to be successful, we must find a way of modelling such a hugely complex system of systems. As recent examples of Whole of Government and multinational operations during the pandemic have shown, co-ordinating action across the civil powers of a single nation state is challenging enough; to be truly successful, we need to be able to consider how to operate across the traditional borders between civil and military powers (without surrendering to totalitarianism and a one-party state) and national boundaries. What follows is an attempt to devise an initial mapping of such a system, designed to allow us to *analyse* multi-domain conflict, and to *conduct* it more effectively. As George Box (1976) said, ‘all models are wrong’ (p.792); the following model seeks to be slightly less wrong than those currently in operation.

¹ See, *inter alia*, Clare 2020; Gady and Stronell 2020; Jones and Diaz de Leon 2020; McCoy 2018; Ministry of Defence 2020; TRADOC 2017 and 2021.

Figure 2: Illustration of domains as per UK doctrine (Ministry of Defence 2020: p. 18)

3. Modelling the Multi-Domain

The following model is adapted from a conceptual framework for understanding and designing Influence Operations (Kodalle *et al.* 2019). Any abstraction of reality is inevitably a simplification, and it would be easy to devise an ever-more detailed taxonomy of the battlespace; at this stage, we are concerned with building a model that *works* more or less effectively. If we accept that the forms of conflict we will encounter in the future will cut across 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. The PMESII framework divides an operational environment into the following zones:

- P** – Political.
- M** – Military.
- E** – Economic.
- S** – Social.
- I** – Infrastructure.
- I** – Information.

This framework is then set alongside the complementary ASCOPE methodology, used to gain a better understanding of an Operational Environment in a COIN context. ASCOPE refers to:

A	–	Areas
S	–	Structure
C	–	Capabilities
O	–	Organizations
P	–	People
E – Events		

The PMESII/ASCOPE frameworks lead to creation of a 6x6 matrix, allowing us to define target areas as variables (PMESII) within the dimensions offered by ASCOPE (see Fig. 3 below).

	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 3: The PMESII/ASCOPE matrix²

The matrix is now expanded from two dimensions into three, adding a layer for each of the five domains of warfare (Land, Sea, Air, Space, Cyber). This then creates a cube composed of $6 \times 6 \times 5 = 180$ cells, allowing us a high degree of precision in defining the origin, target, and spread of an attack (fig. 4).

This basic model lends itself easily to tailoring and/or refinement. In its original form, the 3-D matrix was composed of a $6 \times 6 \times 4$ 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 $5 \times 5 \times 5$ 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*.

Figure 4: the 3-D model of the multi-domain battlespace, ASCOPExPMESIIx5 Domains of warfare (Land, Sea, Air, Space, and Cyber)

A 3-D model is of course much more challenging to visualise than a 2-D map, but the development of VR and AR technology offers a number of possible ways for employing this model; it gives us the ability to trace the path taken by an attack from one domain moving into others, and tracking the spread of its effect. (Consider a cyber

² 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>.

attack launched from a land base, transmitted through a satellite, to disable or degrade the effectiveness of maritime GPS systems; if such systems are carried on commercial freight shipping, this will effect international supply lines, and have a further effect on a national economy, civilian morale, and political stability.) Such a process of modelling and analysis can be enhanced by feeding in real-time data from the ever-growing range of sensors proliferating in civilian and military environments, while AI-driven Big Data analysis could see this form the basis for a predictive early warning system for future conflicts. Even at this initial stage, this model offers a means of analysing possible future events, and invites the user to think beyond the conventional idea of Force A launches Attack B on Target C, by presenting a much wider and deeper possible attack surface.

4. Next Steps

As stated throughout this paper, the model presented above makes no claims to be definitive; it does however seem to offer a more comprehensive and detailed conception of the battlespace within which multi-domain, unrestricted conflict can, does, and will operate. At a theoretical level, it seems to offer promise; how can we test it at a *practical* level? The obvious answer (assuming that starting a war is seen as undesirable), is to engage in a simulation or wargame. The matrix that forms the basis for this model was devised during the creation and testing of a wargame (Ormrod *et al* 2019) designed to simulate influence campaigns on an international level, taking a Whole of Government perspective and constructing teams of players from the military, governmental, business and academic sectors (precisely the multi-stakeholder perspective needed for combatting unrestricted warfare). In order to develop and refine the model proposed here, it must be tested, and the aim for future work is to scope the requirements for putting such an exercise into operation. As done in the 2019 exercise, the steps required will be:

1. assemble a team of interested stakeholders and subject matter experts to *design* the exercise, and a parallel group, drawn from as wide a pool as possible, to *test* it;
2. design an environment/gameworld within which the events of the exercise will occur;
3. devise a scenario (or set of scenarios) inviting/requiring a multi-domain response, with the use of our model as a support/guide for action and response;
4. playtesting (with an emphasis on Red Teaming; those engaged in defence must always consider the mindset of those *attacking* them – in order to protect a system, it is vital to know how it can be destroyed);
5. recording, reviewing, and revising the model, on the basis of the exercise.

We know that wargaming is a powerful tool for analysing previous actions and positing future events; the fact that the gaming of multi-domain conflict has already begun³ shows that it is seen as potentially helpful for considering the evolution of conflict. What this paper has sought to do is to challenge the ways in which we have previously conceptualised warfare, and to offer an initial step towards a better understanding and preparation for may lie ahead. The model it presents is portable and scalable, but it does not claim to be definitive.

References

- Box, G. E. (1976). "Science and Statistics", *Journal of the American Statistical Association*, Vol. 71, No. 356 (Dec., 1976), pp. 791-799.
- Brooks, R. 2016. *How Everything Became War and the Military Became Everything: Tales from the Pentagon*, Simon & Schuster, New York. Kindle Edition.
- Carment, D., and Belo, D. (2020) "Gray-zone Conflict Management: Theory, Evidence, and Challenges", *Journal of European, Middle Eastern, & African Affairs*, 9 June, [online], www.airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zone-conflict-management-theory-evidence-and-challenges/.
- Carter, N. (2019) "Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019", *gov.uk*, 5 December, [online], www.gov.uk/government/speeches/chief-of-the-defence-staff-general-sir-nick-carters-annual-rusi-speech.
- Clare, P. (2020). "The Answer is Multi Domain Operations – Now What's the Question?". *Wavell Room*, 13 February, [online], wavellroom.com/2020/02/13/the-answer-is-multi-domain-operations-now-whats-the-question/.
- Coleman, K. (2006). "The Challenge of Unrestricted Warfare - A Look Back and a Look Ahead", *Directions*, 12 January, [online], <https://www.directionsmag.com/article/3039>.
- Coleman, K. (2009). "Confronting UnRestricted Warfare", *military.com*, 3 March [online], <https://www.military.com/defensetech/2009/03/03/confronting-unrestricted-warfare>.
- Collins, S. and McCombie, S. (2012) "Stuxnet: the emergence of a new cyber weapon and its implications", *Journal of Policing, Intelligence and Counter Terrorism*, Vol.7, no. 12, pp.80-91.

³ Freedburg 2019; Jensen 2019; Lockheed Martin. 2019; Schuety and Hill 2018; Woodford 2019a and 2019b

- Debord, G., tr. Knabb, K. (1978). "In girum imus nocte et consumimur igni", the anarchistlibrary.org [etext].
- Farwell, J.P. and Rohozinski, R. (2011) "Stuxnet and the Future of Cyber War", *Survival*, 53:1, pp. 23-40.
- Freedburg, S.J. (2019). "Army Multi-Domain Wargame Reveals C2 Shortfalls", *Breakingdefense.com*, 12 September, [online], <https://breakingdefense.com/2019/09/army-multi-domain-wargame-reveals-c2-shortfalls/>.
- Gady, F-S, and Stronell, A. (2020). "Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030", NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.
- Hammes, T.X. (2004) *The Sling and the Stone: On War in the 21st Century*, Zenith Press, St Paul, Mn.
- Hird, J. (2020) "AIR TRAFFIC MANAGEMENT: A CYBERSECURITY CHALLENGE", *Transport Security International*, 21 August 2020, [online], www.tsi-mag.com/air-traffic-management-a-cybersecurity-challenge/.
- Hoffman, F.G. (2018) "Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges", *Prism*, Vol.7, no.4, pp. 30-47. cc.o.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf?ver=2018-12-04-161237-307
- Jensen, B. (2019). "Welcome to Fight Club: Wargaming the Future", warontherocks.com, 4 January, [online], warontherocks.com/2019/01/welcome-to-fight-club-wargaming-the-future/.
- Jones, M.A. and Diaz de Leon J. (2020). "Multi-Domain Operations", *Three Swords Magazine*, November, p.38-41. jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf.
- Kodalle T, Ormrod, D., Sample, C., and Scott, K. (2020). "A General Theory of Influence in a DIME/PMESII/ASCOP/IRC2 Model", *Journal of Information Warfare*, Vol. 19, Issue 2, Spring, [online], <https://www.jinfowar.com/journal/volume-19-issue-2/general-theory-influence-dimepmesiiascopirc2-model>.
- Lind, W.S., Nightengale, K., Schmitt, J.F., Sutton, J.W., and Wilson, G.J. (1989). *The Changing Face of War: Into the Fourth Generation*, *Marine Corps Gazette*, October 1989, pp. 22-26.
- Lockheed Martin. (2019). "Learning through Wargaming: Helping Define the Roadmap for Multi-Domain Operations", Defense News, 13 September, [online], www.defensenews.com/native/lockheed-martin/2019/09/13/learning-through-wargaming-helping-define-the-roadmap-for-multi-domain-operations/.
- Lucas, E. (2019). "The West slumbers as its enemies run amok", *Standpoint*, 18 September, [online], standpointmag.co.uk/the-west-slumbers-as-its-enemies-run-amok/.
- Luke, B. (2012). *Recognizing And Adapting To Unrestricted Warfare Practices By China*. Graduate thesis, US Air War College, Montgomery, Al.
- McCoy, K. (2018). "Competition, Conflict, And Mental Models Of War: What You Need To Know About Multi-Domain Battle", *Modern War Institute*, 26 January, [online], mwi.usma.edu/competition-conflict-mental-models-war-need-know-multi-domain-battle/.
- Ministry of Defence. (2020) *Joint Concept Note 1/20: Multi-Domain Integration*, Development, Concepts and Doctrine Centre, Shrivenham.
- Morris, L. J., Mazarr, M.J., Hornung, J. W., Pezard, S., Binnendijk, A., and Kepe, M. (2019) *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, RAND, Santa Monica, CA.
- Ormrod, D., Scott, K., Scheinman, L., Kodalle, T. Sample, C. Turnbull, B., and Ormrod, A. (2019) "The Persuasion Game: Serious Gaming Information Warfare and Influence". *Journal of Information Warfare*, Vol. 19, Issue 2, Spring, [online], www.jinfowar.com/journal/volume-19-issue-2/persuasion-game-serious-gaming-information-warfare-influence.
- Perkins, D.G. (2017) "Multi-Domain Battle The Advent of Twenty-First Century War", *Military Review*, November-December, [online], www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/Multi-Domain-Battle-The-Advent-of-Twenty-First-Century-War/.
- Qiao, L., and Wang, X. (2020) *Unrestricted Warfare: China's Master Plan To Destroy America*, Shadow Lawn Press, Lambertville. [Kindle Edition].
- Raine, J. (2019) "War or peace? Understanding the grey zone", *IIIS.org*, April 3, [online], www.iiis.org/blogs/analysis/2019/04/understanding-the-grey-zone.
- Reynolds, L. (2019) "ASPI International Conference: War in 2025", *Australian Government Department of Defence Ministers*, June 13, [online], <https://www.minister.defence.gov.au/minister/lreynolds/speeches/aspi-international-conference-war-2025>.
- Rivera, J. (2014). "Understanding and Countering Nation-State Use of Protracted Unconventional Warfare", *Small Wars Journal*, 25 October, [online], smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare.
- Schuety, C., and Hill, L. (2018). "An Air Force 'Way Of Swarm': Using Wargaming And Artificial Intelligence To Train Drones", warontherocks.com, 21 September, [online], warontherocks.com/2018/09/an-air-force-way-of-swarm-using-wargaming-and-artificial-intelligence-to-train-drones.
- Shaw, W.T. (2004) SCADA System Vulnerabilities to Cyber Attack, *EE Online*, September/October, [online], electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm.
- Stone, J. (2013) "Cyber War Will Take Place!", *The Journal of Strategic Studies*, Vol. 36, No. 1. pp. 101-108.
- Tamimi, A., Hahn, A., and Roy, S. (2020) "Cyber Threat Impact Analysis to Air Traffic Flows Through Dynamic Queue Networks", *ACM Transactions on Cyber-Physical Systems*, Vol. 4, Issue 3 (May), pp. 1-22.
- TRADOC. (2017) *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040*, U.S. Army Training and Doctrine Command (TRADOC), Fort Eustis, VA.
- TRADOC. (2021) *The U.S. Army in Multi-Domain Operations 2028*, U.S. Army Training and Doctrine Command (TRADOC), Fort Eustis, VA.

- Trend Micro. (2019) "One Flaw too Many: Vulnerabilities in SCADA Systems", *Trend Micro*, 16 December, [online], www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems.
- Tzu, Sun, tr. Lionel Giles. (2000) *The Art of War*, Allendale Online, Leicester.
- Woodford, S. (2019a). "Wargaming Multi-Domain Battle: The Base Of Sand Problem", *Mystics and Statistics*, 11 January, [online], www.dupuyinstitute.org/blog/2019/01/11/wargaming-multi-domain-battle-the-base-of-sand-problem/.
- Woodford, S. (2019b). "What Multi-Domain Operations Wargames Are You Playing? [Updated]", *Mystics and Statistics*, 25 January, [online], www.dupuyinstitute.org/blog/2019/01/25/what-multi-domain-operations-wargames-are-you-playing/.
- Yadav, G. and Paul, K. (2019), "Assessment of SCADA System Vulnerabilities", *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1737-1744.
- Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Random House, New York.