Information Warfare and the Connected Battlefield

Dr. Brett van Niekerk

Associate Professor, University of KwaZulu-Natal

Introduction

The Fourth Industrial Revolution (4IR) extends the information revolution (Third Industrial Revolution) with increasing degrees of integration amongst cyber, physical and biological systems. The 4IR is predicted to impact on all sectors, including the nature of conflict (Schwab, 2016). Key concepts that form part of 4IR include (but are not limited to):

- Data science and big data analytics, often driven and/or automated by artificial intelligence and machine learning;
- Cloud computing, providing remotely accessible computing resources;
- Internet of Things (IoT), where hyper-connected devices can act as sensors and actuators to produce large amounts of information and cyber-physical interconnections;
- Augmented reality, overlaying information on glasses, map, or image;
- Cyber-security, due to vulnerabilities introduced by connecting insecure 'non-traditional' devices onto networks.

Some of the 4IR concepts have been present in the military setting in some form, such as augmented reality similar to head up displays, and the IoT concept evolves network centric warfare (or as Wassel (2018) calls it, 'data warfare') into what has become known as the 'Internet of Battlefield Things' (IoBT) or the 'Internet of Military Things' (IoMT) (Castiglione, Choo, Nappi, and Ricciardi, 2017). IoT implementations in the military have the potential to support command and control (C2) of Multi-Domain Operations (MDO) in a range of areas (Seffers, 2017). As such, MDO in the future can be considered to include a hyper-connected battlefield which results in an increased attack surface for information warfare (IW) (Cenciotti, 2017; van Niekerk, Pretorius, Ramluckan and Patrick, 2018). This paper will consider IW in the context of both MDO and the IoBT.

Multi-domain Operations and Information Warfare

The traditional 'physical' domains of military operations include land, sea, air, and space; however, there is increasing need to dominate in the electromagnetic spectrum (EMS), cyber, and the broader information environment (Ween, Dortmans, Thakur, and Rowe, 2019). The MDO approach has been described as a "joint warfighting concept that will bring to bear all of the firepower, both kinetic and non-kinetic" to provide superiority across the battlespace in an unprecedented way (South, 2019).

Figure 1 illustrates multiple operational domains: the four 'physical' domains are illustrated in the centre of the figure; these domains usually are mobile and communicate through broadcast mediums at various frequencies (the EMS). Cyberspace becomes an extension of this, providing the data and information transfer mechanisms, such as networking protocols. Whilst the contemporary information domain is considered almost identical to cyberspace, the information environment is broader and includes printed and cognitive information as well. These all support the human element, which encompasses strategic and tactical decision-making processes (for example, command and control) for the warfighters and commanders but extend more widely to society, the economy, and politics.

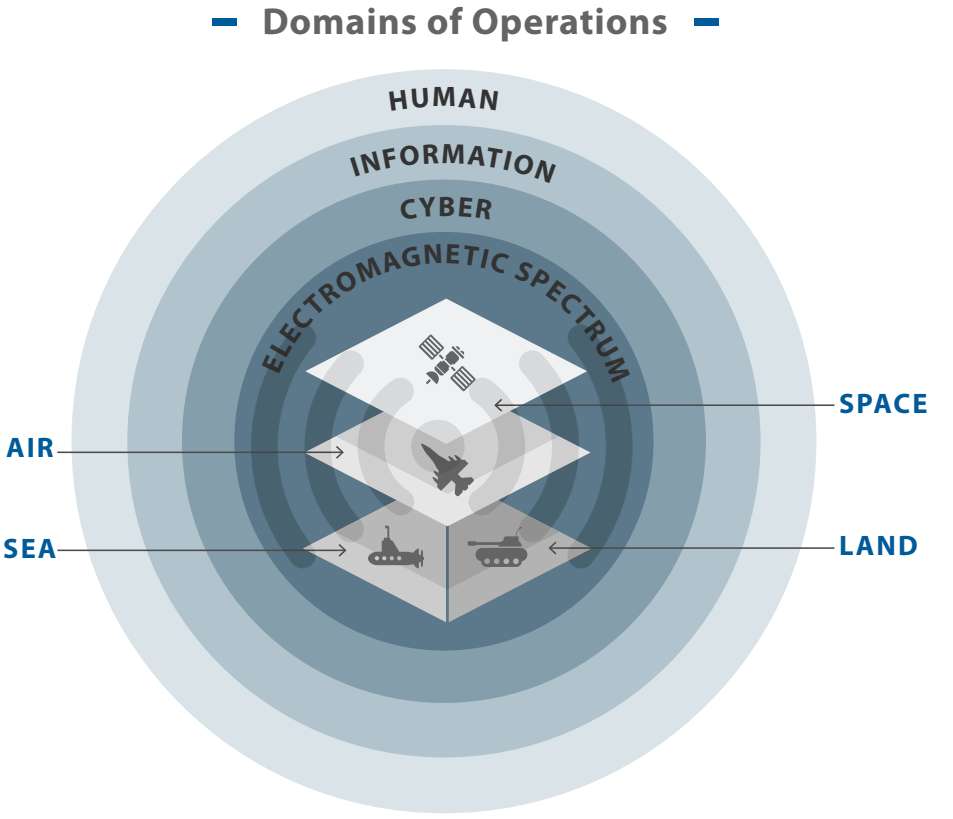

Figure 1: *Domains of Operations*

Information warfare, in its earlier form, comprised operations that could affect and/or protect information across the physical, virtual and cognitive domains (Brazzoli, 2007; Waltz, 1998). These 'pillars' of IW included electronic warfare (EW), cyber-operations, psychological operations (PSYOP), intelligence, network centric warfare or information infrastructure warfare, and command and control warfare (C2W) (Brazzoli, 2007).

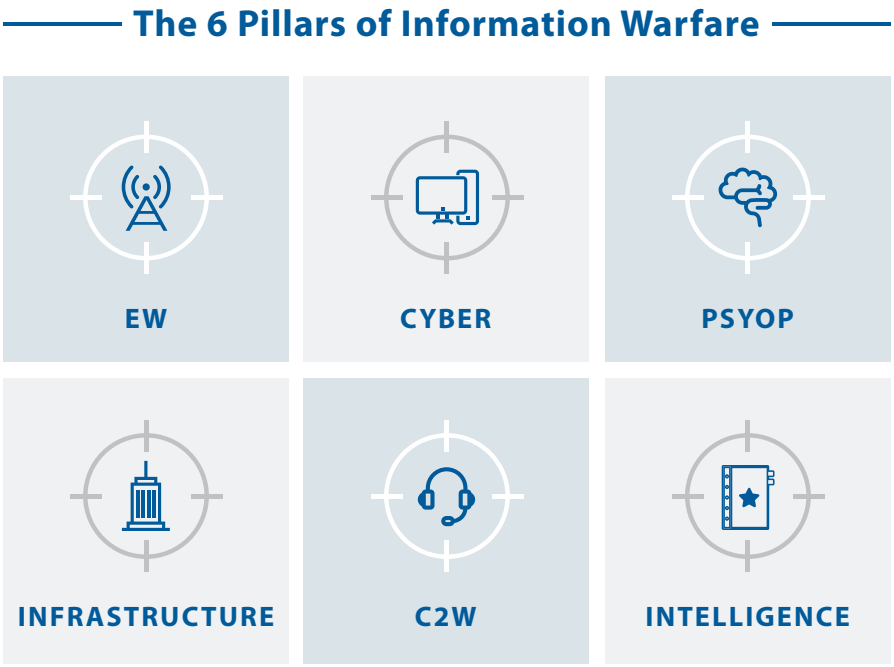

Figure 2: *'Pillars' of Information Warfare*

Modern use of the term 'information warfare' tends to refer more to the cognitive aspects, such as disinformation and influence campaigns, often driven by social media and instant messaging (Stengel, 2019). Emerging discussions focus on the 'convergence' of EW and cyber in what is known as cyber electromagnetic activities (CEMA) (UK Ministry of Defence, 2018; US Department of the Army, 2014). However, a greater convergence of IW pillars can be argued particularly given the apparent success of coordinated information and physical operations in Ukraine, despite not providing a 'decisive' victory (Valeriano, Jensen, and Maness, 2008; van Niekerk, 2015).

Offensive IW typically has one of the "'5 Ds": deny, degrade, disrupt, deceive, or destroy' (Sterling, 2019) as a strategic or operational objective; however, others have also proposed objectives such as:

- Disrupt, deny, destroy, manipulate, and steal (Hutchinson and Warren, 2001);
- Degrade, deny, corrupt, and exploit (Borden, 1999; Kopp, 2000);
- Interrupt, modify, fabricate, and intercept (Pfleeger and Pfleeger, 2003).

Ultimately human decision making is targeted at tactical, operational and strategic levels; however, conflict through cyberspace and the information environment is increasingly targeting societal, political and economic decision making as well as military operations or operators. With the growing focus on disinformation and influence campaigns by state and non-state actors, particularly through online 'news' websites and social media, the more objectives of IW at the higher strategic level have been rephrased to the 4 Ds: dismiss, distort, distract, and dismay (White, 2016). Such types of operations target the 'will' of a population or politicians and, combined with the more operationally focused elements of IW in a given battlespace, aim to reduce or remove popular or political support towards a conflict or its military objectives.

IoBT and Information Warfare

Castiglione, Choo, Nappi, and Ricciardi (2017: 16) indicate that the battlefield has seen "an increasing number of ubiquitous sensing and computing devices worn by military personnel and embedded within military equipment". It was reported that NATO was investigating the potential benefits of IoT to the military in areas such as situational awareness, surveillance, logistics, medical applications, base operations and energy management (Seffers, 2017; Stone, 2018; Wassel, 2018). IoBT/IoMT also has a vast potential to support C2 in MDO through "combined operations logistics support; tactical-level situational awareness; targeting; monitoring of vehicle and soldier status; battlefield medical care and even environmental monitoring" (Seffers, 2017).

Ren and Hou (2018) propose a "Combat Cloud-Fog" architecture with three tiers. A 'combat resource' tier includes the military equipment such as platforms and sensors in the traditional four physical domains. Cenciotti (2017) uses the ex-

ample of an F-35 aircraft that has sensors to collect information about its environments and potential threats; it also has internal sensors to monitor its performance and therefore can be seen as both a 'thing' on the Internet, but also as a group of sensors. Valeriano, Jensen, and Maness (2008) consider the F-35 equivalent to a computer server. This indicates the growing complexity of modern military systems, the reliance of digital information, and the amount of data that can be generated (relating to concepts associated with 'big data').

The second tier of Ren and Hou's (2018) architecture includes a 'fog layer', for localised distributed computing and storage. The third layer then comprises of cloud computing, with greater storage and comprising of multiple 'fog network' links. The fog network can be thought of serving the tactical and operational levels of C2, whereas the cloud network serves the operational and strategic levels of C2. Given the scope of MDO, it is wise to extend the sensors of the "Combat Cloud-Fog" architecture to include sensors in the EM domain as part of the combat resource set.

> *The potential for the algorithms to be 'tricked' is of particular concern to those needing to make command decisions based on analysed data being presented to them: can the information about the battlespace be trusted? At a far more tactical level, can a pilot or control station on a warship trust the information being displayed? Any hesitancy or incorrect decision is ultimately the objective of information warfare.*

Monitoring also needs to be provided in the cyber domain throughout the Combat Cloud architecture to aid in cyber-security. There have been recorded incidents of 'connected' military units and/or equipment being affected by cyber-incidents: in 2009 was reported that malware had affected warships and a military airfield (Page, 2009; Willsher, 2009), mobile malware was used to track artillery units (Volz, 2016) and there are now growing concerns over cyber and electromagnetic threats to satellites and space-based systems (Garner, 2020; Rajagopalan, 2019). Compromised IoT devices have been used to launch distribut-

ed denial-of-service (DDoS) cyber-attacks were some of the largest recorded at the time they occurred (Fruhlinger, 2018).

Such incidents and wider concerns related to information systems and security point to the inherent risk of highly interconnected systems. Van Niekerk, Pretorius, Ramluckan, and Patrick (2018) illustrate how information warfare can be used to target IoT and humans through vulnerable IoT. Numerous such theoretical attacks can be applied to military scenarios, such as:

- Wiper malware or ransomware that destroys data and system software can create catastrophic effects for aircrafts or submerged submarines, for example;
- Injecting PSYOP messages to heads-up-displays of pilots can distract and dismay the pilot by suggesting the aircraft systems are compromised and adversely impact time-critical decision-making;
- Cyber-attacks manipulating sensor arrays (for example, sonar array or air defence radar) randomly to provide false targets and hide actual targets, thereby distorting the view of the battlespace;
- Using malware and social media on the phones of military personnel to determine deployments and thereby generate intelligence relating to operations.

Table 1 illustrates possible 'generic' IW threats relevant to the cloud-fog IoBT architecture.

Table 1: *IW threats to the IoBT*

Cloud-Fog Architecture	Domain	IW threats
Tier 3: cloud	Physical	Destruction of cloud network infrastructure
	Cyber	DDoS to overload the cloud network
		Network intrusion to steal information
		Network intrusion to manipulate information
		Network intrusion to destroy information

Cloud-Fog Architecture	Domain	IW threats
Tier 2: fog network	Physical	Destruction of fog network infrastructure
	Electromagnetic	Jamming of wireless receivers to the fog network
	Cyber	DDoS to overload the fog network
		Network intrusion to steal information
		Network intrusion to manipulate information
		Network intrusion to destroy information
Tier 1: combat resource	Physical	Destruction of sensors / equipment
	Electromagnetic	Jamming of wireless links amongst devices
		Directed energy to destroy electronic devices
	Cyber	Malware on devices to track units
		Malware to degrade equipment performance
		System intrusion to manipulate sensor information
	Cognitive	PSYOP messages transmitted to devices

In general, the IoBT may result in a congested EM spectrum and network due to the increasing number of EM signals and the quantity of data being transferred. This in turn may increase the susceptibility to EW and DDoS attacks as each signal could present itself as 'noise' to each other, and jamming will increase this 'noise' level to degrade or disrupt the effectiveness of the communication links. In a similar manner, the closer to the 'threshold' of a network the data quantity is, the more susceptible it will be to being flooded and overwhelmed by malicious traffic.

> ***The fog network can be thought of serving the tactical and operational levels of C2, whereas the cloud network serves the operational and strategic levels of C2. Given the scope of MDO, it is wise to extend the sensors of the "Combat Cloud-Fog" architecture to include sensors in the EM domain as part of the combat resource set.***

IoBT will possibly contribute to the 'convergence' of cyber, EW, and PSYOP at the tactical level; van Niekerk, Pretorius, Ramluckan and Patrick (2018) discuss some

aspects of this convergence in a general context. Above the possibility of cyber being used to inject a PSYOP message to target pilots is mentioned; similarly EW could be used to 'overpower' radio communications to transmit PSYOP messages to personnel. This convergence can be thought of as a layered model of IW: EW targets the physical layer of the network, cyber targets the higher layers and protocols, and a payload option for the cyber component is the distribution of PSYOP messages.

Another aspect to consider are the algorithms that are implemented for data analysis and for the functioning of military equipment. Due to the quantity of data produced by modern equipment, it is impossible for humans to analyze all of it and a degree of automation is needed, usually implemented with Artificial Intelligence (AI). However, there have been instances illustrating that modified inputs have resulted in AI providing an incorrect classification (Field, 2017; Lemos, 2021). Often new technologies are implemented without taking security into account, and it is no different with AI. In the academic space, there is a sharp increase in the amount of research investigating attacks on AI systems including adversarial attacks to induce incorrect outputs, as well as data poisoning (also known as model poisoning) which corrupts the training data to produce a flawed model (Constantin, 2021; Lemos, 2021). The potential for the algorithms to be 'tricked' is of particular concern to those needing to make command decisions based on analysed data being presented to them: can the information about the battlespace be trusted? At a far more tactical level, can a pilot or control station on a warship trust the information being displayed? Any hesitancy or incorrect decision is ultimately the objective of information warfare.

Conclusion

Multi-domain operations encompass all physical environments and can extend into the electromagnetic and cyber domains as well. The Internet of Battlefield Things provides a mechanism to achieve multi-domain operations through embedded sensors providing a common picture of the operating environment(s). However, IoT in general has been seen to be vulnerable to compromise, and

a hyper-connected battlespace could increase the attack surface for information warfare across the physical, electromagnetic, cyber and cognitive domains. Attacks could target the physical infrastructure, the signals, network protocols, algorithms, data, and the human psychology.

References:

Borden, A. (1999). What is Information Warfare? *Air & Space Power Journal*, November 2. Available from: *http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html [*2 July 2009].

Brazzoli, M. S. (2007). Future Prospects of Information Warfare and Particularly Psychological Operations. In L. le Roux, *South African Army Vision 2020* (pp. 217-232). Pretoria: Institute for Security Studies.

Cenciotti, D. (2017). Cybersecurity In The Sky: Internet of Things Capabilities Making Aircraft More Exposed To Cyber Threats Than Ever Before, The Aviationist, 20 June. Available from *https://theaviationist.com/2017/06/20/cybersecurity-in-the-sky-internet-of-things-capabilities-to-make-aircraft-more-exposed-to-cyber-threats-than-ever-before/ [*26 September 2021].

Constantin, L. (2021). How data poisoning attacks corrupt machine learning models, *CSO Online*, 12 April. Available from *https://www.csoonline.com/article/3613932/how-data-poisoning-attacks-corrupt-machine-learning-models.html* [5 October 2021].

Field, M. (2017). Graffiti on stop signs could trick driverless cars into driving dangerously, *The Telegraph*, 7 August. Available from *https://www.telegraph.co.uk/technology/2017/08/07/graffiti-road-signs-could-trick-driverless-cars-driving-dangerously/* [5 October 2021].

Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, CSO Online, 9 March. Available from *https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html* [29 September 2021].

Garner, T. (2020). Why Satellite Cybersecurity Must Be Prioritized in the New Frontier, *NextGov*, 1 May. Available from *https://www.nextgov.com/ideas/2020/05/*

why-satellite-cybersecurity-must-be-prioritized-new-frontier/164977/ [10 September 2021].

Hutchinson, W., and Warren, M. (2001). *Information Warfare: Corporate Attack and Defense in a Digital World*. Oxford & Auckland: Butterworth Heinemann.

Kopp, C. (2000). A Fundamental Paradigm of Infowar, *Systems: Enterprise Computing Monthly*, Sydney:Auscom Publishing, 46-55.

Lemos, R. (2021). Expect an Increase in Attacks on AI Systems, *Dark Reading*, 27 April. Available from *https://www.darkreading.com/vulnerabilities---threats/advanced-threats/expect-an-increase-in-attacks-on-ai-systems/d/d-id/1340833* [5 October 2021].

Page, L. (2009). MoD networks still malware-plagued after two weeks, *The Register*, 20 January. Available from *https://www.theregister.com/2009/01/20/mod_malware_still_going_strong/* [10 September 2021].

Pfleeger, P., and Pfleeger, S. (2003). *Security in Computing*, 3rd Edition. Upper Saddle River, New Jersey: Prentice Hall.

Rajagopalan, R.P. (2019). Electronic and Cyber Warfare in Outer Space, The United Nations Institute for Disarmament Research. Available from *https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf* [10 September 2021].

Schwab, K. (2016). The Fourth Industrial Revolution: what it means, how to respond, World Economic Forum, 14 January. Available from *https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/* [25 September 2021].

Seffers, G. I. (2017). NATO Studying Military IoT Applications, *Signal*, 1 March. Available from *https://www.afcea.org/content/Article-nato-studying-military-iot-applications* [25 September 2021].

South, T. (2019). This 3-star Army general explains what multi-domain operations mean for you, Army Time, 11 August. Available from *https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/* [25 September 2021].

Stengel, R. (2019). *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do about It*. London: Atlantic Books.

Sterling, B. (2019). Deny, degrade, disrupt, deceive, or destroy, Wired, 4 May. Available from *https://www.wired.com/beyond-the-beyond/2019/04/deny-degrade-disrupt-deceive-destroy/* [24 September 2021].

Stone, A. (2018). The answer to battlefield logistics problems could be IoT, C4ISRnet, 12 October. Available from *https://www.c4isrnet.com/it-networks/2018/10/12/the-answer-to-battlefield-logistics-problems-could-be-iot/* [25 September 2021].

UK Ministry of Defence. (2018). Cyber and Electromagnetic Activities, Joint Doctrine Note 1/18. Available from *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf* [24 September 2021].

US Department of the Army. (2014). Cyber Electromagnetic Activities, FM3-38. Available from *https://irp.fas.org/doddir/army/fm3-38.pdf* [24 September 2021].

Valeriano, B., Jensen, B., and Maness, R. C., (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

van Niekerk, B. (2015). "Information Warfare in the 2013-2014 Ukraine Crisis", in: Richet, J. (ed.), Cybersecurity Policies and Strategies for Cyberwarfare Prevention. Hershey, PA: IGI Global, pp. 307-339.

van Niekerk, B., Pretorius, B., Ramluckan, T., and Patrick, H. (2018). "The Impact of IoT on Information Warfare", in: Fields, Z. (ed.), *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, Hershey, PA:IGI, pp. 141-164.

Volz, D. (2016). Russian hackers tracked Ukrainian artillery units using Android implant: report, Reuters, 22 December. Available from *https://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU* [29 September 2021].

Waltz, E. (1998). *Information Warfare: Principles and Operations*. Boston & London: Artech House.

Wassel, P. (2018). 3 Military Applications of The Internet of Things, Augmate, 27 April. Available from *https://www.augmate.io/3-military-applications-of-the-internet-of-things/* [25 September 2021].

Ween, A., Dortmans, P., Thakur, N., and Rowe, C. (2019). Framing cyber warfare: an analyst's perspective, *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 16(3), 335–345.

White, J. (2016). Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation, Policy Brief 2017/13, Institute for European Studies. Available from *https://www.ies.be/node/3689* [25 September 2021].

Willsher, K. (2009). French fighter planes grounded by computer virus, *The Telegraph*, 7 February. Available from *http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html* [26 September 2021].

Dr. Brett van Niekerk is a Senior Lecturer at the University of KwaZulu-Natal, and serves as chair for the International Federation of Information Processing Working Group on ICT in Peace and War, and the co-Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has numerous years of information security and cyber security experience in both academia and industry, and has contributed to the ISO/IEC information security standards and international working groups. He has over 70 publications and presentations to his name. In 2012 he graduated with his PhD focusing on information operations and critical infrastructure protection. He is also holds a MSC in electronic engineering and is CISM certified.