On Information Warfare: A Response to Taddeo

Tim Stevens

Accepted for publication in *Philosophy & Technology* 26(2): 221-5.

Keywords: information technologies; information warfare; dominion; war.

Mariarosario Taddeo's recent article, 'Information Warfare: A Philosophical Perspective' (2012) is a welcome addition to the literature on information communications technologies (ICTs) and warfare, originating as it does from beyond the epistemological walls of the communities of security practitioners and security academics who ordinarily dominate debate on the informational ways and means deployed in the pursuit of strategic political ends.[1] She is correct to assert the shift of warfare 'toward the non-physical domain', such that 'the boundaries of reality stretch to include non-physical objects, actions and interactions as well as physical ones', and interrogates the ethical implications of the 'new modes of warfare […] being developed specifically for deployment in such a new environment' (*ibid.*, p. 111). In this short response, I wish to draw attention to two issues arising from the article. The first concerns the applicability of 'information warfare' terminology to current military and political discourse, on account of its relative lack of use in the contemporary context. The second is a short examination of the political and ethical implications of treating ICT environments as a 'domain', with its obvious ramifications for the pursuit of 'dominion', particularly through military action.

Terminological issues

As Taddeo notes, information warfare (IW) is not a single form of warfare but rather an umbrella term within whose semantic folds we may discern several distinct forms of warfare. In

[1] Notable exceptions include Gray (1997), Der Derian (2009).

the mid-1990s, Libicki (1995) distinguished seven modes of IW, including electronic warfare (EW), psychological warfare, economic information warfare and cyberwarfare. However, it is also important to recognise that the term itself has fallen out of use by governments and militaries in recent years. The propaganda elements of the concept have been incorporated into 'information operations' (IO) and 'influence', and the more technical and operational aspects into the doctrines of network-centric warfare (NCW) and network-enabled warfare (NEW), amongst many others, including the important category of computer network operations (CNO). Even whilst it had greater currency, IW was a problematic concept whose practical implementation often fell far short of its theoretical attractiveness, not least because non-conventional forces such as insurgents benefited from IW as much as regular forces (Betz, 2006).

One of the principal reasons IW terminology diversified to the point of the near-extinction of the original term is that the information-technological landscape has over the last few decades become several orders of magnitude more complex than its original proponents can ever have imagined. Information warfare emerged, as Taddeo notes, in the context of a putative revolution in military affairs (RMA), which spread from the Soviet Union in the 1970s and 1980s. Since that time, the multiplying uses—and abuses—of ICTs have necessitated the repeated redrafting of military doctrine and the devising of numerous typologies of ICT-contingent operations that have all but nullified IW as a discrete concept.

Writing a decade after his original comments on IW, Libicki (2007, p. 19) noted that the 'official abandonment' of the term—by the US Department of Defense, at least—provided an opportunity to return to it 'a greater clarity'. To this end, he proposed a definition of IW as 'the use of information to attack information', in which, 'as the purpose of information is to make better decisions, the purpose of information warfare must therefore be to confound the making of these decisions, including those made by machines' (*ibid.*, p. 20). This definition continues to

inform thinking on the various forms of warfare sometimes assigned to the overarching rubric of IW and is important for distinguishing what might be IW and what is not. Although it is not universally accepted—partly because IW no longer figures prominently in Western military doctrine—it provides a useful contrast to the definition of IW suggested by Taddeo (2012, p. 114):

> …. the use of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances.

This definition is motivated by the salient observation that warfare has shifted towards the 'non-physical domain' and usefully incorporates physical and non-physical agents and targets into what we might otherwise term a sociomaterial assemblage of humans and non-humans (*sensu* DeLanda, 2006). It also clarifies that enemy 'resources' are not confined to the physical domain alone, and may be of cognitive or other informational character.

However, it makes it rather less straightforward to determine what is covered by this definition of IW and what is not. Of particular note is the inclusion of battlefield 'drones and semi-autonomous robots' which, while undoubtedly dependent upon ICTs, would not normally be considered agents of IW. One might argue that they are indeed IW agents but this can only apply in some secondary and attenuated sense of being used to disrupt the cognitive resource of a target population. Even then, this effect is more readily understood as part of an 'influence' or propaganda operation. My feeling is that Taddeo's definition is a useful one—if one wishes to persist with use of the IW term—but suffers more from a few problematic exemplars than from

any serious inherent weakness. However, if one is attempting to engage with governments and militaries on ethical matters pertaining to IW, it may be necessary to revisit the inclusivity of this definition of IW, or to develop a more nuanced and possibly more developed suite of terms that can be addressed individually without fear of confusing one's interlocutors.

Domain and dominion

This possible terminological over-reach has an interesting parallel in contemporary political discourse. Although Taddeo explicitly—and quite correctly within the constraints of an article—restricts her comments to 'ICTs-based warfare', rather than straying into related issues such as 'information crime, terrorism or activism', governments have not been so restrained in their formulations of 'cyber security'. This form of security has come to cover almost anything done by anyone involving a networked computer, and encompasses not only cyber warfare, cyber espionage, critical information infrastructure protection, and cyber terrorism, but also intellectual property protection, cyber crime, child online safety, e-government, and many other problems and practices besides. Although in time—like IW—we will probably see a diversification of terms and policies under that broad umbrella, the current formulation of cyber security betrays a totalising perspective on what most states are calling 'cyberspace', even as many scholars reject that term for its analytical inexactitude. In this totalising view, 'cyberspace' is a monolithic concept at odds with its evident empirical complexity. In its current articulation as a fifth 'domain' alongside land, sea, air and space, this linguistic conceit allows for the presentation of cyberspace as something over which to exert dominion, as a geostrategic environment in which the exercise and pursuit of power and influence must be normalised as part of global geopolitics (Betz & Stevens, 2011).

It is for this reason that the information environment enabled by the Internet and other ICTs has become so important to national security. It is not only here that specific national security issues arise—as in IW—but also where all other national security objectives may be pursued. Indeed, it may be that ICTs are 'the common underlying factor upon which all security sectors are destined to converge' (Yould, 2003, p. 78). My concern is that if we view IW as a monolithic concept glossing myriad complexity we may also fall prey to this totalising vision of a 'domain' over which control must be exerted. It may just be that the 'shock of the new' facilitates such interpretations. Wertheim (1999, p. 221) argues that 'the ontology of cyberspace is ex nihilo …. a new space that simply did not exist before', and also describes it as a domain. For governments, the novelty of this domain is such that the hoary old security syllogism—beginning, 'something must be done…'—reverberates throughout political discourse.

If, as many have argued, one of the characteristics of ICTs is that global communications have been accelerated to near-instantaneity, we should be cautious, as Virilio (2008, p. 42) suggests, of the thesis that 'the liberation of speed, the freedom of speed, seems to be the fulfilment of all freedoms'. This freedom of global movement has been the dream of technologically-advanced militaries for decades and the 'new domain' of cyberspace would seem to offer them an increasingly attractive environment in which to tackle adversaries both state and non-state, wherever they happen to be. This perspective might also account for the libertarian visions of early cyberspace 'pioneers' for whom this environment really was new and potentially liberating (quintessentially, Barlow, 2001). The intervening years have shown this dream to be illusory, or at least dangerously seductive, as MacKinnon (2012) has set out in her study of the increased imposition of governmental and commercial controls on political and personal expression on the Internet. So too for governments, for whom 'cyber' capabilities frequently encounter significant defensive capabilities, catalyse unintended consequences, and fail to deliver information superiority. Nowhere is this more clearly seen than in the failure of Western militaries informed

by RMA thinking to deliver swift and decisive victories in Iraq and Afghanistan (Dalby, 2009). However, this has not prevented a rapid militarisation of global ICT environments, a process led by the West (Deibert & Rohozinski, 2010, p. 6). As Taddeo cogently argues, there is a lack of an ethical framework to deal with such actions, let alone any consensus on which legal regimes apply to those activities we might call information warfare. Little wonder that one of the key components of 'cyber' foreign policy is to develop norms of appropriate military behaviour in this environment (Stevens, 2012).

Taddeo's work helps to inform these discussions, particularly in its concern with the applicability of just war theory. I have not engaged here with her claim that just war theory needs to re-examine the assumptions of what constitutes war in order to include the 'peculiarities' of IW scenarios (Taddeo, 2012, p. 118). If this is the case—and I make no claim to the contrary-we would do well to ensure that our concepts of IW remain relevant to contemporary discourses of ICTs and war if we hope to engage with political and military actors in the development of an ethical framework for IW. It is my hope that the present contribution has served to further this project in some small way.

Acknowledgements

The author acknowledges the support of an Economic & Social Research Council scholarship (ES/H022678/1), funded under the Research Councils UK 'Global Uncertainties' programme. Thanks also to Mariarosaria Taddeo.

References

Barlow, J.P. (2001). A declaration of the independence of cyberspace. In P. Ludlow (Ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp. 27-30). Cambridge, MA: The MIT Press.

Betz, D.J. (2006). The more you know, the less you understand: The problem with information warfare. *Journal of Strategic Studies*, *29*(3), 505-533.

Betz, D.J. & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge.

Dalby, S. (2009). Geopolitics, the revolution in military affairs and the Bush doctrine. *International Politics*, *46*(2/3), 234-252.

DeLanda, M. (2006). *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London: Continuum.

Deibert, R. J. & Rohozinski, R. (2010). Beyond denial: Introducing next-generation information access controls. In R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, pp. 3-13. Cambridge, MA: The MIT Press.

Der Derian, J. (2009). *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. New York: Routledge.

Gray, C.H. (1997). *Postmodern War: The New Politics of Conflict*. London: Routledge.

Libicki, M.C. (1995). *What Is Information Warfare?* Washington, DC: National Defense University.

Libicki, M.C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy*, *33*(1), 148-170.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology*, *25*(1), 105-120.

Virilio, P. (2008). *Negative Horizon*. London: Continuum.

Wertheim, M. (1997). *The Pearly Gates of Cyberspace: A History of Cyberspace from Dante to the Internet*. London: Virago.

Yould, R.E.D. (2003). Beyond the American fortress: Understanding homeland security in the information age. In R. Latham (Ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, pp. 74-98. New York: The New Press.