ABSTRACT:

Destabilizing Terrorist Networks: Disrupting and Manipulating Information Flows in the Global War on Terrorism

K. A. Taipale *

Prelude.

"Information warfare is about the exercise of power on the information front. ... It is about using information to influence others in ways that serve your mission." – Dorothy Denning [1]

"All that we have to do is to send two Mujahedin to the farthest point East to raise a piece of cloth on which is written al-Qa'ida in order to make the generals race there to cause America to suffer human economic and political losses without their achieving for it anything of note … ." – Osama bin Laden, October 2004. [2]

Introduction.

It is said that information, or perhaps more appropriately, knowledge, is power. [3] But information or knowledge in the abstract is not power. Rather, the power attributed to information arises from its usefulness (or uselessness) for decision-making in the context of

---

* *Kim Taipale, BA, JD (New York University) MA, EdM, LLM (Columbia University)* is the executive director of the Center for Advanced Studies in Science and Technology Policy and a senior fellow at the World Policy Institute where he directs the *Program on Law Enforcement and National Security in the Information Age* and the *Global Information Society Project.*

1 Dorothy Denning, *Power Over the Information Front*, Conference Paper, Global Flow of Information, Yale Information Society Project (2005) (describing the *information front* and presenting a taxonomy based on breaking the information environment down into three areas: information, channels, and actors.)

2 Translated transcript, provided by the U.S. government, of Osama bin Laden's videotaped message released and aired on the al-Jazeera satellite television network during the weekend before the US presidential elections, as reported in WASH. POST (Nov. 1, 2004) *available at* http://www.washingtonpost.com/wp-dyn/articles/A16990-2004Nov1.html. The release of this statement is itself an example of the "perception management" genre of information warfare and the actions described in the quote are an example of the use of the "misdirection" genre.

3 *Scientia est Potentia*, Latin for *knowledge is power* is often the motto used by military and government intelligence agencies (*see* http://en.wikipedia.org/wiki/Scientia_potentia_est) and was the original motto of DARPA's Information Awareness Office. It was prominently depicted on that office's early logo (discontinued in early 2003, *see* Question 14, IAO FAQ, copy available at http://information-retrieval.info/docs/IOA-logo-stmt.html).

action and relationships in the physical world – that is, *actionable* information is an *instrument* of power. [4] Understood in this way, information warfare is the *protection*, *monitoring*, *disruption*, or *manipulation* of information and information flows to improve one's own decision-making process or to degrade that of the enemy. [5] This paper examines issues relating to the disruption and manipulation of information flows in order to preempt or otherwise constrain terrorist acts in the context of the 'war on terrorism'. [6] It is beyond the scope of this paper to address protection or monitoring of information flows. [7]

---

[4] *Cf.* JAMES DER DERIAN, VIRTUOUS WAR 212 (2001) (Der Derian postulates a theory of the virtual in which he argues in part that virtuality need not be realized, only actualized (citing Deleuze), in order to become self-fulfilling, that is, to create or shape reality). Implicit then it seems, is that once actualized the virtual is essentially the real. For practical purposes, the simulacrum is a reality once it is the basis for decision-making (and results in physical world outcomes) since it is no longer subject to invalidation (cannot be "undone" as the rationale for a decision) even through subsequent falsification or other truth testing (e.g., WMD and Iraq). The power of the virtual then, is in its capacity for self-realization. Likewise, the power of information is in its use to shape perception and influence decision-making leading to physical world consequences. Thus, knowledge in the context of actionable intelligence does not necessarily imply any truth-value to information, only utility. (This holds in other contexts as well, for example, in the "fake but accurate" school of journalism, see Maureen Balleza & Kate Zernike, *Memos on Bush Are Fake But Accurate, Typist Says*, N.Y. TIMES (Sep. 15, 2004)). Technology is truly the art of our times. However, it is beyond the scope of this paper to examine the philosophical or epistemological aspects of information warfare.

[5] That is, to improve or degrade decision-making relative to the actor's axiomatic interests.

[6] I use the phrase 'war on terrorism' throughout this article because it is the prevailing metaphor for the current conflict between organized, but generally stateless actors using asymmetric means, including politically or religiously-motivated violence, against U.S. and other global institutional interests. *But see* Terry Jones, *Why Grammar is the First Casualty of War*, LONDON DAILY TELEGRAPH (Dec. 1, 2001). ("How do you wage war on an abstract noun?") and GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY 3-6 (2003) discussing how metaphors not only affect how we communicate but actually structure our perceptions and understandings from the outset. *Cf.* Der Derian, *supra* note 4 (discussing how the virtual world projected by the military-industrial-media-entertainment complex structures, channels, and ultimately creates our perceptions of war and peace).

[7] In earlier papers I have addressed the issue of using collection, identification, data sharing, and data analysis (including data mining) technologies to *monitor* information flows for counterterrorism purposes. See, e.g. K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev. 2 (1993) [hereinafter, Taipale, *Data Mining*]; K. A. Taipale, *Technology, Security, and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd,* 7 Yale J. L. & Tech. 123; 9 Intl. J. Comm. L. & Pol'y 8 (Dec. 2004) [hereinafter, Taipale, *Frankenstein*]. Additionally, I have addressed the use of architecture to *protect* against cybercrime more generally (not in the context of counterterrorism) in K. A. Taipale, *Internet and Computer Crime: System Architecture as Crime Control,* Center for Advanced Studies Working Paper (Feb. 2003).

Overview.

Information warfare is not new, nor is recognizing the relationship between information, decision-making, and victory itself novel. Sun Tzu wrote of the supreme importance of attacking the enemy's strategy (decision-making) and the use of deception to do so, as well as the importance of spying to improve one's own decision-making capacity. [8] More recently, Colonel John Boyd famously made explicit this dimension of warfare by postulating that the key to success in conflict is to operate within the opponent's decision cycle. [9] Boyd's views have attained wide currency in US military doctrine. With the emergence of modern information societies that are almost wholly dependent on technically mediated information flows to function (and to support economic, military, and political decision-making), the US military is currently undertaking to doctrinalize defensive and offensive information warfare within the Department of Defense warfighting framework. [10]

This paper explores the need for a more comprehensive understanding of information warfare doctrine and policy in the broader context of the war on terrorism – that is, the need for an overarching analytic framework to inform the public debate; one that encompasses not just

---

[8] SUN TZU, THE ART OF WAR 41 (S. B. Griffith, *tr*., 1963, c. 500 BC) ("All warfare is based on deception").

[9] Grant T. Hammond, THE MIND OF WAR: JOHN BOYD AND AMERICAN SECURITY (2001). Note that the conceptual underpinnings for Boyd's concept of warfighting rests on three scientific principles – the second law of thermodynamics, the Heisenberg principle, and Gödel's incompleteness theorem – which together support the idea "that any inward-oriented and continued effort to improve the match-up of concept with observed reality will only increase the degree of mismatch." John R. Boyd, *Destruction and Creation*, unpublished essay at 1, (Sep. 3, 1976), cited in Hammond, *supra* at 16.

[10] *See* Dan Kuehl, *The Evolving Effort to Doctrinalize Information Warfare*, Conference Paper, Global Flow of Information, Yale Information Society Project (2005). *Cf.* Timothy L. Thomas, *Is The IW Paradigm Outdated?* 2 J. INFORMATION WARFARE 117-127 (2003). Of course, potential nation state competitors to US interests, for example, the Chinese, are also developing advanced information capabilities and doctrines. Given the US's dependence on advanced interconnected systems it seems particularly vulnerability. An article in China's People's Liberation Daily expressly recognized this dependency, "an adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the US economy." Cited by George Tenet, Testimony to the Senate Governmental Affairs Committee, Jun. 24, 1998, FEDERAL NEWS SERVICE.

military operations but includes foreign and domestic intelligence and law enforcement information operations in a cohesive and consistent manner. In particular, this paper examines the policy and legal challenges in the use of offensive information operations (including legal sanctions) to disrupt or manipulate information flows short of armed conflict, especially those actions that may impact US domestic information flows or US citizens, either directly or indirectly, or that may conflict with generally recognized democratic norms. This paper is specifically interested in identifying and understanding policy issues arising at the intersection or overlap of the converging military, intelligence, and law enforcement missions intended to prevent terrorist acts by denying, limiting, or degrading the use or usefulness of information or infrastructure for recruiting, planning, financing, inciting, or implementing such acts.

It is a fundamental premise of this paper that the traditional domains and missions of national security and law enforcement organs are converging because of challenges posed by non-state transnational security threats, in particular that of international terrorism aimed at undermining US and global economic, social, and political institutions and power structures through violent asymmetric attacks against US and allied interests and citizens both within the US and abroad. This convergence of mission – evidenced in the reactive shift in focus of the military paradigm from destruction to disruption, [11] and that of law enforcement from

[11] Note that this shift in military paradigm applies to nation-state conflict as well. It has been argued that historically manifest wars of *destruction* (i.e., "total war" among the great powers) gave way to the great war of *deterrence* (the "cold war" and related proxy skirmishes between the two superpowers), which in turn is being (will be) supplanted with wars of *disruption* shaped by international competition and IT-driven military organizations. "We are approaching a stage of development when no one is a soldier anymore but everyone is a participant in combat action. The task now is not to inflict losses in men and materiel but to thwart an enemy's plans, demoralize it, undermine its worldview, and destroy its intrinsic values." – Maj. Gen. G.A. Berezkin, Deputy Head of the Russian Federation Defense Ministry Center of Military-Technical Information Studies, in *Lessons from the war in Iraq*, MILITARY THOUGHT (May 1, 2003). *See also* Chris C. Demchal, *Wars of Disruption*, in NATIONAL SECURITY IN THE INFORMATION AGE 75-112 (Emily O. Goldman, ed. 2004).

prosecution to preemption [12] – challenges existing international and national governing structures both for authorizing and constraining the use of sovereign power (particularly coercive force) because national security power and law enforcement power have traditionally been governed by and managed under disparate – and potentially irreconcilable – doctrines and laws that may not be adequate to fill interstitial gaps in which these new threats operate and where information warfare based counter-measures may need to be considered.

Further, this paper argues that non-state groups – especially fundamentalist groups like al-Qa'ida organized along net-centric segmented tribal lines [13] – are benefiting from and taking advantage of opportunities provided by advanced information technologies to recruit, organize, plan, direct, finance, and execute criminal or terrorist acts, as well as to elicit overt and covert support from various population groups in furtherance of their activities, and that these terrorist groups may not be susceptible to conventional military or law enforcement strategies. [14] This paper adheres to the view that modern information technologies are themselves among the primary enabling mechanisms for the emergence and amplification of certain sub-state organized threats to global security [15] and suggests, therefore, that counter-strategies based on advanced information, organizational, and network theory aimed at disrupting or manipulating the

---

[12] In response to the attacks of 9/11, the U.S. Department of Justice and the FBI have undertaken to reorganize their mission from the traditional role of investigating and prosecuting crime that has already occurred to that of preventing future acts of terrorism. *See* U.S. Department of Justice, *Fact Sheet: Shifting from Prosecution to Prevention, Redesigning the Justice Department to Prevent Future Acts of Terrorism* (May 29, 2002), *available at* http://www.fas.org/irp/news/2002/05/ fbireorganizationfactsheet.pdf.

[13] David Ronfeldt, *Al Qaeda and its affiliates: A global tribe waging segmental warfare?* FIRST MONDAY (2005) *available at* http://www.firstmonday.org/issues/issue10_3/ronfeldt/index.html.

[14] For example, strategies derived from prosecuting hierarchical organized crime operations may not be applicable to leaderless segmented organizations.

[15] See David Ronfeldt & John Arquilla, *What Next for Networks and Netwars*, in NETWORKS AND NETWARS (John Arquilla & David Ronfeldt, *eds*. 2001).

usefulness of information and information resources to these hostile networks needs to be considered. [16] Physical, regulatory, and social disruption and targeting mechanisms aimed at information, channels, and actors are discussed, including actions to disrupt links, target nodes, and introduce misinformation in order to deceive, misdirect, or undermine opposed organizational activity or cohesion.[17]

This paper examines both covert and overt tactics potentially available to military, intelligence, and law enforcement forces, the existing legal and policy regimes governing the use of such methods in each context, and the potential conflict or gaps in law or policy from employing these strategies across jurisdictional and organizational divides. In addition, this paper examines the potential clash between the use of these methods and traditional or current notions of free expression, free association, and due process. This paper reviews various specific legal and technical mechanisms that are currently employed or being considered (for example, material support statutes, control orders, identity nullification, etc.) and suggests some principles that might be applied in order to mitigate the potential harms from misuse or abuse of these techniques as well as to conform their use to circumstances compatible with liberal democratic governance. In sum, this paper aims to inform and engender public debate about the potential use of disruption and manipulation techniques on information and information flows in order to control non-state actors that threaten global or national security.

---

16 *See id.*

17 Although we focus in this paper on the opportunities enabled by advanced information technologies and modern organizational theories, it should be noted that strategies and tactics aimed at disrupting organizational networks are not new. Machiavelli, among others, wrote about disrupting organization by planting seeds of dissension or by eliminating necessary support elements. NICCOLO MACHIAVELLI, THE PRINCE (W. K. Marriot, tr., 1916, c. 1505), THE ART OF WAR (Ellis Farneworth, tr., revised edition, 1965, 1520), and THE DISCOURSES (Leslie J. Walker and Bernard Crick, trs. 1985, 1531)) and manipulating information to create discontent and unrest within enemy forces has been a staple of military theorists since the earliest known western technical warfare writer, Aeneas Tacticus, *On the Defense of Fortified Positions* (Loeb Classics 1923, 360 B.C.).