The Need for Intelligence Community Sponsored Influence Research

Jason Spitaletta, Ph.D.[1]; Gregory Seese, Psy.D., Ian McCulloh, Ph.D.
The Johns Hopkins University Applied Physics Laboratory

Problem Statement

Military Information Support Operations (MISO)[2] is a critical capability in contemporary conflict. Its success depends upon the application of social and behavioral science to analyze target audiences, craft messages, and measure the outcome of their dissemination (Spitaletta, 2013). Recent operational experience has exposed weaknesses in US capability that require redoubled effort to conduct research on the mechanisms and methods of influence and their effective application. In particular, the US needs to better understand the doctrines of adversaries and to develop countermeasures against them. The modern Russian manifestation of information confrontation, often attributed to Chief of the General Staff of the Armed Forces Valery Gerasimov, adapts historical Russian and Soviet tactics of *maskirovka* (surprise, camouflage, concealment, mimicry, disinformation, and deceptive maneuver) in the contemporary information environment (Thornton, 2015). These approaches are a combination of not only overt military but also covert intelligence tactics that, when executed by disciplined professionals, can achieve a variety of economic and geopolitical effects (Pacepa & Rynchlak, 2013). The Chinese "Three Warfares" concept includes psychological warfare, along with legal warfare and media warfare, or the activities designed to disrupt an opponent's decision-making capacity by creating doubts, fomenting anti-leadership sentiments, and generally sapping an opponent's will (Lee, 2014). In additional to the aforementioned state actors, the increasing sophistication and brutality of the Islamic State's psychological warfare tactics (Spitaletta, 2015) exemplify how violent extremist organizations continue to impose their will on selected target audiences through carefully crafted cruelty (Bos, Spitaletta, Molnar, Tinker, & LeNoir, 2013). Current threats to National security consist of the destruction of the North Atlantic Treaty Organization (NATO) through Russian information confrontation, radicalization of American citizens by DA'ESH (ISIS), or online mobilization and hysteria that directly effects the US economy or indirectly effects key import/export markets. All key threats to US national security occur in the information environment. Despite this growing reality, resources within the IC and Department of Defense (DoD) remain focused on the kinetic threats of the last century. Limited resources are devoted to information operations where existential threats exist.

[1] Corresponding author: Jason.Spitaletta@jhuapl.edu; Jason.A.Spitaletta@coe.ic.gov

[2] Joint Publication 3-13.2 Information Operations defines MISO as planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Both "Military Information Support Operations (MISO)" and "Psychological Operations (PSYOP)" are currently used in US military parlance with "PSYOP" referring to the personnel and formations and "MISO" referring to the activities they conduct.

Influence Practice

MISO has historically based its methods on scientific findings. In practice, however, deviations from science-based methods have lessened the effectiveness of MISO (MacKay et al, 2012) and thus a common refrain is to incorporate more theory and analytic findings into the process (Reynolds & Lyle, 2013; DiEullis, Casebeer, Giordano, & Wright, 2014; Giordano, 2016; Spitaletta, 2016).

It is explicitly stated in US Psychological Operations (PSYOP) Doctrine (FM 3-05.301) that Target Audience Analysis (the psychological and behavioral profiling of foreign groups and individuals) is the cornerstone of effective MISO. Yet this is an area that has consistently been identified as inadequate (Lamb, 2005; Munoz, 2012; MacKay et al, 2012; McCulloh et al, 2017; Tatham, 2015).

An integral aspect of TAA is Human Factors Analysis (HFA). The term "human factors" has a broad set of interpretations in industry and academia but the Intelligence Community considers HFA the evaluation of psychological attributes (motivation, thinking style, beliefs, and personality), cultural attributes (values, beliefs and norms that influence behavior), behavioral attributes (responses to context or stimuli independent of personality), as well as the neural correlates of those attributes, in order to influence decision-making (how individuals and groups select a course of action), information-flow (how individuals and groups acquire information required to make a decision), reasoning (how individual and groups process information they receive), neurobiological changes to (or away from) specific states, and ultimately, behavior of individuals and groups in any state or organization (Spitaletta, 2016).

HFA can be subdivided into three types of assessment; group and population analysis (GPA), social network analysis (SNA), and individual and leadership analysis. GPA can include social structures, stratification, and demographics, as well as the key institutions, governance, roles, culture, atmospherics, economic factors, and information networks. GPA should include not only formal structures and influences but also the unofficial, clandestine, and illicit. Social network analysis examines groups of humans within and beyond the social context of institutions. SNA enables human factors analysts to understand the strengths and vulnerabilities of different types of networks, how networks structures affect social processes, and the various roles individuals play with networks. Individual & Leadership Analysis examines the underlying human factors that affect how individuals manage their environment, process information, and make decisions (Spitaletta, 2016).

Operational influence requires a rich contextual understanding of the conditions specific to each operating environment as well as those key individuals whom the US would like to influence (Spitaletta, 2016). Understanding and applying this knowledge is necessary for both mass communication and personalized persuasion. HFA requires substantial funding to conduct surveys of various kinds. Individuals require proper training and background to conduct all of

this work and in a fiscally constrained environment, organizations often lack the necessary budget to have the right people perform the right research with the requisite rigor.

Directions in Influence Research

There is a growing body of scientific literature on the psychophysiological and neurocognitive influence and detection of deception from Russia, China, Iran, and other countries. Recent geopolitical events in the Ukraine, South China Sea and domestically suggest that multimodal measures to influence public opinion have become the main effort of many of the US's adversaries. Scanning world scientific and technology development should be a priority for the US scientific and technological intelligence community (Spitaletta, 2016).

The US intelligence community should also invest in both academic and industrial research and development efforts in the science of persuasion. Cyberpsychology and cyberneurobiology are both interdisciplinary fields that examine the interaction of humans and emerging cyber technology; the former focuses on the psychological (cognitive, affective, behavioral) aspects while the latter concentrates on the biological (genetic, anatomical, endocrinological). Recently released Office of the Secretary of Defense-Strategic Multi-Layer Assessments (OSD-SMA) Office white papers have suggested biopsychosocial models when considering assessing and influencing (Reynolds & Lyle, 2013; DiEullis, Casebeer, Giordano, & Wright, 2014; Giordano, 2016; Spitaletta, 2016). Bio-psycho-social approaches can enable more precise access, assessment, and targeting (Giordano, 2012a, b, 2014). While existing neuroscience-based technology has great potential to influence and/or deter targets in cyberspace, further research will allow planners to rely upon firmly established linkages between perception and actions when developing both their intelligence requirements and the desired psychological actions and effects (Spitaletta, 2014). There are compelling findings among published cyberpsychology and neuroscience research (Frith & Frith, 2012) whose methods can be adapted and incorporated into research designs to test some of the ideas presented in recent white papers (Reynolds & Lyle, 2013; DiEullis, Casebeer, Giordano, & Wright, 2014; Giordano, 2016; Spitaletta, 2016).

Incorporating applied research from neuroscience and captology (the use of computers as a persuasion technology), amongst others, will facilitate individually tailored influence products. Designing technologies with the explicit intent to change individual opinions, reasoning, and ultimately behavior is relatively young (Fogg, 2002). This is not a radical departure from traditional MISO; rather it expands the media, devices, and interfaces through which themes and messages are disseminated. Incorporating individual persuasive technology into product design, by tailoring the interaction based on an individual's set of system preferences, interests, and/or other relevant data (Berkovsky et al, 2012), point to new lines of research in human-computer interaction, cyberpsychology, and decision neuroscience.

The first interaction an individual will have with a social movement, be it nonviolent or violent, will likely be through the Internet and therefore, cyberspace can be what Sun Tzu considered "*entangling ground*", terrain that can be abandoned but difficulty to reoccupy (Spitaletta, 2016).

Cyber influence requires advances in both intelligence and targeting; a precise fusion of existing scientific and technical intelligence capabilities with applied neuroscience and psychological research (Spitaletta, 2014). Contemporary microtargetting incorporates open-source aggregation to develop a demographic profile (Korolova, 2011), but few techniques take the added steps of creating a psychological profile and tailoring the message accordingly (Hirsch et al, 2012). Companies such as Amazon, Google, and Facebook (among others) employ advanced web-analytics to identify individualized marketing opportunities. Contemporary machine learning approaches could be applied and/or co-opted to direct people toward, or away from, specific web content.

The national security community could benefit from lessons learned in the commercial sector as well as in political campaigns. Persuasion, emotion, and trust have become design criteria in online influence (Cuggleman, 2010) and their applicability to MISO is evident. Both personalized and persuasive technologies attempt to influence behavior hold promise (Berkovsky et al, 2012); synthesizing elements from each in conjunction with established methods of social influence holds potential both mass (Cialdini, 2008) and personalized (Burkett, 2013) persuasion. Research in decision neuroscience has contributed much to the scientific understanding of consumer behavior (Gass & Seiter, 2013); the combination of laboratory and naturalistic methods employed in those disciplines could be readily applied to a variety of MISO objectives. Understanding the psychological effect of particular influence products from both a subjective and objective perspective is daunting (Casebeer & Russell, 2005) but the work is necessary, particularly if the US is to become more effective in countering adversary narratives and developing our own (Seese & Haven, 2015).

Adopting commercial and/or novel scientific applications and applying them to national security raises ethical risks and therefore, thoughtful consideration is required. Government agencies, academic researchers, and think-tanks have identified the potential applications, risks, and ethical challenges of employing neuroscience and/or neurotechnology in support of national security objectives (Committee on Military and Intelligence Methodology for Emergent Neurophysiological and Cognitive/Neural Science Research in the Next Two Decades, 2008, The Royal Society, 2012; Defense Science Board, 2012; Giordano & Wurzman, 2011; Tennison & Moreno, 2012).

IC-sponsored research questions need to be formulated around the transition to MISO applications, to successfully apply findings from neurobiology, cognitive science experiments, captology case studies, and the full range of influence research. Technological superiority will not overcome cultural ignorance and thus established reliance on social scientists employing primary and secondary research with both qualitative and quantitative analysis should not be eschewed. Success against modern adversaries requires the IC to understand influence and conduct analysis that supports the military application of behavior change in the same manner that they understand maneuver warfare and the application of kinetic power. Influence is counter-intuitive and intelligence and military leaders are not necessarily trained in the effective employment of this capability. It is, therefore, even more important that proper resources are

allocated for understanding target audiences and assessing the potential impact of influence messages and programs. Integrating neuroscience, computer science, and captology to HFA offers the requisite technology to provide strategic direction, planning, and assessment of influence operations. The US Government should increase resourcing for influence related activities due to its growing importance to national security objectives.

References

Berkovsky, S., Freyne, J., & Oinas-Kukkonen, H. (2012). Influencing Individually: Fusing Personalization and Persuasion. *ACM Transactions on Interactive Intelligent Systems, 2*(2), 9:1-9:8.

Bos, N.B., Spitaletta, J.A., Molnar, A. R., Tinker, J. M., & LeNoir, J. D. (2013). *Human Factors Considerations of Undergrounds in Insurgencies, 2nd Ed*. Alexandria, VA: US Army Publications Directorate.

Burkett, R. (2013). An Alternative Framework for Agent Recruitment: From MICE to RASCLS. *Studies in Intelligence*, *57*(1), 7-17.

Casebeer, W.D. & Russell, J.A. (2005). Storytelling and Terrorism: Towards a Comprehensive 'CounterNarrative Strategy'. *Strategic Insights, IV* (3).

Cialdini, R.B. (2008). *Influence: Science & Practice, 5th Ed*. New York: Allyn and Bacon.

Cuggleman, B. (2010). *Online Social Marketing: Website Factors in Behavioral Change*. Unpublished doctoral dissertation, University of Wolverhampton.

DiEuliis, D. Casebeer, W., Giordano, J. & Wright, N. Cabayan (Eds)(2014). *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

Fogg, B.J. (2002). *Persuasive Technology: Using Computers to Change What We Think and Do*. Palo Alto, CA: Morgan Kaufmann.

Gass, R.H. & Seiter, J.S. (2013). *Persuasion: Social Influence and Compliance Gaining, 5th Ed*. New York: Routledge.

Giordano J. (2012a). Use of neuroscience and technology (neuro S/T) to affect human decision-making: Implications for neuro-ecology. *Strategic Multilayer Assessment (SMA) Report*, Washington, DC: SMA Press.

Giordano J. (2012b). Neurotechnology as demiurgical force: Avoiding Icarus' folly. In: Giordano J. (ed.) *Neurotechnology: Premises, Potential and Problems*. Boca Raton: CRC Press, p. 1-14.

Giordano J. (ed.) (2014). Neurotechnology in National Security: Technical Considerations, Neuroethical Concerns. Boca Raton: CRC Press.

Giordano, J. (Ed) (2016). *White Paper on Assessing and Anticipating Threats to US Security Interests: A Bio-Psycho-Social Science Approach for Understanding the Emergence of and Mitigating Violence and Terrorism.* Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.

Giordano J, & Wurzman R. (2011) Neurotechnology as weapons in national intelligence and defense. *Synesis, 2,* 138-151.

Hirsh, J.B., Kang, S.K., & Bodenhausen, G.V. (2012). Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits. *Psychological Science, 23*(8), 1-4.

Joint Staff (2006). *Joint Publication 3-13: Joint Doctrine for Information Operations*. Joint Warfighting Center Doctrine Division : Fort Monroe, VA

Lamb, C. J. (2005). *Review of Psychological Operations Lessons Learned from Recent Operational*

Experience. National Defense University, Washington, DC. https://fas.org/irp/eprint/lamb.pdf
Lee, Sangkuk. "China's 'Three Warfares': Origins, Applications, and Organizations." *Journal of Strategic Studies* 37, no. 2 (2014): 198-221.
MacKay, A., Tatham, S., & Rowland, L. (2012) . *The Effectiveness Of US Military Information Operations In Afghanistan 2001-2010: Why RAND Missed The Point.* Shriverham, UK: Defence Academy of the United Kingdom.
McCulloh, I., Healy, S., Markakis, P. (2017). Characterization of Open Resources for Planning and Understanding Strategies (Corpus). *Johns Hopkins Applied Physics Laboratory Technical Report AOS-17-0196.* February 2017. Laurel, MD.
Munoz, A. (2012). US Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010. Santa Monica, CA, RAND Corporation.
Pacepa, I. M., & Rychlak, R. J. (2013). *Disinformation: Former Spy Chief Reveals Secret Strategy for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. WND Books.
Reynolds, M. & Lyle, D. (Eds) (2013). *Topics for Operational Considerations: Insights from Neurobiology & Neuropsychology on Influence and Extremism—An Operational Perspective*. Washington, DC: Strategic Multilayer Assessment Office, Office of theSecretary of Defense.
Royal Society. (2012). *Brain Waves 3: Neuroscience, conflict, and security*. London: The Royal Society Science Policy Centre.
Schmid, A. (2005). Terrorism as psychological warfare. *Democracy and Security*, *1*(2), 137-146.
Seese, G & Haven, K. (2015). The Neuroscience of Influential Strategic Narratives & Storylines. *IO Sphere, Fall 2015*, 33-38.
Spitaletta, J. (2013). Neuropsychological Operations: A Concept for Counter-Radicalization. In Reynolds, M. and Lyle, D. (Eds) (2013). *Topics for Operational Considerations: Insights from Neurobiology & Neuropsychology on Influence and Extremism—An Operational Perspective*. Washington, DC: Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.
Spitaletta, J.A. (2014). Use of Cyber to affect neuroS/T based Deterrence and Influence. In D. DiEuliis, W. Casebeer, J. Giordano, N. Wright, & H. Cabayan (Eds)(2014). *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.
Spitaletta, J.A. (2015). Terror as a Psychological Warfare Objective: ISIL's Use of Ritualistic Decapitation. In J. Giordano & D. DiEuliis (Eds) (2015). *White Paper on Social and Cognitive Neuroscience Underpinnings of ISIL Behavior and Implications for Strategic Communication, Messaging, and Influence*. Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.
Spitaletta, J.A. (Ed) (2016). *Bio-Psycho-Social Applications to Cognitive Engagement.* Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense.
Tatham, S. (2015). Using Target Audience Analysis to Aid Strategic Level Decisionmaking. U.S. Army War College, Strategic Studies Institute, Carlisle, PA.
Tatham, S. (2015). Target Audience Analysis. Three Swords Magazine. NATO Joint Warfare Center, Stavanger, Norway. http://www.jwc.nato.int/images/stories/threeswords/TAA.pdf
Tennison, M.N. & Moreno, J.D. (2012). Neuroscience, Ethics, and National Security: The State of the Art. *PLoS Biol 10*(3): e1001289. doi:10.1371/journal.pbio.1001289.
Thornton, R. (2015). The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. *The RUSI Journal*, *160*(4), 40-48.