SMALL WARS JOURNAL

smallwarsjournal.com

A Theory of Dark Network Design (Part One)

by Ian S. Davis, Carrie L. Worth, and Douglas W. Zimmerman

Editor's Note: This essay is the first in a six-part series on a theory of dark network design. This series was originally submitted as a thesis graduation requirement for a MS in Defense Analysis at the Naval Postgraduate School in Monterey, CA. Dr. Nancy Roberts served as the thesis advisor, and Dr. John Arquilla served as the second reader. An electronic version of the complete thesis is available at http://edocs.nps.edu/npspubs/scholarly/theses/2010/Dec/10Dec_Davis_Ian.pdf

Abstract

This study presents a theory of dark network design and answers two fundamental questions about illuminating and interdicting dark networks: how are they configured and how are they vulnerable? We define dark networks as interdependent entities that use formal and informal ties to conduct licit or illicit activities and employ operational security measures and/or clandestine tradecraft techniques through varying degrees of overt, or more likely covert, activity to achieve their purpose. A dark network must design itself to buffer environmental hostility and produce output to achieve its purpose according to its design state. The level of hostility in the environment and the requirement for secure coordination of work determine the dark network's design state. These factors yield four typological dark network configurations: Opportunistic-Mechanical; Restrictive-Organic; Selective-Technical; and Surgical-Ad hoc. Each configuration must allow the secure coordination of work between the dark network's directional, operational, and supportive components and should adhere to the six principles of dark network design we identify: security, agility, resilience, direction setting, control, and capacity. If a dark network's configuration does not fit its design state or violates the principles of dark network design, the network will be vulnerable to illumination and interdiction.

Part One: Theory of Dark Network Design

Current theories on dark networks do not address what determines their configuration in an effort to operationalize their network purpose. We submit that dark networks have natural configurations and that these configurations differ according to the network's purpose and design state. Although no two networks are exactly the same, we submit dark networks have similar basic components that are configured to produce output through coordinated work to achieve a purpose. First, we will review our two dimensions of dark network design: relative hostility of the environment and the requirement for the secure coordination of work. Next, we describe the four typological configurations of dark networks: Opportunistic-Mechanical, Selective-Technical, Restrictive-Organic, and Surgical-Ad Hoc. We identify and define the three fundamental components of dark networks: directional- responsible for developing and framing the network's purpose; operational- responsible for conducting decisive action to achieve the purpose; and supportive- responsible for enabling decisive action to achieve the purpose. To

produce output, dark networks must overcome two critical design challenges and configure their components to buffer hostility and coordinate work. They do this by adhering to what we identify as the principles of dark network design: security, agility, resilience, direction setting, control, and capacity. Finally, we introduce our dark network system model that illustrates how a dark network coordinates work in a hostile environment to produce output and achieve its purpose.

Dimensions of Dark Network Design

External Dimension: Hostility of the Environment. Hostility in the environment is the relationship between the dark network and its environment where opposition entities (state or non-state actors) have the will and capacity to counter the intended purpose of the dark network using lethal and non-lethal means.

Internal Dimension: Secure Coordination of Work. The requirement for secure coordination of work is the dark network's need and desire to commit resources to purposely create an efficient state of coordination of work in order to achieve objectives and prevent destruction.

Dark Network Typology

The two design dimensions, the hostility of the environmental hostility and the network's requirement for secure coordination of work, yield four pure-form design states four typological dark network configurations (Figure 15). We refer to these as design states and typological configurations as: Type-I: Opportunistic-Mechanical; Type-II: Restrictive-Organic:; Type-III; Selective-Technical; and Type-IV: Surgical-Ad Hoc.

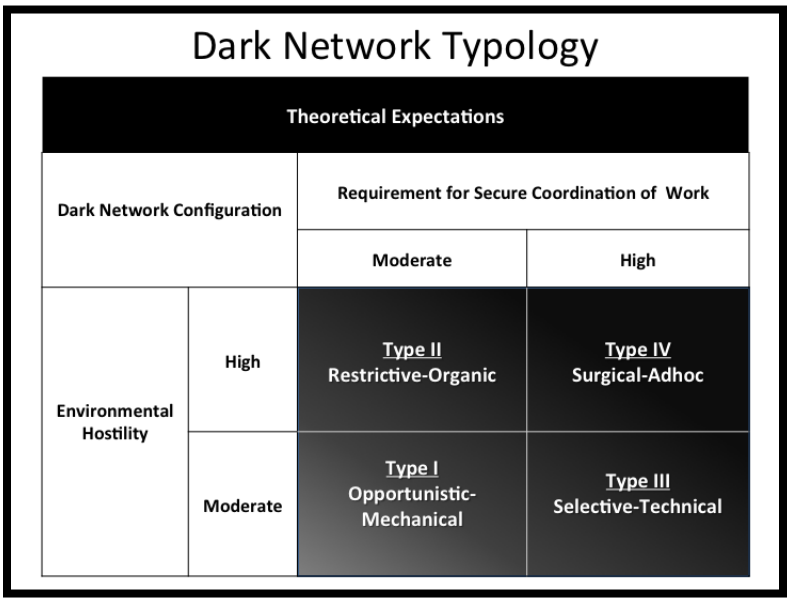

Figure One. Dark Network Typology

Type I: Opportunistic-Mechanical. This type of dark network operates in an environment with a moderate level of hostility and has a moderate requirement for a secure

coordination of work. Activity is opportunistic in nature and the network employs mechanistic governance. Organized criminal networks and paramilitary forces that operate in a selectively-overt (not covert) status are representative to this type of dark network. These networks are aware that the state can (and will) only use a limited application of force to inhibit their efforts. Examples include the Russian Solntsevskaya Brotherhood, Los Zetas in Mexico, and the transnational gang Mara Salvatrucha-13.

Type II: Restrictive-Organic. This type of network operates in environments a high level of hostility, but has a moderate requirement for a secure coordination of work. Activity is restrictive in nature because of the increased environmental hostility and is organic in nature to balance security and operational capacity. This type of network is one that is in a conflict with hostile opposition elements, but may have a high level of support from the community that gives it a more liberal freedom of movement in its environment. Type-II networks will typically maintain a clandestine and covert lifestyle, emerge conduct and overt act, and then return to the underground when threatened. Examples include Indonesia's Jemmah Islamiyah (JI), the Haqqani network in Afghanistan and Pakistan, the South Florida-based anti-Castro movement Alpha 66, and the Provisional Irish Republican Army (PIRA).

Type III: Selective-Technical. This type of network operates in moderately hostile environments but have a high requirement for secure coordination of work. Activity is selective in nature because of the moderate environmental hostility and is generally requires specialized education or technical knowledge. These networks typically resemble a supply chain network with serial workflow. This type of network may be involved in smuggling, financing, and other supportive activities and generally operates from a sanctuary that provides freedom of movement and action in areas of higher hostility. Historical examples of this type of network include the French Resistance Allied pilot evacuation network during World War II and the global network of Hezbollah.

Type IV: Surgical-Ad Hoc. This type of network operates in an environment with a high level of hostility and has a high requirement for secure coordination of work. Activity is surgical in nature because of the high environmental hostility and the cells are generally multifunctional and ad hoc due to its strict adherence to clandestine and covert behavior. Small, highly compartmented cells and singletons operating in an area where they are constantly being hunted typify a surgical-ad hoc network. Historical examples of this type of dark network are the Israeli Mossad covert action network designed to assassinate the Black September terrorists and Mohammed Atta's Hamburg network responsible for conducting the 911 attacks.

Dark Network Components

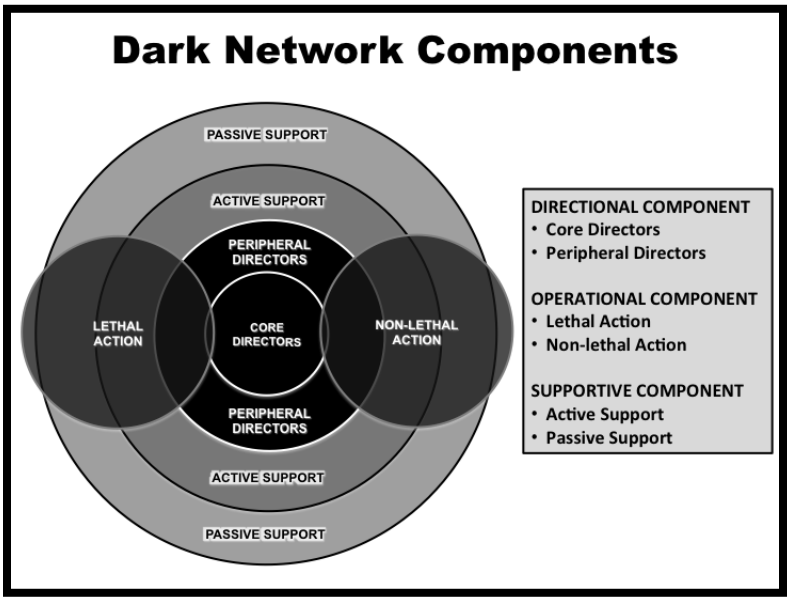

Figure Two. Dark Network Components

Directional Component. The directional component is responsible for developing and framing the network's purpose, what it is going to accomplish, how it is going to accomplish it, and ensures that all activities of the networks are nested in its purpose. They create the network's guiding narrative and direct its implementation. The directional component consists of the core directors and the peripheral directors.

Core Directors. The core directors set the strategic pace and ideology for the network. It is often removed from day to day operations, but will be considered the "face" of the network. The core directors develop and frame the network's purpose and doctrinal ideology that provides strategic direction that serves as the overarching guidance to the entire network. For example, the Tabilan's Quetta Shura, headed by Mullah Omar, serves as the core director for the Taliban network in Afghanistan and Pakistan.

Peripheral Directors. The peripheral directors provide direction and coordinate the work of the operational component and supportive component to produce value based on the network's purpose. In the Mintzberg sense, peripheral directors are the network's middle management, or middle line. It ensures the day-to-day operational and supportive activities nest with the network's strategic direction. The peripheral directors operationalize and direct the execution of operational and support activities based on strategic intent through specified and implied directives based on the network's purpose. The Taliban's core directors consist of the

key players at the operational and tactical levels that direct the activities of the rank and file members of the operational and supportive components.

Operational Component. The operational component is responsible for conducting decisive action (work) to produce effects (value) that achieves the network's purpose. Decisive Action elements are the entities that achieve defined objectives required to achieve the networks objectives related to its purpose. Peripheral directors from the directional component are embedded in the operational component and assume its leadership roles and functions. Decisive action is accomplished through lethal and non-lethal action.

Lethal Action. Lethal action entities achieve their objectives through the decisive use, or implied use of violence using direct and indirect fire weapons that cause destructive or lethal results. These entities may be referred to as direct action elements. Lethal actions are operations or activities (work) that are typically offensive in nature (i.e. ambushes, raids, bombing, assassination, direct and indirect fires, etc.) to cause destructive effects (value) to achieve the network's purpose. Peripheral directors from the directional component are embedded in the operational component and assume its leadership roles and functions. Taliban elements that conduct attacks on the Afghan security forces and coalition partners through direct fire, indirect fire, or improvised explosives devices represent operational components that conduct lethal action.

Non-Lethal Action. Non-lethal action entities achieve their objectives through the decisive use of non-lethal means to execute decisive operations. Non-lethal actions are operations or activities (work) that are typically offensive in nature (i.e. cyber-attack, information operations, subversion, electronic warfare, intelligence operatives, etc.) to cause destructive effects (value) to achieve the network's purpose. Taliban information operation elements that rapidly craft and disseminate media messages designed to erode the legitimacy and degrade the operational capacity of the coalition security forces in Afghanistan and Pakistan are representative of non-lethal decisive action elements.

Supportive Component. The supportive component is responsible for establishing mechanisms and conducting activities (work) to provide resources (value) that enable the operational component to conduct decisive action (work) and produce effects (value) to achieve the network's purpose. The supportive component consists of active and passive supporters.

Active Support. Active support is full-time or part-time activity (work) by actors that are witting of the true nature of their actions (i.e. trainers, safe site keepers, financiers, transportation agents, couriers, recruiters, surveillance and early warning, supply, administrative activities, etc.) to provide resources (values) necessary to resource and enable decisive operations and the network as a whole to achieve the network's purpose. Direct support entities work in concert with decisive action elements and the peripheral directors to give them the materials they need to conduct violent or spectacular events. Indirect support elements often work on the periphery of the network structure and are in general support to the entire network. These indirect support entities typically operate in the domain of the gray networks to interface with sources of passive support. The elaborate network of witting safe house keepers, cache emplacers, intelligence agents, transportation agents, recruiters, and the supply chains that provides all forms of lethal and non-lethal materials exemplifies types of active supporters.

Passive Support. Passive support is witting inaction or unwitting action (work) that enables and/or provides freedom of movement or action (value) for the directional, operational,

or supportive components to achieve the network's purpose. Passive supporters are generally those who are sympathetic to the network's purpose, but will not or cannot take an active role. Passive support can be financial support through putting money in jar at a local bar or simply refusing to give support to opposition forces of the dark network. Dark networks will use criteria-based networks to find sources of passive support. This shared set of attributes forms a basis of strong ties that recruiters can use to turn passive supporters to active members of the dark networks through persuasion or coercion. Passive support is the population where the dark network finds its sanctuary from hostile opposition forces. Afghans that do not outwardly reject the Taliban, or provide information to coalition security forces in order to illuminate and interdict the insurgent network, are passive supporters of the Taliban. This support may be provided willingly, or gain through coercion.

Based on our understanding of the directional, operational, and supportive components of a dark network, we are ready to examine how they work together to achieve a purpose. Next, we will present our dark network system model to illustrate how a network defines a purpose, conducts work, and produces values in a hostile environment.

Challenges and Principles of Dark Network Design

Dark networks must overcome inherent design challenges to conduct secure coordination of work there is an elevated level of hostility in the environment. We postulate that the two fundamental dark network design challenges are buffering external hostility and coordinating work to produce output. To overcome their design challenges, dark networks must design themselves to adhere to the principles of dark network design: security, resilience, agility, direction setting, control, and capacity. Failure to adhere to these six principals could have fatal consequences.

Buffering External Hostility. The first design challenge, buffering external hostility, relates insulating the network from the detrimental effects of the environment and reducing hostility. Three principles of dark network design that enable buffering are: security, agility, and resilience.

- Principle 1: Security. Security encompasses the application technical and non-technical means and methods of clandestine and covert behavior in order to prevent illumination and interdiction of the network.
- Principle 2: Agility. Agility entails the network's ability to adapt rapidly to changes in the environment.
- Principle 3: Resilience. Resilience is the network's ability to react to adversity, such as interdiction by opposition elements, and return to its prior state without catastrophic network disintegration or significant reduction in operational capacity. Compartmentalization, redundancy, and decentralization contribute to the resilience of a dark network.

Coordinating Work to Produce Output. The second design challenge, coordinating work to produce output, is related to the development of mechanisms the enable decisive action that is necessary to achieve the network's purpose. Three principals of dark network design that are critical for coordinating work to produce output are direction setting, control, and capacity.

- Principle 4: Direction Setting. Direction setting provides the overarching purpose for all network activities. The direction keeps members of the network engaged in their

activities and focuses them on the collective goal that transcends the needs and desires of the individual actors. The strategic core and functional periphery of the directional component set the network's direction to achieve an intangible ideological purpose through decisive action that results in tangible output.

- Principle 5: Control. Control is the coordination and synchronization of work that keeps the network focused on achieving its purpose through assignment of roles and responsibilities, evaluation of processes, and regulation of the network's resources on a continuous basis. While dark networks tend to have loose measures of control, they still require mechanisms to manage the network's resources and produce output in a secure manner that does not lead to network illumination and interdiction.
- Principle 6: Capacity. Capacity is the development of the necessary human, physical, and virtual infrastructure to coordinate work between the directional, operational, and supportive components that enables decisive action and achieves the network's purpose.

Dark Network System Model

The dark network system model (Figure Three) provides an illustration of how the directional, operational, and supportive components of a dark network interact to produce output through secure coordination of work that is directed to a common purpose. Adhering to the principals of dark network design enables the network to produce output while buffering environmental hostility. The dark network system model summarizes the theory of dark network design.

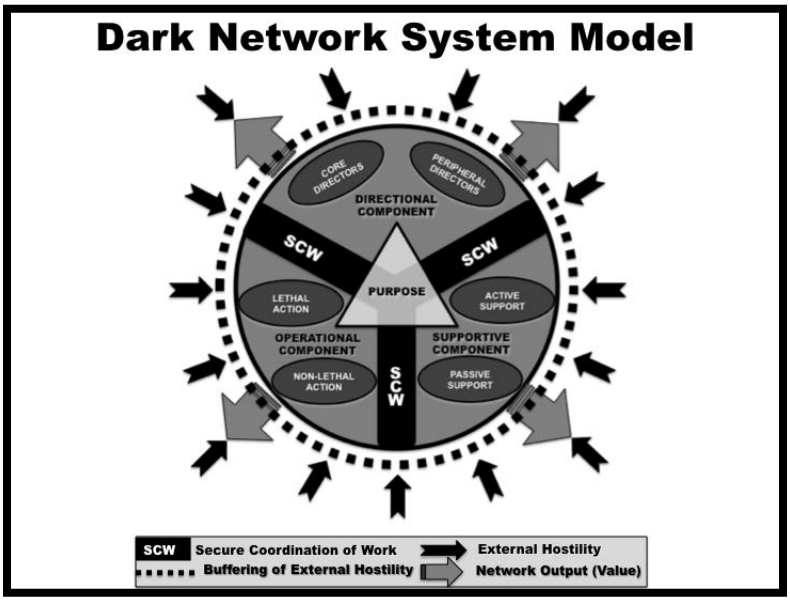

Figure Three. Dark Network System Model

Next, we apply our theory of dark network design to examine four dark networks based on our four design states. We selected our illustrative examples based on three criteria: the transnational nature of the network, the closeness of fit to the typological design state, and the availability of open source information on the network. In Part Two, we examine the transnational gang Mara Salvatrucha-13 (MS-13) to illustrate a Type-I Opportunistic-Mechanical network. In Part Three, we examine the Provisional Irish Republican Army (PIRA) to illustrate

a Type-II Restrictive-Organic network. In Part Four, we examine Hezbollah in Latin America to illustrate a Type-III Selective-Technical network. In Part Five, we examine the Hamburg Network that was responsible for the 9/11 attacks to illustrate a Type-IV Surgical-Ad hoc network. Our theory of dark network design will be used to analyze these examples and determine the network's configuration based on its design state and discover any vulnerability due to configurational mismatch or violation of the principals of dark network design. The final essay reviews the theory and offers conclusions and recommendations.

List of References

Adams, James. *The Financing of Terror*, New York: Simon and Shuster, 1986.

al-Alwaki, Anwar. "44 Ways to Support the Jihad." *The Force of Reason*. (November 2009). Accessed June 2, 2010. http://theforceofreason.com/wp-content/uploads/2009/11/44-Ways-to-Support-Jihad.pdf.

Anklam, Patti. *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World*. Burlington: Elsevier, 2007.

Arpoova, Shah. "The Mullah, the Caudillo, and the Terrorist." *The American: The Journal of the American Enterprise Institute.* 1 April 2009. Accessed on June 7, 2010. http://american.com.

Arquilla, John. "It Takes a Network: On Countering Terrorism." United States House of Representatives. (September 18, 2008). Accessed October 20, 2010. http://armedservices.house.gov/pdfs/TUTC091808/Arquilla_Testimony091808.pdf.

Arquilla, John, and David Ronfeldt. "RAND Monograph Reports - Networks and Netwars: The Future of Terror, Crime, and Militancy." RAND Corporation, 2001. Accessed on November 5, 2010. http://www.rand.org/pubs/monograph_reports/MR1382/.

———. "RAND Monograph Reports: The Advent of Netwar." RAND Corporation, 1996. Accessed on November 5, 2009. http://www.rand.org/pubs/monograph_reports/MR789/.

Azani, Eitan. *Hezbollah: The Story of the Party of God.* New York: Palgrave Macmillan, 2009.

Beam, Louis. "Leaderless Resistance." The Seditionist, 12 (February 1992). Accessed on August 4, 2010. http://www.louis-beam.com/leaderless.htm.

Belasco, Amy. "The Cost of Iraq, Afghanistan, and other Global War on Terror Operations since 9/11." Vers. 7-5700. Congressional Research Service. September 28, 2009. Accessed on June 28, 2010. https://www.hsdl.org.

Bell, J. Bowyer. "Aspects of the Dragonworld: Covert Communication and the Rebel Ecosystem." *Journal of International Intelligence and Counterintelligence* 3, no. 1 (1989): 15–43.

———. "Dragonworld (II) Deception, Tradecraft and the Provisional IRA," *International Journal of Intelligence and Counterintelligence* 8, No. 1 (1995), 25–50.

———. *The Secret Army*: *The IRA Rev 3rd Ed.*, New Brunswick: Transaction Publishers, 1997.

Borgatti, Stephen P., Ajay Mehra, Daniel J. Brass, and Giuseppe Labianca. "Network Analysis in the Social Sciences." *Science* 323, no. 5916 (February 2009): 892–895.

Borgatti, Stephen P., and Daniel S. Halgin. "Analyzing Affiliation Networks." In *The Sage Handbook of Social Network Analysis*, edited by Peter Carrington and John Scott. Essex: SAGE Publications Ltd, 2004. Accessed November 5, 2009. http://www.steveborgatti.com/publications/bhaffiliations.pdf.

Borgatti, Stephen P., and Pacey C. Foster. "The Network Paradigm in Organizational Research: A Review and Topology." *Journal of Manangement* 29, no. 3 (2003): 991–1013.

Borgatti, Stephen P., and Xun Li. "On Social Network Analysis in a Supply Chain Context." *Journal of Supply Chain Management* 45, no. 2 (2009): 5–22.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin Group, 2006.

Burt, Ronald S. Structural Holes: The Social Structure of Competition. Cambridge: Harvard University Press, 1992.

Burton, Fred. "Mara Salvatrucha: The New Face of Organized Crime?" Accessed on August 11, 2010. http://www.stratfor.com/memberships/48568/mara_salvatrucha_new_face_organized_crime?ip_auth_redirect=1.

Bush, George W. Executive Order 13224 - Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism. The White House. Washington, DC: Government Printing Office, September 23, 2001.

Caribbean Financial Action Task Force. "Money Laundering Prevention Guidelines for CFATF Member Governments, Free Trade Zone Authorities, and Merchants." The Caribbean Financial Action Task Force. 2001. Accessed June 2, 2010. http://www.cfatf-gafic.org/downloadables/doc/FTZ%20Recom.%20final-March%202001%20_En_.pdf.

Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. "Destabilizing Networks." *Connections* 24, no. 3 (2001): 31–34.

Carlile, Michael K. Into the Abyss: A Personal Journey into the World of Street Gangs. April 7, 2010. Accessed November 5, 2010. http://people.missouristate.edu/MichaelCarlie/.

Castells, Manuel. "Afterward: Why Networks Matter." in *Network Logic: Who Governs in an Interconnected World?*, edited by Helen McCarthy, Paul Miller and Paul Skidmore, 221–225. London: Demos, 2004.

———. *The Rise of the Network Society*. Cambridge: Blackwell Publishers, 1996.

Cline, Lawrence E. "Pseudo Operations and Counterinsurgency: Lessons from other Countries." United States Army War College Strategic Studies Institute. June 2005. Accessed November 8, 2009. http://www.carlisle.army.mil/ssi/pubs/display.cfm?PubID=607.

Commonwealth of Virginia Department of State Police Virginia Fusion Center. "Mara Salvatrucha 13 (MS-13) Intelligence Report," July 2008. Accessed on November 15, 2010. http://info.publicintelligence.net/VFCMaraSalvatrucha.pdf.

Coogan, Tim Pat. *The IRA*, London: Harper Collins, 2000.

Covin, Jeffrey G., and Dennis P. Slevin. "Strategic Management of Small Firms in Hostile and Benign Environments." *Strategic Management Journal* 10 (1989): 75–87.

Curtis, Glenn, and Tara Karacan. *The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe*. Ferderal Research Division, Library of Congress. Washington, DC: Government Printing Office, December 2002.

Daft, Richard L. *Essentials of Organization Theory and Design*. 8th Edition. Madison: South-Western Educational Publishing, 2003.

Daoust, Daniel C. and Joseph E. Osborne. "Counter-Organization Targeting: A Theoretical Framework for Analysis." Master's Thesis, Naval Postgraduate School, 1996.

de Nooy, Wouter, Andrej Mrvar, and Vladimir Batagelj. *Exploratory Social Network Analysis with Pajek*. Cambridge: Cambridge University Press, 2005.

Department of Defense. *Department of Defense Dictionary of Military and Associated Terms*. April 2010. Accessed on October 26, 2010. http://www.dtic.mil/doctrine/dod_dictionary/.

———. "Irregular Warfare: Countering Irregular Threats." Vers. 2.0. United States Joint Forces Command Joint Operating Concepts. May 17, 2010. ACCESSED JUNE 22, 2010. http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf.

Embassy of El Salvador, "The Peace Accords." Accessed October 23, 2010. http://www.elsalvador.org/embajadas/eeuu/home.nsf/politics.

Everton, Sean F. *Tracking, Destabilizing, and Disrupting Dark Networks Using Social Network Analysis*. Monterey, CA: Naval Postgraduate School, 2009.

The Federal Bureau of Investigation. "The MS-13 Threat: A National Threat Assessment." Accessed on August 11, 2010.

Felix, Christopher. *A Short Course in the Secret War*. New York: Madison Books, 2001.

Franco, Celinda. "The MS-13 and 18th Street Gangs: Emerging Transnational Gang Threats?" *CRS Report for Congress*, January 22, 2010. Accessed on August 11, 2010. http://opencrs.com/document/RL34233.

Galbraith, Jay, Diane Downey, and Amy Kates. *Designing Dynamic Organizations*. New York: American Management Association, 2002.

Gates, Robert M. "United States Department of Defense Quadrennial Defense Review Report." U.S. Department of Defense. February 12, 2010. Accessed February 17, 2010. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

Giraldo, Jeanne K., and Harold A. Trinkunas. *Terrorism Financing and State Responses: A Comparative Perspective*. Stanford, CA: Stanford University Press, 2007.

Gilbert, James. “Yuma Border Patrol Agents Arrest MS-13 Gang Member.” *Yuma Sun.* Accessed October 13, 2010. http://www.yumasun.com/common/printer/view.php?db=yumasun&id=49993.

Granovetter, Mark. "The Strength of Weak Ties: A Network Theory Revisited." *Social Theory I* (1983): 201–233.

Grdovic, Mark. "SWCS PUB 09-1: A Leader's Handbook to Unconventional Warfare." United States Army John F. Kennedy Special Warfare Center and School. November 2009. Accessed on January 27, 2010. http://www.soc.mil/swcs/swmag/Assets/SWCS%20Publications/Leaders%20Guide%20Final.pdf.

“Groups - Middle East – Active – Lebanon: Hizbullah.” *Jane’s World Insurgency and Terrorism*, April 29 2010. Accessed on June 4, 2010. http://www4.janes.com.libproxy.nps.edu.

Haaretz News Service, October 29, 2010. Accessed on November 5, 2010. http://www.haaretz.com/news/diplomacy-defense/mexico-thwarts-hezbollah-bid-to-set-up-south-american-network-1.300360.

Hanna, David P. *Designing Organizations for High Performance*. Reading: Addison-Wesley Publishing Company, 1988.

Hannigan, John A. “The Armalite and the Ballot Box: Dilemmas of Strategy and Ideology in the Provisional IRA,” *Social Problems*, 33, No. 1 (October 1985): 31–40. JSTOR (800629)

Hanlon, N. “Banking 101 with Chavez and Ahmadinejad” *The Americas Report*, May 07, 2009. Accessed on June 5, 2010. http://www.centerforsecurity.org.

Harness, William J. “MS-13 Mara Salvatrucha.” *Conroe ISD Police Department Report* (2006), Accessed on April 11, 2010. http://police.conroeisd.net/Docs/MS%2013%20Gang.pdf.

Henzel, Christopher. "The Origins of al Qaeda's Ideology: Implications for U.S. Strategy." *Parameters*, Spring 2005: 69–79.

“The hijackers... and how they were connected.” *Sydney Morning Herald.* September 22, 2001. Accessed on October 13, 2010.

Horigan, John and Max Taylor, “Playing the Green Card: The Financing of the Provisional IRA, Part 1.” *Terrorism and Political Violence*, 11, No. 2, Summer 1999, 1–20

———. “Playing the Green Card: Financing the Provisional IRA, Part 2,” *Terrorism and Political Violence*, 15, No. 2, Summer 2003, 1–60.

———. “The Provisional Irish Republican Army: Command and Functional Structure”, *Terrorism and Political Violence*, 9: 3, 1997, 1–32. Accessed October 13, 2010. http://dx.doi.org/10.1080/09546559708427413.

Hudson, R. *Terrorist and Organized Crime Groups in the Tri-Border Area (TBA) of South America*. Washington DC: Library of Congress Research Division, 2003.

Hulnick, Arthur S. and Daniel W. Mattasusch. "Ethics and Morality in U.S. Secret Intelligence" in *Ethics of Spying: A Reader for the Intelligence Professional*, edited by Jan Goldman, 520-521. Lanham: Scarecrow Press, 2006.

International Institute for Counter-Terrorism. "ICT Commentaries- Venzuelan Ties to Hezbollah." *International Institute for Counter-Terrorism*. August 18, 2008. Accessed on March 2, 2010. http://www.ict.org.il/NewsCommentaries/Commentaries/.

Jackson, Brian A. "Counterinsurgency Intelligence in a Long War: The British Experience in Northern Ireland," *Military Review*, (January/February 2002): 74–85.

Jackson, Brian A., John C. Baker, Kim Cragin, John Parachini, Horacio R. Trujillo, Peter Chalk, *Aptitude for Destruction: Case Studies of Organizational Learning in Five Terrorist Groups*, Santa Monica, CA: Rand Corp, 2005.

Jansen, Erik. "MN3121: Organizational Design for Defense Analysis." Naval Postgraduate School, Fall Term 2009.

Jimenez, Edgar A., James S. McCullar, and Kevin M. Trujillo. "Pseudo Operations and Deception in Irregular Conflict." Naval Postgraduate School, 2010.

Jones, Derek. "Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Conternetwork Operations." United States Army Command and General Staff College School of Advanced Military Studies. May 21, 2009. Accessed on November 5, 2009. http://www.cgsc.edu/sams/media/Monographs/JonesD-21MAY09.pdf.

Juergensmeyer, Mark. *Terror in the Mind of God*. Berkeley: University of California, 2003.

Karmon, Eli, *Iran and its Proxy Hezbollah: Strategic Penetration in Latin America Working Paper*. Madrid: Elcano Royal Institute, August 2009. Accessed on October 28, 2010. https://www.realinstitutelcano.org.

Khoury, Jack. "Mexico Thwarts Hezbollah Bid to set up South American Network," June 7, 2010. Accessed December 13, 2010. http://www.haaretz.com/news/diplomacy-defense/mexico-thwarts-hezbollah-bid-to-set-up-south-american-network-1.300360.

Kittner, Cristina Brafman. "The Role of Safe Havins in Islamist Terrorism." *Terrorism and Political Violence* 19, no. 3 (2007): 307–327.

Krackhardt, David. "The Strength of Strong Ties: The importance of Pilios in Organizations." in *Networks and Organizations: Structure, Form, and Action*, by Nitin Nohria and Robert G. Eccles, 216–239. Boston: Harvard Business School Press, 1992.

Krebs, Valdis E. "Mapping Networks of Terrorist Cells." *Connections* 24 (2001): 43–52.

Krul, Chris and Sebastian Rotella, S. "Drug probe finds Hezbollah link; Officials say they've broken up Colombian ring that helped fund the militant group." *Los Angeles Times*, October 22, 2008. Accessed on June 14, 2010. http://www.proquest.com.libproxy.nps.edu/.

Liang, Qiao, and Wang Xiangsui. "Unrestricted Warfare." IWS - The Information Warfare Site. PLA Literature and Arts Publishing House. February 1999. Accessed on October 7, 2009. http://www.iwar.org.uk/iwar/resources/china/iw/unrestricted-warfare.pdf.

LaVerle, Barry, Glenn E. Curtis, Rex A. Hudson, Nina A. Kollars, *A Global Overview of Narcotics Funded Terrorist and Other Extremist Groups*. Washington DC: Library of Congress, 2002. Accessed on June 3, 2010. http://www.loc.gov/rr/frd.

Logan, Sam, Ben Bain and Kate Kairies. "Deportation Feeds a Cycle of Violence in Central America." *World Press*, March 31, 2006. Accessed on July 11, 2010. http://www.worldpress.org/Americas/2304.cfm.

Looney, Robert E. "Following the Terrorist Informal Money Trail: The Hawala Financial Mechanism. Naval Postgraduate School Center for Contemporary Conflict, Monterey, CA, November 1, 2002.

Martin, Bryan, Gabriel Szody, and Joshua Thiel. "Radical Destabilization: A Low Cost, High Success Policy Option for the United States." Naval Postgraduate School, 2010.

McCargar, James. "Part 1: Fundementals and Forms of Action." in *A Short Course in the Secret War*, by Christopher Felix, 15–151. Lanham: Madison Books, 2001.

McCormick, G. H., and G. Owen. "Security and Coordination in a Clandestine Organization." *Mathematical and Computer Modeling*, no. 31 (2000): 175–192.

McDermott, Jeremy. "Youths Flock to Massive El Salvadoran Gang that is their Only Chance of a 'Job'," *The Scotsman*, sec. International, April 13, 2004. Accessed on April 2, 2010. http://thescotsman.scotsman/international.cfm?id=416482004&format=print.

Milward, H. Brinton, and Joerg Raab. "Dark Networks as Problems Revisited: Adaptation and Transformation of Islamic Terror Organizations since 9/11." University of Southern California. September 29, 2005. Accessed on August 4, 2010. http://www.usc.edu/schools/sppd/private/documents/bedrosian/dark_networks.pdf.

Mintzberg, Henry. *Mintzberg on Management: Inside Our Strange World of Organizations*. New York: The Free Press, 1989.

Mintzberg, Henry. "Organization Design: Fashion or Fit?" *Harvard Business Review* 59, no. 1 (January/February 1981): 103–116.

Miro, Ramon J., "Organized Crime and Terrorist Activity in Mexico, 1999-2002", *Library of Congress Report* (February 2003), Accessed on November 29, 2010. http://www.loc.gov/rr/frd/pdf-files/OrgCrime_Mexico.pdf.

Miryekta, Cyrus, "Hezbollah in the Tri-Border Area of South America." *Small Wars Journal*, September 10, 2010. Accessed on October 25, 2010. http://smallwarsjournal.com/blog/journal/docs-temp/533-miryekta.pdf.

Molnar, Andrew R., Jerry M. Tinker, and John D. LeNoir. "Chapter 1: Underground Organization within Insurgency." in *Human Factors Considerations of Undergrounds in Insurgencies*, by Special Operations Research Office, 17–35. Washingtoc D.C.: Special Operations Research Office, 1965.

———. "Chapter 5: Clandestine and Covert Behavior." in *Human Factors Considerations of Undergrounds in Insurgencies*, 101–108. Washington, D.C.: Special Operations Research Office, 1965.

Molnar, Andrew R., William A. Lybrand, Lorna Hahn, James L. Kirkman, and Peter B. Riddleberger. *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare*. Washington, D.C.: Special Operations Research Office, 1963.

Moloney, Ed. *A Secret History of IRA*, 2nd ed., London: Penguin Books, 2007.

Nadler, David, Michael Tushman, and Mark B. Nadler. *Competing by Design: The Power of Organizational Architecture*. New York: Oxford University Press, 1997.

Nagorsky, Thomas. President Ahmedinejad Threatens U.S. With War 'Without Boundaries'. September 21, 2010. Accessed on October 13, 2010. http://abcnews.go.com/International/iran-president-threatens-us-war-boundaries-nuclear-faclities/story?id=11689305&page=1.

National Commission on Terrorist Attacks Upon the United States. "Al Qaeda Aims At The American Homeland." Accessed on August 30, 2010. http://www.9-11commission.gov/report/911Report_Ch5.htm.

National Counterterrorism Center, "Hizballah," *Counterterrorism Calendar 2010.* Accessed on November 8, 2010. http://www.nctc.gov/site/groups/hizballah.html.

Obama, Barack. "National Security Strategy." The White House. May 27, 2010. Accessed on May 28, 2010. www.whitehouse.gov/sites/default/files/rss.../national_security_strategy.pdf.

Peters, Gretchen, "Drug Trafficking in the Pacific Has a Distinct Russian Flavor," *San Francisco Chronicle,* 30 May 2001. Accessed on November 29, 2010. http://articles.sfgate.com/2001-05-30/news/17600134_1_svesda-maru-russians-largest-cocaine-seizure.

Phillippone, Douglas, *Hezbollah: the Network and Its Support Systems, Can They be Stopped?* (Monterey, CA: Naval Postgraduate School, 2008).

"The Plot: A Web of Connections." *The Washington Post.* September 24, 2001. Accessed October 13, 2010. http://www.washingtonpost.com/wp-srv/nation/graphics/attackinvestigation_24.html.

Prager Security International. *Denial of Sanctuary: Understanding Terrorist Safe Havens,* edited by Michael Innes. Westport: Prager Security International, 2007.

"Provisional Irish Republican Army" *Jane's World Insurgency and Terrorism*, Jane's Terrorism and Insurgency Center (2009). Accessed on September 28, 2010. http://www8.janes.com.libproxy.nps.edu/JDIC/JTIC/documentView.do?docId=/content1/janesdata/binder/jwit/jwita107.htm@current&pageSelected=&keyword=&backPath=http://jtic.janes.com/JDIC/JTIC&Prod_Name=JWIT&activeNav=http://www8.janes.com/JDIC/JTIC.

Raab, Jorg, and H. Brinton Milward. "Dark Networks as Problems." *Journal of Public Administration Research and Theory* 13, no. 4 (October 2003): 413–439.

Rabasa, Angel, et al. "Ungoverned Territories: Understanding and Reducing Terrorism Risks." RAND Corporation, 2007. Accessed on October 12, 2009. http://www.rand.org/pubs/monographs/2007/RAND_MG561.pdf.

Robb, John. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2007.

Roth, John, Douglas Greenburg, and Serena Wille. "Monograph on Terrorist Financing". National Commission on Terrorist Attacks Upon the United States. Washington, DC: Government Printing Office, August 21, 2004.

Ruppersberger, C.A. "Dutch". Statement on threat of gangs. Accessed November 6, 2010. http://dutch.house.gov/2006/07/07-14-06-MS13Gang.shtml.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia: University of Philadelphia Press, 2008.

———. *Understanding Terror Networks.* Philadelphia: University of Philadelphia Press, 2004.

Silke, Andrew, "In Defense of the Realm: Loyalist Terrorism in Ireland Part 1: Extortion and Blackmail*," Studies in Conflict and Terrorism* (1998): 331–361.

Simons, Anna, and Davis Tucker. "The Misleading Problem of Failed States: A 'Socio-geography' of Terrorism in the Post-9/11 Era." *Third World Quarterly* 28, no. 2 (2007): 387–401.

Sparrow, Malcolm K. "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks* 13 (1991): 251–274.

Steele, J. Michael. "Models for Managing Secrets." *Management Science* (INFORMS) 35, no. 2 (1989): 240–248.

Stewart, T. "Six degrees of Mohamed Atta." Business 2.0. December 2001. Accessed October 13, 2010. http://www.business2.com/articles/mag/0,1640,35253,FF.html.

Sullivan, Mark P. *Latin America: Terrorism Issues.* Washington DC: Congressional Research Service, 2009.

Sullivan, John P. and Samuel Logan. "MS-13 Leadership: Networks of Influence." *The Counter Terrorist.* August/September 2010. Accessed on November 9, 2010. http://digital.ipprintservices.com/display_article.php?id=428186.

"Suspected MS-13 Gang Leader Arrested in Santa Cruz." KSBW News.com. Accessed December 1, 2010. http://www.ksbw.com/news/23772715/detail.html.

Treverton, G., Matthies, C., Cunningham, K.J., Goulka,J., Ridgeway, G., Wong, *A. Film Piracy,Organized Crime and Terrorism*. Santa Monica, CA: RAND Corporation, 2010.

Turney-High, Harry Holbert. *Primitive War*, 2nd Edition (Columbia: University of South Carolina Press, 1991).

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1971.

United States Congress. "MS-13 and Counting." *Hearing before the Committee on Government Reform*. House of Representatives, 109th Congress, 2nd Session, July 14, 2006, serial no. 109-174 and September 6, 2006, serial no. 109–182.

United States Congress, *Weak Bilateral Law Enforcement Presence at the U.S.-Mexico Border: Territorial Integrity and Safety Issues for American Citizens,* Joint Hearing of the

109th Congress, 1st Session, November 17, 2005. Washington D.C.: U.S. Government Printing Office, 2006.

United States Department of Justice. "Indictment of ZACARIAS MOUSSAOUI." December 11, 2001. Accessed on November 2, 2010. http://www.usdoj.gov/ag/moussaouiindictment.htm.

United States Department of Justice, "Mara Salvatrucha," *Drugs and Crime Gang Profile*, November 2002. Accessed on November 15, 2010. http://webzoom.freewebs.com/swnmia/mara.pdf.

United States Department of Defense. Transcript of bin Laden Video Tape. December 13, 2001. Accessed on October 13, 2010. http://www.defenselink.mil/news/Dec2001/D20011213ubl.pdf.

United States House of Representatives, Committee on International Relations. *Iran: A Quarter Century of State-Sponsored Terror.* Washington DC: US Government Printing Office, 2005.

United States Senate Committee on Homeland Security and Governmental Affairs. *Hezbollah: Financing Terror Through Criminal Enterprise, Testimony of Dr. Matthew Levitt*. 109th Congress, 1st Sess. May 25, 2005

Van De Ven, Andrew H., Andre L. Delbecq, and Jr., Richard Koenig. "Determinants of Coordination Modes within Organizations." *American Sociological Review* (American Sociological Association) 41, no. 2 (April 1976): 322–338.

Ware, Michael. "Los Zetas called Mexico's most dangerous drug cartel," *CNN.com.* Accessed on November 29, 2010. http://www.cnn.com/209/WORLD/americas/08/06/mexico.drug.cartels/index.html.

White, Robert W. "Don't confuse me with the facts: More on the Irish Republican Army and Sectarianism." *Terrorism and Political Violence* 10, no. 4, (1998): 164–189. Accessed on October 1, 2010. http://dx.doi.org/10.1080/09546559808427487.

White, Robert W. *Provisional Irish Republicans: An Oral and Interpretive History*. Westport, CT: Greenwood Press, 1989.

Wood, Randall, "South America's Tri-Borders Region," *SAIS Review*, 25, No. 1, Winter-Spring 2005, 105.

Woodrow Wilson International Center for Scholars Latin American Program. "Iran in Latin America: Threat or 'Axis of Annoyance'?" Woodrow Wilson Center Reports on the Americas. 23. Edited by Cynthia Arnson, Haleh Esfandiari and Adam Stubits. Washington, DC, January 2010.

World's Most Dangerous Gang. DVD. Produced by Andrew Tkach. 2006; U.S.A. and Canada: Warner Home Video, 2006.

Major Ian Davis is a United States Army Special Forces officer and recently graduated from the Naval Postgraduate School in Monterey, CA with a Masters of Science in Defense Analysis. Major Davis has over 23 years of active duty service with the majority of his career assigned to 7th Special Forces Group (Airborne) in key enlisted and officer operational billets. He is currently conducting an internship with CJSOTF-A en route to his next assignment at 7th Special Forces Group (Airborne).

Major Carrie Worth is United States Air Force Special Operations Command (AFSOC) aviator and recently graduated from the Naval Postgraduate School in Monterey, CA with a Masters in Defense Analysis. After graduating from the United States Air Force Academy in 1997, Major Worth has accumulated over 4,800 flight hours in assignments throughout AFSOC community. She is currently en route to her next assignment at Special Operations Command Europe.

Major Douglas Zimmerman is a United States Army Intelligence officer and recently graduated from the Naval Postgraduate School in Monterey, CA with a Masters of Science in Defense Analysis. Major Zimmerman has over 14 years of active duty service and spent the majority of his career supporting Special Operations forces with assignments in the 4th PSYOP Group (Airborne), 10th Special Forces Group (Airborne), 7th Special Forces Group (Airborne) and USASOC Headquarters. He is currently conducting an internship in the Common Operational Research Environment (CORE) Laboratory and the Naval Postgraduate School.