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.

![Dark Network Typology Diagram](image)

**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 Jemnah 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.
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 Taliban’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](image)

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**


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


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.