DARK NETWORKS IN A BRIGHT NETWORK WORLD

By

PETRA MAEN MDANAT

_____

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelors degree
With Honors in

Political Science

THE UNIVERSITY OF ARIZONA

M A Y 2 0 1 9

Approved by:

_____

Professor Kirssa Cline Ryckman

School of Government and Public Policy

Table of Contents:

Abstract

Bright networks spend billions of dollars each year trying to eliminate dark networks, and yet they still persist to be a threat to regional stability, especially in regions that have weak states. The purpose of this research paper is to determine what bright network behaviors are prolonging the lifetime of dark networks, to determine if these behaviors are of a direct or indirect nature, and figuring out the reasons why legitimate actors would behave in a way that is compromising to their own goals. This purpose will be analyzed through a set of hypotheses, which will then be tested on two case studies. The common theme among all my hypotheses is that there are underlying motivations for bright networks to sponsor dark networks and these are further explored in the case studies. Overall, this paper explores the complexities of dark networks and the struggles of bright networks to eliminate these organizations. This paper looks to further develop the relationship between bright and dark networks and identify where the overlap might be perpetuating, rather than decreasing, dark network activities. Overall, dark networks feed off of corruption, chaos, and instability; therefore states with these issues are prone to dark network insurgencies.

Chapter 1: Introduction

Since the attacks of September 11, the U.S. has put a considerable amount of effort into ensuring that similar events never happen again. Counterterrorism efforts have increased yearly since then, the Stimson Study Group put out a study in which they calculated government spending on counterterrorism, their research "suggests that total spending that has been characterized as Counter Terrorism-related totaled $2.8 trillion

during fiscal years 2002 through 2017." All this to say that the U.S. puts a momentous emphasis on the security of our nation and terrorist organizations, threaten this security. Organizations that thrive during periods of chaos and instability and operate illicitly and illegally can be categorized into the group of "dark networks". Some dark networks might include terrorist organizations, cartels, black market groups, and more. We have been trying to combat these organizations with no permanent success over the last two decades; this is largely in part because these illicit, covert, underground networks have found ways to gain support from legitimate actors, or "bright networks" which has increased their ability to survive and bounce back from multiple targeted military operations against them. Through researching terrorist organizations in hopes of better understanding how governments can stop these insurgencies around the globe, I was fascinated to discover that legitimate governments and government agencies (bright networks) themselves could be behaving in a way that perpetuates these dark networks which they are trying to eliminate.

The purpose of this research is threefold. First, to figure out what bright network behavior (if any at all) might be perpetuating the activities and longevity of dark networks. Second, if these activities are mainly directly or indirectly targeted to perpetuate these networks. Finally, are the bright networks that are behaving in this way doing so as a means to achieve international or domestic benefits or and what pressures are states facing from other states to deal with dark networks within their region?

Thesis Framework

In the following sections, I will do this by first defining dark and bright networks and briefly discussing their similarities and differences in structure, nature, and purpose, specifically the strengths and vulnerabilities of a network system. This portion will be a recounting of the research of other experts who have extensively looked at these aspects of dark networks. Next, I will be discussing what specific behaviors of bright networks might be perpetuating dark networks such as using them to fight their wars or overthrow a regime/leader (initiating/funding them), using them as scapegoats for domestic state issues (straying from the real problem of an unstable government), using them to gain leverage at the international level, etc. This section will also probe the various international and domestic elements that might be motivating these bright networks to do so. Then specific case studies will be analyzed that display both the behaviors of the bright networks and the successive outcome thereafter. This section will also explore the intent/motivation (or lack thereof) specific to these cases of bright networks for perpetuating dark networks and how the perpetuation was a calculated strategic move or an unintended consequence of a hasty or uninformed decision. The cases that will be explored are the Taliban's continued control over Afghanistan and why they are still in power after multiple international efforts to uproot them and the blood diamond economy as propped up and puppeted by Charles Taylor in Africa and how buying these diamonds expanded the scope and power of dark networks globally.

Previous Research

The relationship between bright and dark networks has just started to be more deeply explored since experts are still grappling with the nature of these complex organizations. The major research I have found on the topic cover mainly what dark

networks are, their characteristics, and their structures. When discussing these topics as a background for my research I will be relying heavily on the accomplished materials of experts who laid the foundation for my own research such as (but not limited to) Jörg Raab and H. Brinton Milward and Renee M. Bakker. While experts mainly looked into networks independently (referring to their innate nature and structure), I hope to explore dark networks in the context of international and domestic actors and how they may directly or indirectly influence them. Building on the work of previous research, my ultimate goal is to shed more light and offer insight into how governments could be working against themselves in regards to defeating dark networks. Jorg Raab and Brinton Milward briefly mention, “there may also be connections between the illegal networks, dark networks in our terms, and the legal networks striving to destroy them” (Dark Networks as Problems, page 415). However, their focus was more on network analysis and similarities and differences between different groups considered dark networks. I would also like to look at dark networks in the context of the international system and not dependent of any outside actors or motivations. It is important to portray both the effect bright networks are having on dark networks and vice versa. Many international actors have changed their international policies because dark networks play a role in their domestic and international goals. Pressures and incentives from other states who also have an agenda in regards to dark networks might also affect the outcome of behavior from states regionally associated with dark networks. Indeed Jorg and Milward discussed these pressures in their own research:

> “There is increasing evidence of a close connection between Al Qaeda and the failed states of Liberia, Sierra Leone, and Burkina Faso in West Africa. The

> connection appears based on Al Qaeda's need to exchange cash for diamonds. This is fueled by the pressure from the United States and Western Europe to clamp down on Al Qaeda's use of legitimate banks for international monetary transactions" (Jörg, Milward, Dark Networks as problems, 425).

I would like to discuss these types of relationships and pressures in similar cases to fully understand what type of incentives or benefits we are providing dark networks and figure out how we can avoid it in the future.

Importance of research question

Since the coining of the term "dark network", there has been much research on what they are and how they operate, and how social network analysis might be used to disrupt these networks however I have seen very little research dedicated to how they operate in the context and influence of bright network operations. It is important to understand how the behaviors of a bright network can influence the behaviors of dark networks and what motivations they have for operating in the spheres of bright networks. Looking at the big picture in this way will hopefully bring more clarity to why these organizations make certain decisions or take part in certain behaviors. By only looking at these groups as a separate entity without considering the involvement or influence of external actors, will distort future research and predictions because dark networks are not independent variables, but rather extremely dependent variables in the international context. In other words their actions heavily rely on those of bright networks.

Chapter 2: Setting the Foundation

Throughout the rest of this research, concepts such as hierarchy structure and network structure will be used consistently and terms such as bright network and dark network will be referred to repeatedly. It is important to set a baseline definition of these terms and concepts so as to fully appreciate the scope of this research and also to understand how other experts have understood these terms and concepts. Furthermore, defining these terms and concepts is vital in applying them to modern day complexities and issues. This chapter also seeks to cover the innate complexities of network systems by first looking at networks as a general and independent variable by looking at the advantages and disadvantages of this system, and then by applying these general characteristics more specifically to that of *dark* networks.

Concepts

It is a common misconception that dark networks are a new phenomenon, in actuality they have been around as long as bright networks have been around. We can depict their presence in history from Robin Hood's outlaw gang in the 14th century, to the 300 year struggle between states and piracy groups, to the present day with the continued survival of the Taliban, Al-Qaeda, ISIS, the drug cartels of South America, and the blood diamond trade in Africa. All these dark networks have proven to be challenges that bright networks must deal with.

Networks, as defined by Eilstrup-Sangiovanni and Jones, is a system in which actors are linked by enduring formal and informal relations and Walter Powell adds that this must be towards a common goal ("Neither Market nor Hierarchy: Network Forms of Organization"). Hierarchies, on the other hand, are characterized by a top-down system

as a mode of functioning. “What distinguishes networks from hierarchies is the capacity of lower-level units to have relationships with multiple higher-level centers as well as lateral links with units at the same organizational level. Networks are never managed by a single (central) authority”(Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening than Many Think, Page 11). See *figure 1.1* and *figure 1.2* for a visual interpretation of the differences between hierarchical and network structures. *Figure 1.1* shows the chain of command system that a hierarchy uses to disseminate power with a centralized leader-distributing top down power. *Figure 1.2* shows the horizontal decentralized structure of a network with different nodes coming together at different points with power distribution balancing among the nodes instead of stemming from one in particular.

Figure 1.1 Hierarchical Structures

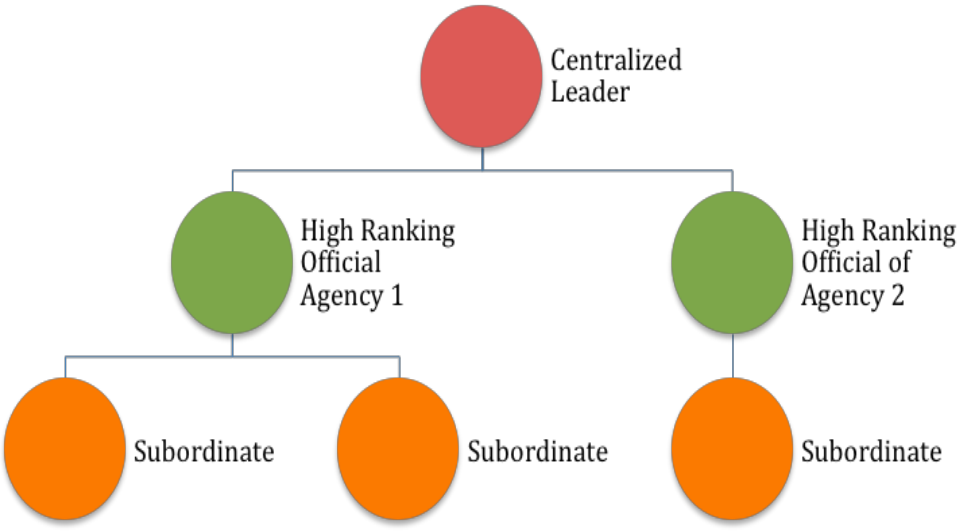
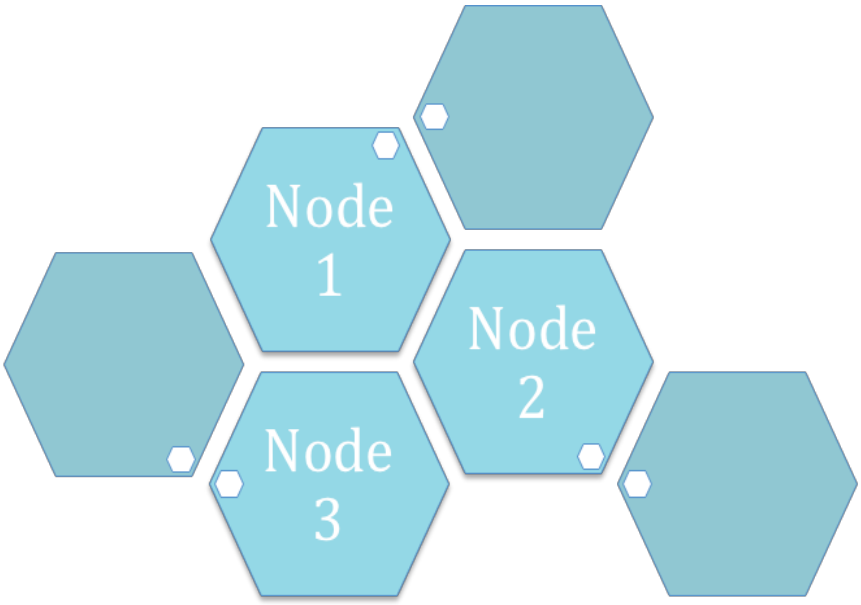


Figure 1.2. Network Structures



Dark networks are organizations that have common characteristics that are agreed upon by scholars including Eilstrup-Sangiovanni and Jones, and Milward Raab, ad Bakker who listed similarities which include a management style that is decentralized and horizontal in structure and is “covert and illegal” in nature. Dark Networks rely on government, police, and military instability in order to effectively function. Their intent might be economic gain, spread of an ideology or extremist view, or spread of a political perspective through criminal activities and possibly terror depending on the organization.

Bright networks are defined as overt networks that are legal and fight the existence of dark networks. (Milward & Raab, Page 34) These include legitimate state governments, intelligence organizations, think tanks, etc. The network of legal organizations is not as cohesive as those of their illegal counterparts because each state and organization has domestic pressures that may not be in line with each other, where as with dark networks they rally around the need to stay secret and untracked by bright networks.

Dark networks have advantages that make it hard for states to control and exterminate. This is not to say that ridding ourselves of dark networks is an impossible task; in order to do so, there needs to be a better understanding of their weaknesses structurally (as multiple scholars have discussed before me) but also in a global context and evaluating their actions as a reaction to the behaviors of bright networks. This next portion of the research will delve into the structural advantages and disadvantages of networks (not necessarily dark networks) in general before exploring how it might be interpreted in the global context.

Advantages

First, the nature of networks is very different from structures of many legitimate governments; where governments are usually hierarchical or at least have a clear division of power, dark networks survive by dividing power up among actors or nodes or "hubs" within their network. This makes it much more difficult for states to get rid of a dark network by simply destroying the top of the hierarchy. Dark networks have adapted from this form of vertical power, to a more flexible horizontal structure in which the most powerful nodes are extremely hard to detect, because power no longer derives from the top, but is balanced across nodes. Divvying up power in this way ensures the survival of the network even when a section is destroyed. Destroying one node no longer means eminent danger for dark networks. In a vertical structure of power, destroying one actor in the chain creates massive instability in the entire system, but for network organizations, getting rid of a node is a low cost result. Networks even get rid of nodes

internally if they are not producing the results they want. In more simpler terms, dark networks have learned from the mistake of putting all their eggs in one basket; they have made the strategy of cutting off the head of the snake in order to kill the whole obsolete.

States can no longer rely on disintegrating a dark network from the top as their primary method because the snake (dark networks) has many heads (nodes) and if you chop one off, another will grow in its place. Instead when they find a node, they do not get rid of it, they must use it to find other nodes like a puzzle, and then determine the best course of action in dealing with it. Networks are adaptable “compared to hierarchies, network boundaries are more easily re-definable and can adjust more rapidly to situational exigencies. As discussed, networks can "scale" to meet new requirements or needs and a relative lack of physical infrastructure also enables networks to relocate operations from one geographic area to another in response to changing constraints” (Eilstrup-Sangiovanni, Jones Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening than Many Think, 15).

Networks, compared to hierarchies, have the ability to expand quickly and efficiently.

> “They have the ability to grow by adding sideways links to new individuals or groups. In principle, a loose organizational structure allows networks to expand freely, integrating new nodes as necessary. If new requirements or problems arise, networks can adapt by adding new links to groups with relevant expertise. A networked structure also facilitates recruitment. Due to their dispersed, transnational structure, networks can tap into wider sets of resources such as

> diaspora populations, and local autonomy allows networks to tailor their message and activities to different communities, thereby increasing their support base."(Eilstrup-Sangiovanni, Jones Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening than Many Think, 14)

This mechanism allows dark networks to grow exponentially, increasing in size while also gaining new experts to fill gaps where needed. Flexibility to expand and diversify has made it increasingly more difficult for bright networks to find and manage dark networks; as a result, governments have put more resources towards uprooting these invasive underground networks, which aim to create instability and chaos.

Networks also communicate more rapidly than hierarchies tend to, allowing them faster reaction times and the ability to bounce back quicker. Their flat decentralized horizontal structure allows for the spread of information throughout the network without any obstacles getting in the way as they might if it were a vertical structure. Some of these obstacles include rank, bureaucracy, power limitations, etc. which tend to slow down the dissemination, processing, and reaction to information among an organization. Faster spread of information also allows for faster use of the information, especially in a horizontal structure, where there is no need to wait for approval from the top like in vertically structured organizations.

Disadvantages

Although networks have adapted to create a new flexible organizational system, there are some disadvantages that work against them. Although the spread of communication is quicker than that of a hierarchical system, the information, which is being distributed,

can oftentimes be unreliable or false in nature. While vertical systems have accountability for where information comes from, networks have a more fluid system with no real consequences for nodes or members who disseminate false information. This disadvantage could result in reactions under false pretenses that could threaten the safety of the entire organization.

Networks also suffer from excessive risk taking which results in mistakes and exposure to risk, which is unnecessary and dangerous to the organization. Networks have little accountability and a lack of a central decision maker; thus each node is somewhat independent and free to behave as they wish. Decentralization allows fluidity among the network, but also lacks a command system to regulate decision-making. Many decisions that are carried out independently by nodes are not completely thought out or reviewed, so they may be using resources wastefully, not helpful to the overall mission of the organization, or only provide short term benefits. Cohesiveness is hard to achieve in a network because there are many independent moving parts that do not respond to a centralized entity.

Another issue that many networks encounter is a lack of a common goal or target or overall unity. This is also a result of a lack of a centralized government which is crucial to creating a common rhetoric among an organization. A charismatic leader is often a rallying point for an organization, but most of the time networks that lack this often do not have a clear idea of what their purpose is. Without a sense of purpose, it is much easier for an organization to fall apart when external pressures are applied.

Characteristics of Dark Networks

By nature dark networks are illegal and covert and employ violence, terrorism, and criminal behavior to achieve their ends. As discussed earlier, networks utilize a flat or horizontal structure as a mode of operations and functioning; however dark networks are known to adapt from this completely flat structure to a more hybrid form, which uses both aspects from vertical hierarchical models and horizontal network models. This allows them to maintain the flexibility that a network provides while reinforcing the structure that a hierarchy provides within an organization. Hierarchical structures are too basic of a structure for such complex organizations that are trying to stay undetected; they fail when a chain is broken whereas networks are more flexible.

Dark networks inherently have a relationship with bright networks because covert organizations rely on instability within sectors of bright networks in order to function. The less control states and governments have over police, military, private sectors, enforcement of the law etc. the more control, territory, and resources these criminal organizations can usurp and utilize to expand their influence. Instability or preoccupation with other issues also means that the states have less time to go after these dark networks; Baker and Faulkner argue that “every secret organization has to solve a fundamental dilemma: how to stay secret and at the same time insure the necessary coordination and control of its members.” (Baker and Faulkner, 1993) If governments are distracted with bigger problems, they will not be able to focus their efforts on expelling covert organizations from their territories. Jorg and Milward explain that

> “Keeping up the pressure in as many countries as possible through concerted international collaboration is vital. When put under intense pressure from legitimate states, dark networks have to constantly worry about the security of their organizational structure, modes of communication, and so forth, so that fewer resources and less attention remain for their specific activity” (Jörg, Milward, Dark Networks as problems, 433)

Covert Networks are rational actors that behave in a way which brings the most benefits to the organizations while maintaining a low-cost system. This proves that dark networks are not irrational and only behave in ways that they do because they want to use violence or terrorism; this is completely false. The utilization of these criminal acts is a means to an end; these groups are benefitting from committing crimes even though that might seem counter intuitive. This might also mean that bright networks are providing some of these benefits. Dark networks use violence, terror, etc. as deliberate strategies to create instability, augment support, gain legitimacy, collect resources, and many more benefits that might be hidden internally within an organization.

Chapter 3: Relationship between Bright and Dark Networks

This chapter will first cover the complexities of the relationship specifically of bright and dark networks by analyzing their purpose, nature, motives, and goals as they pertain to each other and how they are reconciled to fighting covertly. This chapter will also discuss the boundaries of these two types of networks by examining where they overlap

in social, political, and economic spheres. The second major section in this chapter pertains to the difficulties that bright networks face in trying to combat dark networks at the international level. Since the main purpose of this research is to help experts combat these illicit organizations by providing them with more information, it is important to cover what difficulties bright networks are facing in eliminating these groups.

Overlapping Spheres between bright and dark networks

Since covert networks thrive as a result of chaos and disorder in the sphere of overt networks, and overt networks strive to eliminate covert networks; there is an inherent relationship between the two. Bright Networks and Dark Networks have the same goal for their organization and that is to stay relevant and survive. This is a source of tension for both because the existence of one inherently threatens the existence of the other. For one to venture into the sphere of another is when conflict occurs. Conflict is inevitable because both dark and bright networks need to operate at some level into the sphere of the other. For bright networks this need stems from the need to eliminate them and therefore collect intelligence on them, infiltrate them, and exterminate them. Bright network legitimacy is reliant on the perceived success of combating terrorist and criminal organizations. If they cannot succeed in doing this, then domestic audiences will start to question their necessity and that threatens the organization as a whole. On the other hand, dark networks must at times cross into bright network territory also to collect intelligence, in addition to gathering resources like recruits, weapons, food, civilian support, and more. Dark networks are not usually self-sufficient (unless their purpose is economic like drug cartels) and their income stream is limited; therefore they sometimes must venture into bright network economic territory in order to afford

survival. Sometimes dark networks can strike deals with bright networks that are struggling to operate effectively. Developing states that are weak and have high levels of corruption are most prone to this because they lack the power, resources, or legitimacy to provide government services to their people. For instance, corruption might cause their security apparatus to be inept, the government might not have the funds to provide housing or food stipends to the poor, and there is usually a high rate of unemployment among the population. All these factors make it easy for dark networks to take advantage of the situation as well as the civilians living in these states. In these circumstances demands surpass the ability of governments and there is room for organizations that are not part of the official government apparatus to operate. This may take the form of a vigilante security apparatus, a rebel group may recruit civilians who are struggling to make a living and find jobs, these groups can even function as para-governments, creating laws and enforcing them with violence and providing “justice”.

Bright networks make concessions to dark networks or co-operate with them if they begin to lose more than they are gaining by fighting them. It is only natural that overt and covert networks should overlap and share spheres in some situations because both dark and bright networks operate in the same territory and are fighting for control and power over that territory; as two rational actors, cooperation or complacency is at times considered the most beneficial option for a networks operating within the same region. For example, Hezbollah in Lebanon has “evolved significantly from its origins as a guerilla group in the early 1980s into a major political and military force” (Counter Extremism Project, 2019). The government realized that the group was growing in

popularity and was gaining resources that made them a real threat to their power; so they decided to tolerate the group and integrate them into their political, economic, social, and religious system. The Lebanese government and people have accepted this status because the government does not have the power or the resources to combat their growing involvement in Lebanese affairs. Complacency has also decreased the amount of violence because at this point, the two organizations are operating symbiotically and many now consider Hezbollah a legitimate force in Lebanon.

States will always do what is in their own best interest even if it is at the expense of other states. States that support (either directly or indirectly) dark networks outside their sphere of influence are getting benefits (which may or may not be available to states in that region) at little cost to them, although it might be at a high cost for states that are actively dealing with dark networks within their territory. This lack of solidarity among states puts weaker states, more prone to instability, at a higher risk of falling victim to dark networks that thrive on disorder. For example, The U.S. under Bill Clinton delayed their intervention in Rwanda when the genocide broke out in 1994. It is now proven that they knew the full extent of what was going on, but decided not to act because of the chaos that ensued when George H.W. Bush intervened in Somalia in 1992. The U.S. leadership, having no interests in Rwanda, decided not to act in the best interest of the state, but this inaction caused the suffering and death of hundreds of thousands of people.

International Difficulties in Fighting Dark Networks

A lack of agreement on what constitutes a dark network has created international tension and difficulties between states who may support these organizations and those that are actively fighting them. The term “dark networks” is relatively new, it is more known among specialists and researchers, and experts, but there is still a sense of murkiness surrounding the term. This is in part because there is a lack of international agreement on what is considered a dark network. For example, the U.S. has its list of terrorist organizations, the European Union has its own version of this with variations to the U.S. version, each state differs slightly in who it considers a dark network. Some might consider these organizations as political parties, or social organizations, or freedom fighters, etc. A lack of consensus at the international level can create obstacles when governments are trying to fight what they perceive as illegitimate covert illicit networks. The same situation is happening with the threat of terrorism, and indeed there is much overlap in dark networks and terrorist organizations (terrorist organizations are one of many forms of dark networks. Terrorism does not have a common international definition; each state has its own version of the meaning and each varies slightly. This is problematic in the sense that you cannot fight what you do not know and cannot define explicitly. This lack of definition points to the fact that there are still aspects of both of these organizations that are still not fully understood.

Gaps in understanding dark networks are mainly due to the covert and illicit nature of dark networks. Experts have been able to define and describe networks well because they had full access to study them because unlike dark networks, they are overt and modestly transparent. On the other hand, the innate nature of dark networks is covert

and illicit. Their primary goal is to outmaneuver bright networks and ensure they know as little about them as possible. That is the only viable way they can function; their purpose and goals are the polar opposite of that of legitimate governments and security services (most of the time, or at least theoretically). Therefore, it is more difficult for experts to come to a definite agreement of what they are because they collect information that is collected either covertly or from members who are caught, or eyewitnesses; both unreliable sources.

Chapter 4: Bright Network Behavior

This chapter will clarify what specific behaviors are compromising the success of bright networks in fighting dark networks. It has been divided into two sections; first behaviors of direct support and second, behaviors of indirect support for these organizations. This section was difficult to divide since you can sometimes make a case for one type of support to be placed in the opposite category. However, in order to perfectly separate the two, you would need to know the true motivations of bright networks when they behave in these ways. This can be very murky because often times, states do not want the international community to know their true intentions when they support (either directly or indirectly) dark networks. The way that this research separates the two categories is by how bright networks must interact with dark networks in order to support them. For example, if they interact with them directly or officially, it has been labeled as “direct” support; and if there is a third party or no direct contact with the network, then it has been labeled as “indirect” support. These categories are also labeled from most important forms of support to those that have fewer consequences.

This portion of research will serve to answer the questions posed in my introduction, which ask do states support dark networks and What specific behaviors are considered support.

Direct

Financial Support

The most direct and traceable form of sponsorship by bright networks of dark networks is monetary aid. Many dark networks "go out of business" because they no longer have the funds to pay members, under take operations, or provide supplies and resources. This is especially true for politically or religiously motivated organizations because their purpose is not to make profits (unlike the drug cartel or human trafficking industry) but to sell a message or overthrow a regime. These groups heavily rely on these corrupt funds from legitimate actors to function on a day-to-day basis. Bright networks that fund dark networks usually do so because they want something specific from them. For example, a bright network actor like a political figure could interact and fund a dark network if they wanted dugs from the drug cartel or a person from the sex trafficking organization. Another example might be a state funding a terrorist organization to create instability in another country or region. In this manner, bright networks are using the existence of an underground black market to receive benefits not available in the normal market. Bright networks also rely on these activities to be covert and under the table as to not bring attention to illegal activities from the international community.

Militarization

States will often use dark networks to fight proxy wars in various regions of the world. Major powers have supported dark networks (usually politically or religiously motivated) by providing them with weapons, equipment, training, money, and supplies. A historical example of this would be the Unites States, Saudi Arabia, and Pakistan's militarization of Afghan fighters (Mujahideen) in the proxy war against the Soviet Union in the 1970s. Subsequently after the end of the war, and as a result of an instable region, these fighters became radicalized and had the means to organize into a terrorist network, which had catastrophically effects in the region and around the globe. Bright networks have not learned from this lesson and continue to arm and support rebel groups in Syria and Yemen who have the potential to become a new prototype of Al Qaeda.

Legitimizing

Dark networks are illegitimate actors by definition, but sometimes they can grow to be more powerful, and therefore legitimate in the eyes of the domestic audience. An illicit organization can do this by becoming powerful from the bottom up by catering to the grass roots sector of society. This usually occurs in weak states where services do not meet the need of society by a large margin. Again, with the example of Lebanon, the government did not fulfill the demand at the domestic level; this left a gap where organizations like Hezbollah could insert themselves and supply these demands. This gained them legitimacy from the Lebanese people and therefore the government had to reconcile some of their power to them in order to stay in power at all. Anther way bright networks legitimize dark networks is by making them a concern at the domestic or international level. Doing this legitimizes their threat, their power, and their organization.

The simple act of officially recognizing these organizations gives them more power and authority over bright networks.

Indirect

Turning a Blind Eye

Research suggests that this is the most common type of support of dark networks because it requires no action to be taken and no issue to be acknowledged. The reasons that this is so prevalent, especially in weak states, is because bright network actors are gaining benefits from ignoring the problem; For example, they might receive bribes or pay offs, they might be endangering their safety, or they might be risking the displeasure of their domestic audience. The Russian Mafia is well known for paying off police officers and political figures in exchange for free operation in certain areas; this is also the case with the drug cartels in Mexico. Low wages in these states push state officials and security services to accept bribes as well fear for their own safety if they do not comply. In some states, where dark networks are more tolerated by the constituency, fighting against organizations will anger the people and create tension and instability in the country. For example, the United States has accused Pakistan of holding back information regarding the whereabouts of Osama Bin Laden. Although this has not been confirmed, there is speculation that Pakistan did turn a blind eye to Al Qaeda operations in their territory because the Pakistanis sympathized with the group and their cause. Turning Bin Laden over would have jeopardized the domestic atmosphere in Pakistan and that is a credible reason to ignore international pressure to provide intelligence.

Financial Support

This mode of providing support to illicit organizations can be done directly or indirectly. Indirectly providing financial support means that a bright network had an interaction with a third party who interacted directly with the dark network. This is usually by means of buying goods at a reduced price through that third party. The benefit for bright networks is receiving the goods at a cheaper rate than buying through the legitimate economy would have been. This could also include a state giving aid to another state and then that state which received the aid directly supports a dark network with that money. When these types of interactions occur is extremely difficult to assess if the bright network that indirectly supports a dark network did so knowing where their money would go, or was it a purposeful transaction with the intent of removing the blame (if caught) from themselves.

Chapter 5: Expectations

This section will cover my hypotheses that will be tested through my case studies later in this paper. These expectations are based off of previous knowledge and research into this topic of which I hope to shed light on through real historical cases. Below I state the hypothesis I have and then I explain why and how I have come to these conclusions. These expectations will also be discussed at length in each of my case studies and this portion serves as a set up to that section of my paper.

Hypothesis 1:

When states do not have the capacity to fight dark networks, they will be more willing to fund them if there are domestic and/or international benefits to gain.

Weak states are more susceptible to working with dark networks because of internal factors that make them less able to fight off these organizations. These factors include corruption in security services and political spheres, lack of resources and funds to fight insurgent networks, and lack of control over territory or populations. Keeping with our previous example of Hezbollah in Lebanon, we can see that the weakness of the state paved the path for Hezbollah to take root and gain popularity. Now Lebanon provides them with direct support by giving them some political authority by creating their own political party and tolerating their social, religious, and economic operations. Another example would be the drug cartels in Mexico; corruption in security services and political spheres has made it easier for these illicit organizations to run rampant in Mexico. Bribery, pay offs, black mail, and many more forms of corruption have become a normalized aspect of Mexican social, political, and economical affairs. The state has come to expect and profit off of these networks because they provide them with financial benefits that the state does not have the resources to provide for them.

States will also use dark networks if they fear an international or domestic threat to their power is gaining ground. For example, in 2013 riots broke out against Bashar Al Assad and his corrupt regime. He was afraid he would be overthrown like Saddam Hussein was. This threat to his regime pushed him to seek protection from rebels and foreign fighters. Throughout the Syrian Civil War he continually utilized ISIS and ISIL to fight

insurgencies and international militaries on his behalf even though it weakened his power and gave him less control over territory.

Hypothesis 2:

When pressured by outside states to stop funding dark networks, bright networks are more likely to use indirect support.

International leverage is an important aspect of international relations; leverage is a tool that all international players use in order to get what they want. This can be in many forms like doing favors, complying with international regulations/standards, or supporting policies at the international level, etc. when states put pressure on other states to either stop supporting dark networks and instead fight them, many states will put of the façade of complying but then switch their methods to indirect forms of support. This gives bright networks the best of both worlds; leverage for complying with international pressure, and continued benefits for indirectly supporting underground organizations.

Hypothesis 3:

States that have domestic pressure to aid dark networks, do so to seek to gain leverage and approval from constituents and to balance regional powers that may be considered threats.

This expectation builds off of the previous one; it states that one of the reasons states might continue to aid dark networks despite international pressure to not do so, is

because they are also balancing domestic pressure to be more lenient with dark networks. Often times, states must balance between what more powerful states want and what their citizens want; this can get complicated when the two do not align and even harder when both jeopardize a regime's power and stability. States also have to deal with regional powers that they may see as a threat. This makes supporting dark networks a more desirable form of behavior because it can help to destabilize other actors in the region and keep ethnic minorities in check and occupied. Combinations of international, regional, and domestic benefits come together to make supporting dark networks a rational and even smart decision for some states.

Hypothesis 4:

States that are receiving funds to fight dark networks are more likely to keep these networks alive in order to continue to receive these funds.

States that aid other states to fight dark networks might not realize that doing so causes the unintended consequence of creating a complicated complex in which states that receive aid to fight criminal organizations come to rely on this financial support and thus do not want to lose it. Therefore, they make sure the threat continues to exist by directly supporting it. The cycle continues to be perpetuated and dark networks continue to have a strong foothold in these regions. While the intentions are good on the part of the state giving aid, the inadvertent product is working against their well-placed intention. This is called moral hazard in political science and it is the risk of making a situation worse by interfering (even with good intentions). Typically, moral hazard is used to

describe perpetuating conflict, but the idea applies to this theory as well. The example below portrays how moral hazard is used in international relations to convey the risk of intervention in the midst of humanitarian crises.

> "The international community has sought to insure vulnerable groups against the risk of genocidal violence, as codified recently in The Responsibility to Protect. In so doing, however, it inadvertently has encouraged such groups to engage in the risky behavior of launching rebellions that may provoke genocidal retaliation" (Kuperman, 221).

Hypothesis 5:

Once states stop sponsoring dark networks in whatever capacity they are doing so, they will lose their sources of power, legitimacy, and support and eventually it will become too costly for them to operate in an illicit capacity and they will disintegrate.

Terrorist organizations are rational thinkers; this means that they operate according to a cost-benefit analysis. If the costs exceed the benefits, it is no longer rationale or feasible to sustain the illegal network. At this point in time, the benefits, which they procure, outweigh the costs of running their organizations. In order to make it more costly for them; states must cut off all avenues of support (either directly or indirectly benefiting dark networks) and slowly let them run out of resources until they are no longer able to operate at a loss. In order to accomplish this, states must combine intelligence, resources, and agree on a common goal in regards to dealing with dark networks.

Historically, piracy was an extensive dark network that states were struggling to combat at the time. While some states were using pirates to fight proxy battles, all legitimate actors were being harmed by their existence. As a result, states came together and decided to eradicate piracy all together.

> "Piracy ended when Western nations took concerted action against pi- rates and ceased using them for their own purposes, for example, sponsoring them to ravage the shipping of other nations" (Jörg, Milward, 416).

I believe the same thing must be done in order to eradicate dark networks now. While some states are benefitting from their existence, I think they are more costly at the international level and states must come together at the international level in order to fight them.

Chapter 6: Case Studies

The two case studies that will be focused on are Pakistan and its endorsement of the Taliban and Al Qaeda throughout recent history and the blood Diamonds in Africa and how legitimate governments, to gain financial benefits, used the corruption of the leader Charles Taylor for their own personal gain. Both these cases will bring up topics discussed previously in the expectations section and show how they can be applied to real case studies.

Pakistan, the Taliban, and Al-Qaeda

In the specific case studies of Pakistan and the Taliban it is expected that state leaders behaved in a way that was prioritizing their interests and power over the common good of the region and the international arena. Knowing the rationality of states, perception of benefits from either supporting dark networks or simply turning a blind eye to them and allow them to continue to operate will supersede international pressure to fight against dark networks.

Historical complexity:

By researching the historical, cultural, and ideological context of Pakistan and the region it is situated in, we can better understand the logic that is used for states in those regions to make decisions and why they behave the way they do at the international level.

Historically, Pakistan has been subjected to a politically unstable region. Their neighbor Afghanistan has been a major source of this instability; they are divided ethnically and religiously and have not had a stable government that Pakistan could communicate with or rely on. During the Soviet invasion in Afghanistan Pakistan supported the Mujahideen against the Soviets in their first effort to wield influence in the region. Since then, Pakistan has had a consistent role in the region. When the Taliban first took root in Afghanistan, Pakistan supported the organization.

> "Pakistan was an important regional player in the Afghan power game, and it had supported the Taliban movement to checkmate its regional rivals and keep itself in a position of greater influence than others" (Akhtar, 59)

However, in light of the events of September 11 and mounting international pressure to fight the war on terrorism, Pakistan decided to join the coalition to fight terrorism. They did this because continuing to support the Taliban would have brought upon them the wrath of the international community who supported ad sympathized with the United States after the attacks of September 11. However, Pakistan's domestic audience still sympathized with the Taliban.

> "Pro-Taliban feelings still run deep in Pakistan and well beyond the Pashtun territories. As such, the Taliban will remain an important force in the political process of Pakistan whatever shape it takes in the coming years" (Akhtar, 60)

Switching from Direct to Indirect support

At first, Pakistan was directly supporting the Taliban by legitimizing them. They did this by recognizing them as a real contender for the new government of Afghanistan. Pakistan claims they initially supported the Taliban because they seemed like a stable and coherent group, but once major powers like the United States and Saudi Arabia rejected them; Pakistan did the same. However, they did not completely stop supporting them they just did so under the table, so to speak. They used the strategy of turning a blind eye in order to allow the group, as well as Al Qaeda, to operate in their territories where Pakistani masses were more sympathetic of their presence.

Connection to Hypothesis

The Taliban has been present since they formed post Soviet invasion of Afghanistan in the 1970s. It is now 2019 and the Taliban still controls large expanses of Afghanistan.

There are many reasons for this, but a major factor is that it receives support from Afghanistan's neighbors: Pakistan. They allow these insurgents to hide along the bordering mountains of the two countries. International pressure has forced Pakistan to use indirect methods of support in order to balance pressure from both domestic and international actors.

At the domestic level, constituents support the Taliban in rural tribal areas where Pakistani government control is limited and weak. This supports the claims in hypotheses, 2 and 3 which state:

> *2. When pressured by outside states to stop funding dark networks, bright networks are more likely to use indirect support.*
>
> *3. States that have domestic pressure to aid dark networks, do so to seek to gain leverage and approval from constituents and to balance regional powers that may be considered threats.*

Furthermore, Pakistan has international and domestic benefits to gain by indirectly supporting the Taliban and Al Qaeda. Some motivations for Pakistan to support these illicit organizations according to Jones and his article Counterinsurgency in Afghanistan include to balance the power against India in the region and in Afghanistan, to gain leverage in Afghanistan by supporting instability, to keep a military front/presence in border areas near Afghanistan AND India where borders were once porous and weak, and to divide ethnic Pashtuns from uniting across Pakistan and Afghanistan. This can be applied to hypothesis 1, which states that:

When states do not have the capacity to fight dark networks, they will be more willing to fund them if there are domestic and/or international benefits to gain.

Pakistan has another motive to continue indirectly supporting the Taliban and Al Qaeda. They want to keep international leverage with the United States as well as keep the aid they are providing them with in order to fight terrorism. If terrorism were eliminated, then Pakistan would lose both its leverage and its financial support from the United States. This phenomenon is described in hypothesis 4 which says:

States that are receiving funds to fight dark networks are more likely to keep these networks alive in order to continue to receive these funds.

This issue is described as moral hazard, which is the unintended consequence of interference and aid. Insurgents border Pakistan and are threatening the stability of Afghanistan. Meanwhile, major powers offer training, weapons, and money to Pakistan to fight off the Taliban. In order to keep up this stream of income and legitimacy, Pakistan does not completely uproot the problem but rather allows it to occur at a low level so that they keep their international aid and so that their neighbors are always unstable and unable to compete or threaten them.

The Blood Diamonds in Africa

The "blood" or "conflict" diamonds in Africa was known to finance multiple international criminal organizations in the 1980s and 1990s. Blood diamonds are diamonds that are extracted and exported from Africa illegally in order to finance illegal organizations. This usually took the form of trading diamonds for arms and other resources that dark networks might need. Diamonds were the perfect good to launder and export because they were easy

to hide and cheap to export and very difficult to trace back to illegal organizations. Charles Taylor was a major actor in this illegal trading enterprise, making regional and international conflict a side business in which no one benefitted but him.

> Liberian president Charles Taylor, a supporter of the rebels in Sierra Leone, frequently purchased diamonds from the rebels and then resold them to gem-cutters as bona fide Liberian diamonds. Similar laundering occurs in Eastern European countries, where countries that are cash-strapped but loaded with weapons from the Cold War era are more than eager to accept and repack- age rough diamond (Wu, 7)

As the president of Liberia, Charles Taylor, would have been considered a legitimate actor of a bright network. Although in hindsight, he was a warlord who was charged for war crimes and sentenced to fifty years in prison. His direct support for dark Networks such as the RUF (Revolutionary United Front) perpetuated not only local African illegal organizations but also international ones like the Taliban, Al Qaeda, and many others like them.

> “The conflict diamond trade channels billions of dollars into black market economies turning it into easy money for terrorists whose cells are involved in a range of money making activities that include diamond trading."155 Other terrorist groups, such as Hamas and Hezbollah, have also bought African diamonds and sold them outside the continent, making a large profit and using it to buy arms. Hezbollah, specifically, "has funneled millions of dollars through the DRC to its organization. The ability of international terrorists to utilize a commodity such as conflict diamonds has awoken many in Europe and the West to the reality that the

> conflict diamond trade is not just Africa's problem, but is a far-reaching problem" (Hummel, 1158).

Charles Taylor became the leader of a dark network with the title of a bright network position.

> "After Taylor and other warlords overthrew the Doe regime and Taylor was elected president, Monrovia, the capitol, became a mecca for all types of dubious individuals seeking to extract Liberia's natural resources, sell guns and military hardware, and launder money for diamonds. Liberia under Taylor, like Afghanistan under the Taliban, was like a gang become a state-where the state itself is a gang, the law does not exist" (Berkeley, 15)

As Taylor's government became more and more like a dark network; he started to rely on the instability of the surrounding countries to keep his regime inconspicuous. As a result he was involved in several civil wars in countries like Sierra Leone, the Democratic Republic, and Liberia and was the main financier of weapons, equipment, and diamonds that flowed straight into conflict zones across Africa.

Many countries bought these blood diamonds from Liberia boosting dark networks economies across the globe. This form of indirect support caused global consequences like the attacks of September 11, multiple bombings, profit on human rights violations, thousands of civilian casualties, civil wars in Africa and many more. When the United Nations came together along with the United States, the United Kingdom, and many other states that have major demands in diamonds, the international community was able to put

restrictions and laws in place to enormously decrease the sale of these illegal diamonds by bright networks. 20% of diamond sales used to come out of the illegal diamond economy in Africa. Now, since these restrictions have been put in place and states have been working together to ensure diamonds come from legal sources, only 1% of diamond sales come from illegal sources. This historical event helps to clarify hypothesis 5 in this research paper, which states that:

> *Once states stop sponsoring dark networks in whatever capacity they are doing so, they will lose their sources of power, legitimacy, and support and eventually it will become too costly for them to operate in an illicit capacity and they will disintegrate.*

This method can be applied not only to blood diamonds in Africa but also to other dark networks and this case study can be used as evidence that cutting off resources from legitimate actors will make illicit operations too costly and force these groups to stop their illegal behavior.

Conclusion

This study has brought to light the way that dark networks and bright networks interact with each other and when these interactions result in bright networks supporting dark networks. This support may not necessarily be direct support, in fact in the case of Liberia and the blood diamonds, many corporations and the international community in general could not tell what diamonds were being used in a corrupt manner and which were legitimate. This resulted in the financial support of dozens of illicit organizations across the globe. Other legitimate governments, like in the case of Pakistan, indirectly

support dark networks knowingly by turning a blind eye to their operations. Pakistan did this by allowing terrorist groups like Al Qaeda and the Taliban to set up safe havens along the Afghan-Pakistan border. This benefitted Pakistan because they were receiving aid from the United States in order to fight these groups. Domestic pressure to allow these groups to operate in Pakistan (especially in the rural areas with little centralized control) also pushed them to turn a blind eye even though they were also balancing international pressure to fight the war on terrorism. By applying these hypotheses to real cases we can appreciate the complexity of the relationship between domestic and international pressure when it comes to dealing with dark networks. Both of the cases brought up in this research supports the hypotheses posed previously and gives more context to how and why bright networks might support dark networks.

For future research on this topic, it would be interesting to continue to explore the complexities of dark networks further by looking at more case studies. It would be beneficial to juxtapose economically motivated dark networks (like the drug cartels or human trafficking groups) and politically and religiously motivated dark networks. The two groups have different goals, tactics, and mentalities and this might affect how they behave with bright networks and with each other.

Overall, dark networks are still need to be studied further, but difficulties arise by the covert nature of these networks and the complex relationships that have yet to be explored with bright networks.

Works Cited

Akhtar, Nasreen. “PAKISTAN, AFGHANISTAN, AND THE TALIBAN.” International Journal on World Peace, vol. 25, no. 4, 2008, pp. 49–73. JSTOR, www.jstor.org/stable/20752859.

Bakker, René M., Milward, Brinton, Raab, Jorg. “A Preliminary Theory of Dark Network Resilience.” *Journal of Policy Analysis and Management*, vol. 31, no. 1, 2012, pp. 33–62. www.jstor.org/stable/41429257.

Baker, Wayne E., and Robert R. Faulkner. 1993. The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. American Sociological Review 58.

Berkeley, Bill. 2001. The graves are not yet full: Race, tribe, and power in the heart of Africa. New York: Basic Books.

“Chapter 1. Country Reports: South and Central Asia.” U.S. Department of State, U.S. Department of State, www.state.gov/j/ct/rls/crt/2017/282845.htm#PAKISTAN.

“COUNTERTERRORISM SPENDING: Protecting America While Promoting Efficiencies and AccountabilityStimson Center, 2 May 2019, https://www.stimson.org/sites/default/files/file-attachments/CT_Spending_Report_0.pdf

Eilstrup-Sangiovanni, Mette, and Culvert Jones. “Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening than Many Think.” *International Security*, vol. 33, no. 2, 2008, pp. 7–44. *JSTOR*, JSTOR, www.jstor.org/stable/40207130.

“Hezbollah's Influence in Lebanon.” Counter Extremism Project, 31 Oct. 2018, www.counterextremism.com/hezbollah-in-lebanon.

Hummel, Joseph. “Diamonds Are a Smuggler's Best Friend: Regulation, Economics, and Enforcement in the Global Effort to Curb the Trade in Conflict Diamonds.” *The International Lawyer*, vol. 41, no. 4, 2007, pp. 1145–1169. *JSTOR*, www.jstor.org/stable/40707834.

Jones, Seth G. “Insurgents and Their Support Network.” Counterinsurgency in Afghanistan: RAND Counterinsurgency Study--Volume 4, RAND Corporation, Santa Monica, CA; Arlington, VA; Pittsburgh, PA, 2008, pp. 54–61. JSTOR, www.jstor.org/stable/10.7249/mg595osd.12.

Kuperman, Alan J. “Mitigating the Moral Hazard of Humanitarian Intervention: Lessons from Economics.” Global Governance, vol. 14, no. 2, 2008, pp. 219–240. JSTOR, www.jstor.org/stable/27800703.

Raab, Jörg, and H. Brinton Milward. “Dark Networks as Problems.” *Journal of Public Administration Research and Theory: J-PART*, vol. 13, no. 4, 2003, pp. 413–439. *JSTOR*, JSTOR, www.jstor.org/stable/3525656.

Sinai, Joshua, et al. “Perspectives on Terrorism.” *Perspectives on Terrorism*, vol. 10, no. 2, 2016, pp. 104–104. *JSTOR*, JSTOR, www.jstor.org/stable/26297558.

Walter W. Powell, "Neither Market nor Hierarchy: Network Forms of Organization” Research in Organizational Behavior, Vol. 12 (1990), pp. 295-3

WU, STEVEN. “Dying for Diamonds: Diamonds, Africa, and War.” *Harvard International Review*, vol. 22, no. 4, 2001, pp. 6–7. *JSTOR*, www.jstor.org/stable/42764061.