Mapping Security:
A Network Analysis

by

Darryl MacPherson

Submitted in partial fulfillment of the requirements
for the degree of Master of Arts

at

Dalhousie University
Halifax, Nova Scotia
March 2006

Your file Votre référence
ISBN: 978-0-494-16518-8
Our file Notre référence
ISBN: 978-0-494-16518-8

DALHOUSIE UNIVERSITY

To comply with the Canadian Privacy Act the National Library of Canada has requested that the following pages be removed from this copy of the thesis:

Preliminary Pages
- Examiners Signature Page (pii)
- Dalhousie Library Copyright Agreement (piii)

Appendices
- Copyright Releases (if applicable)

Dedication

In Loving Memory of Edith Odessa MacPherson - My Mother. She left us too early. It is my sincere hope that she would be as proud of me now, as I have always been of her. God Bless you Mom.

TABLE OF CONTENTS

List of Tables

List of Figures

Abstract

The terrorist attack of 9/11 has created and/ or accelerated increased pressure to change the manner in which traditional security and policing organizations are structured and behave. The "network" argument posits that due to the unique nature of security threats existing today, security and policing have become more flexible, fluid and responsive, thus, differing from previous static, fixed and insular traditional approaches.

This research clarifies our understanding of a local security and policing network by a). Describing their unique nature and b). Examining their network qualities and characteristics. It addresses more general developments in late modern policing and security as well as developments in local security networks with respect to the pluralization of policing responsibilities and command structure.

This research suggests that transitions in organizational and operational practices are occurring, but are still in the early stages of development. It may be that the Theory of Networks will need to be redefined by the more complex realities of organizational limits in the real world of security agencies, taking into consideration the complex and changing mandates and core societal values.

List of Abbreviations and Symbols Used

CCG	Canada Coast Guard
CBSA	Canada Border Service Agency
CCRA	Canada Customs and Revenue Agency
CFIA	Canadian Food Inspection Agency
CFNCIU	Canadian Forces National Counter Intelligence Unit
CROPS	Criminal Operations Officer
CSIS	Canadian Security Intelligence Service
CIC	Citizenship and Immigration Canada
CISC	Criminal Intelligence Service Canada
CISNS	Criminal Intelligence Service Nova Scotia
CMA	Canada Marine Act
DFO	Department of Fisheries and Oceans
DND	Department of National Defence
HC	Health Canada
HPA	Halifax Port Authority
HRM	Halifax Regional Municipality
HRP	Halifax Regional Police
IBET	Integrated Border Enforcement Team
IJMT	Integrated Joint Management Team
I & P	Immigration and Passport
IRPA	Immigration and Refugee Protection Act
ISPF	International Shipping and Port Facilities
JFO	Joint Force Operation
L & F	Lands & Forrest
MSOC	Marine Security Operations Centre
MOU	Memorandums Of Understanding
MTSA	Marine Transportation Security Act
MTSR	Marine Transportation Security Regulations
NCO	Non-Commissioned Officer
NCO i/c	Non-Commissioned Officer in charge
NPET	National Ports Enforcement Team
NSIS	National Security Investigation Section
PAL	Provincial Air Lines
PP	Passport
PSEPC	Public Safety and Emergency Preparedness Canada
RCMP	Royal Canadian Mounted Police
SCIS	Secure Criminal Information System
SLA	Service Level Agreement
TAG	Threat Assessment Group
TC	Transport Canada
USC	United States Customs
USCG	United States Coast Guard
VACIS	Vehicle and Cargo Inspection System

Acknowledgements

There are many people to thank within the department. First and foremost, I would like to thank Dr. Chris Murphy for his support, guidance and patience throughout this academic endeavor. I have admired Dr. Jim Stolzman whose approachability was fundamentally responsible for recruiting me into the Sociology program. Special thanks goes to Dr. Don Clairmont whose dedication, keen wit and friendship provided the motivation to see me through this experience. I would like to thank Dr. Julian Hermida and Dr. Winston Barnwell for their insight, time and friendship. I would also like to take this occasion to acknowledge Mary Morash-Watts and Lori Vaughan. Their technical assistance and ever-present welcoming demeanor was always appreciated.

This research could not have been conducted without the cooperation, time and assistance of those who's task it is to protect the security and integrity of Canada. As such, I express my sincere gratitude to Staff Sergeant Murray Urqhart of the Royal Canadian Mounted Police for providing me with the initial contacts required to begin this journey. Most importantly, my most sincere appreciation is extended to those practitioners who opened their doors and shared their time and knowledge. Their candor and honesty has been instrumental in providing a concrete basis for increasing our understanding of security networks. They have contributed to the building of trust between the world of academia and that of the practitioner.

CHAPTER 1

INTRODUCTION: THEORY AND METHODOLOGY

The tragic events of September 11, 2001 have generated an expanded role for police and intelligence agencies throughout the world. Governments have been required to respond effectively to increasingly sophisticated criminal and terrorist networks. The war on terrorism is not one against an identifiable and tangible country, region or religion, but rather with a foe Urry (2002) describes as a "liquid modernity." It is a conflict based on competing ideologies and philosophies composed of dimensions not easily definable. While terrorism is not a new phenomenon, the ability for terrorist activities to transcend state or geographic boundaries has until now been limited. Global actors have challenged North American complacency resulting from geographical isolation and no significant historical threats to our collective security. These terrorist networks

> Roam the globe, possessing the power of rapid movement, across, over and under many apparent regions, disappearing and then reappearing, transmuting their form, cropping up like the islands of an archipelago, unexpectedly and chaotically (Urry, 2002, 65).

This newly developing threat has motivated the global community, including Canada to expand its security efforts through the creation of new agencies and expansion of responsibilities for existing security and policing entities. The composition and operations of this new and expanding security and policing apparatus in Canada operates in a fashion, remaining ubiquitous, yet also obscure. This new security and policing "assemblage" has been described as shifting from a hierarchical structure of traditional organizations whereby information, activities and governance flows in a vertical manner, to new "nodal networks," whereby relationships and information is characterized by a lateral flow (Castells, 2000a and b; Shearing and Wood, 2003a). This organizational

response represents not only a change in organizational structure and interaction, but also an extension and expansion of state power.

The terrorist attack of 9/11 has created and/ or accelerated increased pressure to change the manner in which traditional security and policing organizations are structured and behave. The "network" argument posits that due to the unique nature of security threats existing today, security and policing have become more flexible, fluid and responsive, thus, differing from previous static, fixed and insular traditional approaches. This thesis is an attempt to describe and explain the operations of a functioning local security network as portrayed by participants within this network.

This research will attempt to clarify our understanding of a local security and policing network by a). Describing their unique nature and b). Examining their network qualities and characteristics. By doing this, it will be possible to develop a better understanding as to how this new mode of security organization actually works, how they are organized differently, their operational advantages and disadvantages and examine consequences for security governance and accountability. This will provide an empirical exploration and analysis of a "local security network" that has emerged post 9/11 and an empirical basis for a grounded theoretical analysis. Finally, it will shed some light on more general developments in late modern policing and security and of developments in local security networks with respect to the pluralization of policing responsibilities and command structure. These are essential issues given the shifting nature of late modern security and policing, which to date, both empirically and to a lesser extent, theoretically remain largely unexplored. In an open and democratic society greater transparency on

issues of such importance should be researched whenever possible and not left to mere speculation or theorizing.

Theoretical Background

Policing Risk and Security

"Policing" rather than the police more accurately portrays current trends indicative of network societies – fragmentation and coalitions that extend beyond traditional perceptions associated with policing (Perrucci and Potter, 1989). Traditionally, the term 'policing' has been limited to the enforcement capacity of police organizations entrusted to maintain the peace in a reactive manner and provide law enforcement activities to control crime. For the purposes of this case study I have extended the term policing to include any public agency that has a designated role in the preservation of national security either through enforcement, intelligence or some other policing capacity.

Much has been explored with respect to the "elimination, shifting, sharing and privatizing" of policing responsibilities (Shearing, 1996; Murphy, 1998; Shearing and Wood,. 2003b; Crawford and Lister, 2003; Bayley and Shearing, 2001; Hermer *et al.*, 2002). An era of postmodern policing has emerged, which is marked by the decentralization and privatization of governing responsibilities (Johnston, 1992). Our traditional understandings of policing parameters have undergone a period of deconstruction whereby a multi-tiered re-conceptualization of policing responsibilities is required. Murphy (1998), has isolated the inherent characteristics in this postmodern transformation; (a) the restructuring and relocation of policing authority and responsibility, (b) the reconceptualization (*sic*) and commodification (*sic*) of public

policing, and (c) the economic and ideological redistribution and rationalization of public and private policing services (2)."

Policing strategies in late modern societies can best be described as shifting from a reactive to a proactive model. This new actuarial model (Ericson and Haggarty, 1997) is commonly referred to as "risk management" and is conceptualized by many terms, including, "risk assessment," "risk analysis," "intelligence led policing" etc. The term essentially implies that "as society has become more fragmented the focus of police work has shifted from traditional modes of reactive crime control and order maintenance towards the proactive provision of security through surveillance technologies designed to identify, predict and manage risks" (Ericson & Haggarty, 1997, xi). This police initiated and preventative model represents a "targeted approach" stressing the identification, analysis and management of problems or risks stemming from people activities or areas (Maguire, 2000).

Gallie (1956) argued that some terms in social theory escape agreed upon definitions, referring to them as "contested concepts." The term "security" epitomizes this analysis, as it is broad, unclear and multifaceted to such an extent that it eludes definition. Security can be conceptualized in the abstract as being subjective or objective (Zedner, 2002). In most operational situations security is defined by the organization and is loosely seen as a threat of some nature, deemed to be in their agencies jurisdiction. Thus, the prevention of threats to national security resides in the jurisdiction of government organizations; therefore, such threats are defined by these organizations. Such a designation is also dependent upon time and space. Acharya (2002) argues, "security in its barest essence

involves reducing vulnerability to threats" (12). Zedner (2002) expands on this by suggesting:

> First, [security] is the condition of being without threat: the hypothetical state of absolute security. Secondly, it is defined by the neutralization of threats: the state of 'being protected from'. Thirdly, it is a form of avoidance or non-exposure to danger (64).

There are many schools of thought respecting the concept of security. Buzan (1991) adheres to the Copenhagen School, focusing on military, political, economic, societal and ecological security. Constructivist security studies either see security as socially constructed, thus "achievable through community rather than through power" or alternatively, that actors who respond to cultural factors define national security interests (Smith, 2002, 3-4). Critical security studies direct their attentions to one of two prevailing veins of thought: (1) focus on "individuals, community and identity," or (2) the "goal of human emancipation" (Smith, 2002, 4; Krause and Williams, 1996, 1997; Booth, 1991). Rounding off this list of conceptual approaches are Feminist (Smith, 2002), Post-structuralist (Klein, 1994; Campbell, 1992) *and* Human security studies (Smith, 2002; Alkire, 2002).

Acharya (2002) suggests, prior to the events of 9/11, security had been based on anticipated threats to the environment, refugees, migration and human rights abuses (23). Perhaps this was the result of complacency on behalf of an otherwise unscathed sense of security existing in the Americas. However, the events of that fateful day re-ignited fears previously associated with a cold war mentality.

Synonymous with the concept of risk assessment, in the context of this analysis, the term security will be limited to an institutional response to an intentional threat to national security emanating from threats of domestic, political, religious or ideological

extremism. Dupont (2004, 77) argues the "governance of security is underpinned by a new risk mentality that adds a layer to the more established punitive mentality" (also see Garland, 2001). Furthermore, he articulates this "future – oriented rationality is focused on the prevention and reduction of risk" (2004, 78).

Distinction is necessary as some of the agencies involved in my research perform a function with respect to many manifestations of threats to security. For this reason, the scope of these threats will exclude natural disasters, accidental catastrophic events or the outbreak of an otherwise naturally occurring threat to public safety in the form of potential pandemics or epidemics as experienced during the outbreak of severe acute respiratory syndrome (SARS) in the summer of 2003. While the concept of "national security is closely linked to both personal and international security, [threats to national security by means of terrorism have a greater capacity to] undermine the security of the state or society" (Privy, 2004, 3). Security agencies must practice due vigilance as "security is an inherently relational concept: provision for it must be endlessly tested both against the latest challenge to its attainment and its vulnerability to that particular challenge" (Freedman, 1992, 732).

The Organization of Policing and Security: Traditional v. Network Models

When considering the organizational dynamics of post modern policing and security efforts there are essentially two organizational approaches of relevance for this study: a) The traditional (Weberian) Bureaucratic model of formal organizations and b) The modern "network" model of organizational integration. Table 1.1 summarizes the comparative characteristics attributed each model.

Table 1.1: Network and Traditional Bureaucratic Characteristic

Traditional	Network
Hierarchical	Lateral
Formal	Informal
Centralized	Decentralized
Insular	Open
Rigid	Flexible
Rational	Lacks Leadership

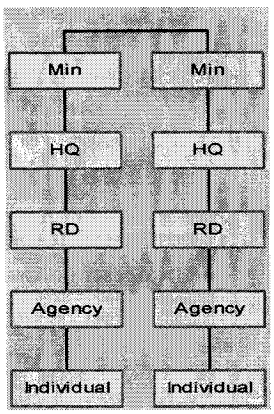
The Traditional Bureaucratic Organizational Model

Bureaucratic models of government base their legitimacy on the Weberian concept of "rational legal authority." This principle is predicated by the assertion that power and authority is legitimated through "some coherent system of laws or rules stemming from an overall system of administration" (Mansfield, 1973, 477). In accordance with the fundamental Weberian principles of this style of authority, administration and procedures are based on, and proscribed by a predetermined and fixed set of "constraints" set out in the distribution of policies and "abstract rules" (Mansfield, 1973).

Max Weber's bureaucratic model hinges on six (6) basic underlying principles. First, Weber contended that bureaucracies were composed of "fixed and official jurisdictional areas, which are generally ordered by rules." Second, he suggested organizations were characterized by a strict hierarchical system of authority (See Figure 1.1). Thirdly, administration is based on written documents known as rules. Fourth, management presupposes thorough and expert training. Fifth, bureaucratic activity is a full-time occupation. Lastly, the management of a bureaucracy follows general rules which are more or less exhaustive, and which can be learned (Weber, 1946).

Figure 1.1: The Hierarchical Bureaucratic Model

Key: Chain of Command
Min = Minister
HQ = Head Quarters
RD = Regional Director
Agency
Individual



This description of the bureaucratic model should not confine or limit our understanding of bureaucracies. The more centralized a bureaucracy, the more formalized activities will be. However, inherent in this cumbersome apparatus on a macro scale, it could also be contended traditional bureaucratic models are much more likely to be decentralized to a certain extent insofar as a degree of leeway may exist for satellite agencies. The creation of rules emanating from the central level functions in such a fashion as to limit the day – to – day activities and authority to make decisions of these satellites (Farrell & Morris, 2003). This arrangement solidifies and adheres to the legitimacy of the centralized administrative apparatus, as it remains these central departments who have been entrusted to conduct these given tasks on behalf of the populous under this means of authority.

Bureaucratic organizations are characterized by a highly **rational** arrangement and are arguably considered to represent a model of efficiency and means of production. However, this meritocratic bureaucratic model is also indicative of a mechanism characterized by excessive red tape, repetition and lack of creativity. This combination of features results in a **rigidity**, which is difficult to overcome. Bureaucratic organizations are criticized for being too centralized; too bureaucratic and inflexible; and too territorial

and **insular**. By creating an island onto themselves they are better able to protect their own interests, but are less open and by default, less conducive to cooperative and collaborative efforts in achieving common objectives. Such a position solidifies the respective agencies "turf" as intelligence remains in the control of this isolated agency. The **hierarchical** manner in which such mechanisms are required to report and disseminate information also represent impediments to efficient, effective and timely responses to emerging acute security threats. Bureaucracies are dependent on **formal** communication and decision-making processes, whereby intelligence and initiatives must first pass through a succession of senior political and organizational officials via written requests. Concerns as to whether this "lumbering" bureaucratic model is able to adapt to the nimbleness of emerging security threats are pervasive among national security circles. Therefore, new, innovative, effective, efficient and proactive approaches are required to address the emerging threats confronting security agencies in a postmodern era.

The "Network" Model of Organization

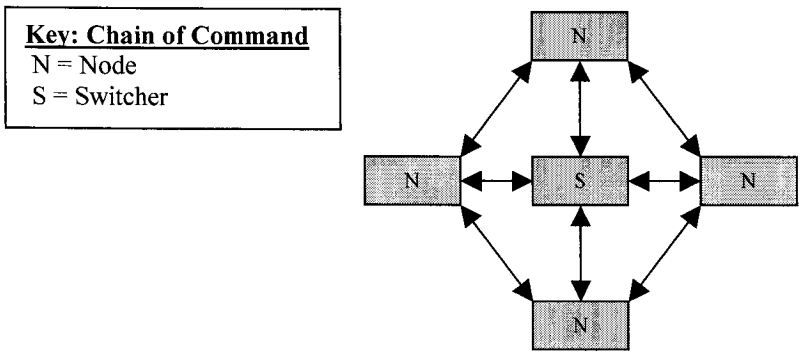
New commitments and security demands have forced conventional organizations to adapt in kind to the evolving threat matrix. Shifting terrorist modus operandi and organizational structures have enabled them to transcend jurisdictional boundaries with relative ease. The irony of terrorism is the fact that terrorists utilize the exact mechanisms used by the capitalist system to expand their interests as well as to extinguish the threat of terrorism. Kahn (2001) noted that "globalization as a process was facilitated by the liberalization of transborder (*sic*) transactions by the dilution of sovereignty. Globalization is essentially a measure of the ease with which, labor, ideas, capital,

technology and profits can move across borders with minimal governmental interference"(1). By default, these attributes of globalization extend to the proliferation of terrorist activities. The expansive network of global resources available to terrorist activities range from cargo boxes entering the ports of receiving nations to airline delivery to cyberspace and other technologies utilized by neo-liberal capitalism. Der Derian (2001) noted:

> Al Qaeda members reportedly used encrypted email to communicate; stenography to hide encoded messages in web images ...; Kinco's and public library computers to send messages; underground banking networks called hawala to transfer untraceable funds; 24/7 cable networks like al-Jazeera and CNN to get the word out and, in their preparations for 9-11, a host of other information technologies like rented cell phones, online travel agencies, and flight simulators....(par 29).

It is clear that the terrorist capacity to capitalize on readily accessible resources has not been stymied by traditional security and policing mechanisms. Thus, this posited organizational transformation, which is suggested to be taking place within the security and policing environment is characterized by a shift in the sharing of information away from the traditional hierarchical fashion consistent with bureaucracies to a networked approach, whereby information is distributed in a lateral more direct means to interconnected "nodes" or "routing points" (Lebkowski, 2000) within a particular network (Figure 1.2). The basic function of networks is to create and maintain linkages and interactions among member nodes. Castells (2000a) suggests among this composition of nodes one or more might possess more influence and power. As such these primary nodes are often referred to as "switchers." Switchers epitomize the factor of power distribution within the network.

Figure 1.2: The Network Model.



The power dynamics inherent within the network phenomenon distinguishes itself characteristically from the traditional bureaucratic model. One of the fundamental attributes of a network approach to governance resides in the "binary process" (Castells, 2000a) of inclusion or exclusion existing between relationships among individual nodes. This innate property allows networks to function in tandem on occasions whereby one node fails to contribute to the "collective capital" (Shearing and Wood, 2003a) of the network by ceasing to effectively perform its mandated task. The result is the absorption of that task by another node in what Castells (2000a, 17) coined as an "automated network" fashion.

It is argued power and influence within this assemblage of nodes appears to be unequally distributed as only certain nodes have the capacity to exploit the opportunities this form of governance yields (Dupont, 2004). Dupont suggests:

> The internal and external dynamics of networks are primarily determined by a contest among actors for dominant or central positions in order to maximize the benefits and minimize the risks associated with their participation. Networks are not egalitarian social structures, and some members are quite powerful while others are barely capable of maintaining their connections. These simultaneous relations of power and cooperation determine the existence and functioning of security networks as much as external circumstances and constraints (84).

The resulting power and influence within this community of nodes is derived from several factors including membership in other networks, the size of the node, jurisdictional considerations and whether or not the node is an aforementioned switcher.

As with any organizational model, networks have inherent advantages, disadvantages and problems, which differ from the aforementioned disadvantages as they have the potential for resolution. Proponents of the network model herald the network capacity to focus on local knowledge expand without limits, manifest the ability to be **flexible** and adaptable. Those within the network would also benefit from the inherent ability to distribute responsibility, resources and uncertainty more evenly across the nodal members. That is to say, the pluralization and proliferation of the security initiative accounts for an increase of agencies sharing responsibility for the overall security effort, sharing resources dedicated to that effort and sharing in the degree of uncertainty regarding direction and functionality.

The success of networks hinges on the **informal** interconnectedness within the nodal network. Rather than conducting operations via a chain and command approach, nodes distribute information **laterally** through routing points. This newly developing post modern security and policing model allows an "integrated" response to national security and risk management. It is **decentralized** and permits the wide distribution of information by avoiding the necessity for clearance and approval of senior officials. By default, the barriers previously indicative of traditional bureaucratic models are dismantled, thereby allowing for greater interconnectedness **openness** and thus access to information.

Summary

There are two separate and distinct organizational models when considering the present security and policing initiative, 1) Network model of organizational integration and 2) Traditional Weberian bureaucratic model of formal police and security organizations. Largely due to the evolutionary and revolutionary capacity of the present threat matrix to security, it is incumbent upon various government and national security agencies to act in a preemptive fashion as to curtail the resolve of such threats to Canadian national security. It has been suggested at the center of this response is a mechanism engineered in such a fashion that it resembles the core characteristics attributed network models. Such an approach would seem in order given the need to respond in kind and effectively to existing and evolving threats. To date, no empirical evidence exists that can either verify or debunk such a claim. Hopefully, this case study of a local security and policing apparatus will serve to provide some insight into this discourse.

CHAPTER 2:

METHODOLOGY

This research is an exploration of an emerging local security and policing network. The purpose is to describe and document the nature of this new environment and explore its unique organizational and operational properties by "mapping" this new security and policing network at the local level and describing the respective security functions as well as the networked relationships as identified by those inhabiting the network. Methods employed throughout this study were largely qualitative in nature. Recognizing the sensitive nature of the subject and the occupations of the participants, every effort was made to accommodate their schedule and preferred venue for conducting the interviews.

This research took on the form of semi – structured interviews, comprised of four distinct subject areas for analysis: 1) Individual institutional characteristics, 2) organizational and operational networked characteristics, 3) governance of this effort and 4) the advantages / disadvantages associated with the response. Throughout the interview guide questions were formulated in both open and closed styles. In some instances a Likert scale was developed to codify answers. This research design allowed respondents to introduce concepts not considered in the literature and then further expanded on these concepts in a qualitative fashion. This interview methodology resulted in providing data for both qualitative and quantitative analysis.

The first section focused on individual security and policing agencies, thus was primarily descriptive. This section encompasses three general subsections dedicated to individual agency mandates, organizational structure and subsequent corresponding operational activities. The second section of the interview guide expands upon the basic

individual organizational and operational components outlined in the previous section by exploring "relationships" between the respondent agencies. The purpose of this particular line of research is based on arguments concerning the nature of networks and was designed to assess agency status and influence in the overall national security apparatus. The third section of the guide had two separate and distinct subsections. The first sub-section was intended to determine the role of senior political and organizational actors in determining needs and responsibilities. The second sub-section, was designed to ascertain how those at the operational level believed the national security network will and should evolve in an effort to maximize the efficiency of this evolving contextual relationship. The fourth and final section was designed to ascertain whether or not the advantages, disadvantages and problems theoretically attributed networks and if in fact this assemblage operates as a network as is defined by many academics, are true to form.

Research Sample

In conducting the recruitment process I utilized "snowball sampling." The catalyst in this selection process involved approaching my former Supervisor within the Royal Canadian Mounted Police (with which I am no longer affiliated) and enquiring about persons I might be able to contact should I wish to conduct research in this field. These requests lead to one contact in the Immigration and Passport Section of the RCMP. From this point on I was able to network and develop a list of persons and agencies that might be interested in assisting me in my research. I also employed a second means of developing my list of perspective participants at a conference I attended on terrorism and organized crime hosted at the University of New Brunswick (Fredericton Campus). Once

again, a networking strategy was utilized. This networking approach was instrumental in the development of my research population.

Sampling

The final sample group was not selected on a random basis, but consisted of a representative portion of a local security network. Certain agencies and sectors were not included in this study due to the inability to obtain cooperation from these agencies. The lack of cooperation was attributed to time constraints from some agencies within the aviation sector and the absence of a response (either affirmative or negative) to requests for inclusion from the Canadian Security Intelligence Service (CSIS).[1] While it would have been ideal to have a representative from these respective agencies included in this case study, responses from the participating agencies would not have changed. In addition, the sample respondents represent a significant proportion of the key actors in the local network encompassing an equally significant representation of national security mandates. The tasks performed by participating sample agencies parallel those not represented in this study; therefore, the results would not have been altered significantly. For example, the absence of the Canadian Security Intelligence Service does not impact the validity of these findings as the inclusion of the National Security Intelligence Service and its respective mandate shares many similarities with those of CSIS.

In and of itself, the sample is composed of central figures composing the local security response as it evolves on a day-to-day basis. Due to the nature of the beast and the inherent necessity to guard against the possible compromising of security and

policing efforts, this sample represents an unprecedented distribution of agencies. All but two key agencies were involved and of these two, the operational characteristics of one (CSIS) can be related to by way of the operational necessities of another (NSIS).

Participants who agreed to take part in this study and the corresponding agencies for which they represent were selected for a variety of reasons. The first criteria for inclusion were that they have some component of a national security mandate. This requirement could be characterized by, but not limited to a support, intelligence, policy or enforcement components. Second, I opted to secure cooperation from as many points of possible security concerns in the general security assemblage in an effort to accurately depict as many of the core and peripheral possible operational activities. In so doing, I recruited respondents concerned with water security as it relates to cargo vessels, surveillance and enforcement. I also gained cooperation from agencies designated with responsibility concerns regarding immigration, as well as agencies with primary responsibility over national security issues. The final criterion necessary for the purpose of this study was the inclusion of respondents from all three levels of government (Federal, Provincial and Municipal. (*See*: Table: 2.1).

The respondents were either those in charge of their respective agencies at the local or regional level, or they were designated by those in a position of authority to respond to my interview request. Despite the eventuality that the Canadian Security Intelligence Service (Primary national security intelligence agency in Canada) and the Canadian Aviation Transportation Security Agency (Under the auspices of Transport Canada) were not a part of my sample group, every effort was made to maintain as diverse a sample group as possible.

Table 2.1: Sample and Jurisdiction

Agency/ Department	Acronym/ Abbreviation	Jurisdiction
Canada Border Service Agency	CBSA	Federal/Provincial
Canada Coast Guard	CCG	Federal/Regional
Citizenship & Immigration Canada	CIC	Federal
Criminal Intelligence Service Nova Scotia	CISNS (RCMP)	International/Fed/Prov/Mun
Department of Fisheries and Oceans	DFO	Federal
*Halifax Port Authority	HPA	Federal
Integrated Border Enforcement Team	IBET (RCMP)	International/Fed
Immigration & Passport	I&P (RCMP)	Int/Fed/Prov/Mun
National Counter Intelligence Unit	NCIU	International/Federal
National Security Investigation Section	NSIS (RCMP)	Federal

* The HPA falls under Federal Jurisdiction, but operates locally.

The Interviews

By and large, the actual conducting of interviews prompted little difficulty. All but two interviews were conducted within the Halifax Regional Municipality (HRM). Of the two interviews conducted elsewhere, one was managed via internet, while the other was conducted at the Bridgewater RCMP detachment as it marked the middle point between the base of operations for that given agency and my place of residence. Previous arrangements had been agreed upon within the Halifax Regional Municipality (HRM), however, foul winter weather had a negative impact on these meeting times. Due to the nature of the other agency and time constraints resulting from that agencies operational activity, the respondent answered the questions and returned them via email accompanied with a "confidentiality warning" stipulating:

> The information contained in this email is confidential. It is intended only for the individual(s) named above. If the reader of this email is not the intended recipient, any distribution or copying of this email is prohibited. If you have received this email in error, please notify the writer by return email and delete all copies (NSIS NCO i/c).

The eight remaining interviews were carried out at the respective agency headquarters.

The timing of the interviews coincided with respondent's regular working hours. They were all informed that their participation was voluntary and they had the option to refuse to answer any question or withdraw entirely from the study. While participants were provided an opportunity to request a pseudonym, it was explained that this would not likely be necessary as any reference to them would be done so by identifying them as a representative from a particular agency rather than through referring to them personally. Respondents were previously contacted and provided the interview guideline for the purpose of assessing whether or not they would be able to grant an interview. At the time of the actual meeting, each respondent was re-presented a copy of the interview questions, asked to read over the consent agreement, indicate preferences as to the recording of the interview and direct quotations, sign and date the document. The duration of interviews ranged between 1.45 to 2.5 hours. Participants were informed verbally prior to agreement of the time required to complete the process and this was followed up in the consent documentation. Upon the completion of rewriting the interviews respondents were provided a copy of the transcripts to ensure accuracy and clarify any follow up questions.

CHAPTER 3

LOCAL POLICING & SECURITY AGENCIES: INSTITUTIONAL & NETWORK CHARACTERISTICS

As defined in chapter one, networks are composed of individual agencies/ departments commonly referred to as nodes. Within the security network individual departments/ agencies/ units represent these nodes. While the purpose of this study is to explore and identify what this network looks like and how it functions in relation to hypothesized models and describe relationships in this local security network, it is essential to first develop some understanding of the individual institutional nodes in the network. This will be accomplished by first considering the "security mandates" of these individual nodes and focusing on the dedication of time, resources and sense of priority placed on security related initiatives. This will be followed by some discussion of key operational activities as they relate to intelligence, enforcement, policy development, strategic and tactical functions.

Security Mandates

Agency Security Mandates

As one might expect the events of 9/11 sparked changes in the way security agencies in Canada go about conducting their business. Generally speaking, in the sample group discussed here, these changes could be categorized as functional changes, policy changes and no change at all.

Functional Changes

Citizenship and Immigration Canada (CIC), Halifax Port Authority (HPA), Department of Fisheries and Oceans (DFO) and the Canada Border Service Agency (CBSA) best manifest functional changes effecting day-to-day operations. Arguably, **Citizenship and Immigration Canada** has undergone the most drastic changes, as most, if not all enforcement and removal functions were shifted from this agency and redirected to the CBSA. Nonetheless, CIC has implemented new documentation technology. As the Acting Director of Operations, Nova Scotia articulated, "our permanent residence [and citizenship] cards are among the best in the world," as they utilize both biometric components and bank note features.

The **Halifax Port Authority** has also experienced structural changes as a result of compliance to the Canada Marine Act (CMA) and the accompanying Marine Transportation Security Regulations (MTSR). These regulations were in accordance with the International Shipping and Port Facilities Code (ISPS), which was implemented in 2004 and included such changes as improved lighting, fencing and more manpower in the form of a Halifax Regional Police detachment dedicated to port operations. Other budgetary increases[2] were dedicated to biometric port security cards, video surveillance (CCTV) and portable security shacks.

Additional funding was provided to the **Department of Fisheries and Oceans** to increase their missions by one flight per week. DFO has a contract with Provincial Air Lines (PAL) and in turn carries a contract with the RCMP and other police agencies. Prior to 9/11 DFO used to fly in a linear fashion and focus on fishing vessels, however, since that time they fly in a snake like pattern and monitor all activity.

The **Canada Border Service Agency** has undergone functional as well as policy changes. The respondent with whom I spoke had previously served with Canada Customs and Revenue Agency (CCRA) prior to the creation of the CBSA. He noted an increase in access to intelligence information, more equipment such as the Vehicle and Cargo Inspection System (VACIS) machines and manpower. To what extent these changes are attributed to the merger of these agencies now comprising the CBSA is unknown. Like the proceeding category, policy changes came in the form of policy attitudes towards developing a knowledge base and looking at situations in a practical sense differently.

Policy Changes

As previously mentioned, policy changes can be separated into two distinct categories. First situations are assessed on an individual basis and the way operational officials address a situation. Second they can be viewed as an official regulated response. In a similar fashion to his colleague from the CBSA, the representative from **Immigration and Passport** (I & P) has expressed an increased emphasis on any investigation involving elements of national security. He articulated, "There is a heightened awareness in an investigators mind set...to look for that component." Background checks and investigations are based on "the country where they came from and where they stayed during transit to their final destination." Similar to the CBSA and I & P, the **Integrated Border Enforcement Team** (IBET) here in the province has also adopted a new perspective on security issues. The NCO i/c for the Nova Scotia IBET noted, "Prior to 9/11 we never paid too much attention to what was happening down in

the U.S. He noted an increased vigilance is necessary given we are "next door to the number one target on the terrorist list."

Other policy changes come in the form of officially designated regulations. While operations on the West Coast are more closely associated with security matters, here on the East coast the **Canadian Coast Guard** (CCG) has taken a more active role with respect to marine security exercises and have a seat in the newly developed Marine Security Operations Centre (MSOC). This is headed up by the Department of National Defence (DND) and also includes HPA, United States Coast Guard, Office of Naval Intelligence and the RCMP. Changes to the National Security Investigation Section (NSIS) came as a result of legislative additions to the Criminal Code, PART II.I Terrorism.

Of the total research sample, only two respondents declared no changes to their respective units post 9/11. However, they did note that future changes were a distinct possibility. The bureau director of the **Criminal Intelligence Service Nova Scotia** (CISNS) said, "no, it hasn't changed, but we are changing." His counterpart, the Regional Counter Intelligence Officer with the **National Counter Intelligence Unit** (NCIU) noted there have been no changes as of yet directly related to that section, but there are discussions underway.

In an effort to properly map the functions of each agency in the local security network under study, a case-by-case description of the various agencies involved will be necessary. The Halifax Port Authority (HPA) represents the only respondent who's mandate appears to be limited to municipal jurisdiction. Put in its simplest terms, the HPA is the "architect of overall security" in the port of Halifax. The spectrum of

responsibilities this entails includes, but is not limited to addressing security concerns at the Richmond Terminal, Ocean Terminal and the Cruise facility. The actual scope of Marine Security extends beyond these primary zones to include the control of access zones, restricted areas and the Bridge Commission. In total, the HPA is responsible for promoting proactive acceptance and application of regulations mandated under the Canada Marine Act (CMA), which incorporates the Marine Transportation Security Act (MTSA).

Supporting Mandates

Certain agencies share institutional security mandates as can be illustrated with the Canada Coast Guard (CCG), Department of Fisheries (DFO) and Criminal Intelligence Service Nova Scotia (CISNS). All three of the respondents from their respective agencies acknowledge a role in national security matters, though such involvement seems to be of a tertiary nature. The CCG has no official mandate in security related matters. However, as the Acting Director of Operational Services (CCG) notes, they "have a major role in providing support to other government departments." As such, since the Royal Canadian Mounted Police (RCMP) do not have their own vessels to operate within the 12 - mile limit; CCG vessels are utilized to get out to enforcement areas. DFO also functions in a similar fashion. DFO's Aerial Surveillance program flies 5-6 missions every week collecting data on both commercial and fishing vessels en route. On occasion a representative from the RCMP might accompany DFO officials on this task. The role of CISNS also has an intelligence component. While the agency has little in the way of a direct mandate concerning national security, despite official documentation otherwise,[3] it

is in the intelligence gathering game and has an obligation to forward any such information to the relevant agency. Members of this unit are on secondment from other agencies; therefore, have a certain responsibility to their respective home agencies.

Border & Immigration Mandates

The next general grouping of security mandates is comprised of border and immigration integrity. The National Counter Intelligence Unit (NCIU) is a Department of National Defence (DND) agency that is charged to "identify and counter threats to the security of DND posed by individuals or groups involved in terrorism, espionage, subversion, sabotage and organized crime." In accordance with the Smart Border Agreement,[4] the Integrated Border Enforcement Team (IBET) as the name suggest is an integrated unit consisting of members from various U.S. agencies and Canadian agencies tasked with securing both U.S. and Canada from threats to national security and organized crime at borders and entry points. This challenge encompasses designated ports of entry and all points in between. Here in Nova Scotia the situation is unique from other IBET's as it represents a water border. The last agency included under this category is the Canada Border Service Agency (CBSA). Simply put, the CBSA controls "the movement of people and goods across the border." This multiplicity of functions stands to reason given the creation of the agency in December 2003 and the amalgamation of its core members from Canada Customs (CCRA), Canadian Food Inspection Agency (CFIA) and certain sections of Citizenship and Immigration Canada (CIC).

Although most of the immigration security functions have been removed from CIC, document integrity still resides within that department and represents a preeminent

proactive factor in securing immigration integrity as it relates to issues concerning national security. Closely associated with document integrity with respect to immigration matters is Immigration and Passport Section of the RCMP. I & P's mandate is to combat and disrupt organized crime involvement in the smuggling and trafficking of persons to Canada. There are many "cross-elements" in this area. Thus, comprising a priority to national security investigations.

The final agency to be discussed is the **National Security Investigation Section** (NSIS). NSIS stands out from the previous agencies in that under the Criminal Intelligence Program, they are equipped with the expertise "required to carry out security related responsibilities assigned to the RCMP." NSIS has special training regarding Codes under the Privacy Act, Access to Information, Canadian Security Intelligence Service Act and other areas of training. NSIS is a significant and fundamental agency in this assemblage as under the Security Offences Act they (RCMP) "has primary jurisdiction for investigating offences related to national security."[5]

Security Related Resources, Time and Priorities

A key characteristic of networks is the functional power positioning of individual nodes. Dupont (2004) argues, size and jurisdiction factors into the power dynamics of any network. Castells (2000a, 15) emphasized the interdependent nature of networks. Therefore, as long as an agency is part of the network and they specialize in a function quintessential to the effective functioning of that network, its status as a member is secure. Presumably, the dedication of resources, time and the sense of priority assigned security related matters would coincide with this distribution. In order to examine the

importance accorded to security related aspects of their respective mandates, respondents were asked to rate the relative importance of resources, time and priorities allocated to the provision of security initiatives. By and large, among these agencies, the distribution of time, resources and priorities dedicated to the national security initiative occupy two opposite sides of the spectrum (Table 3.1). Of the ten agencies in this study four (CBSA,

Table 3.1: Assigning Security Time, Resources and Priorities.

Agency	Time	Priority	Resources (%)
CBSA	HIGH	HIGH	76-100
IBET	HIGH	HIGH	76-100
NCIU	HIGH	HIGH	76-100
NSIS	HIGH	HIGH	76-100
HPA	HIGH/ MODERATE	HIGH	*
I & P	**	HIGH	26-50
DFO	LOW	LOW	0-25
CCG	LOW	LOW	0-25
CIC	LOW	LOW	0-25
CISNS	LOW	LOW	0-25

* Within the Halifax Port Authority the dedication of resources is difficult to quantify as they are built into the general operating budget.

** I & P resources are not pre-determined, rather situation dependent.

IBET, NCIU and NSIS) indicated that 100 percent of their agencies time was dedicated to national security matters. As might have been anticipated, the level of resources dedicated to security related activities corresponded with the allocation of time and priority. Given that two (IBET and NSIS) of these four agencies are lead or composed of RCMP members, the Federal agency designated preeminent in Federal national security matters in conjunction with the respective security mandates of these agencies, the significance of security issues conforms to what would be anticipated. Similar comments can be attributed to the role of NCIU as their mandates relate to military personnel. In addition, the front line duties assigned the

CBSA and the diversity of its mandate also accounts for the vast significance of security related efforts.

Of these four agencies the respective representatives that consistently rated a "High" emphasis on time, resources and priorities, three (NCIU, IBET and NSIS) noted that 100 percent of there time was spent on security related matters. The respondent from the IBET indicated, "That is why we were created." The respondent from NCIU noted, "we are a security agency."

The CBSA stands out from this grouping somewhat in that while 100 percent of their time is dedicated to security matters, they do not all "directly" or strictly pertain to specific security related concerns. Upon performing the various functions the issue of national security is always present. Thus, when asked about the priority placed on national security, the respondent from the CBSA stated, "they're high up."

Within this grouping of criteria there are two agencies, which stand out. While the Halifax Port Authority did not rank in the "High" category with respect to the time component[6] the respondent did emphasize that security was "top priority" at the HPA. Assigning a figure to the amount of resources was difficult largely due to the practice that security provisions have been incorporated into the overall operational budget.

Difficulty in assigning a value to the allocation of in this data set is also found with the Immigration and Passport Section (I & P). Determining time allocations proved difficult with this agency as work is conducted on a "case-by-case basis...[and they] don't really sit down to predetermine the number of hours" required completing the task. While resources dedicated to national security matters ranked in the low/moderate range, they were number one on the list of priorities.

The remainder of the agencies in this assemblage responded as one might have expected or at least were consistent when comparing the three criteria. Given the largely tertiary security mandates of CCG, CIC, CISNS and DFO and their respective functions as facilitators or support organizations, it stands to reason the amount of time and resources dedicated to security related initiatives would be consistent with the nature of their role. When speaking to the respondent from CCG he noted while funding was being decreased, any additional funding has been "earmarked for the allocation of marine security." He went on to say "this is expanding because we are here, not because we are mandated." Thus, while national security issues in these agencies were not high on a regular basis, the emphasis placed on security concerns when and if an incident actually materialized takes precedence.

Prior to addressing operational activities, some mention should be made to budgets. Only 3 of the 10 respondents indicated an increase in their operational budgets. Of these the Halifax Port Authority derived its increase from profits emanating from port operations. The Department of Fisheries and Oceans received extra funding for flying the one extra mission per week, and the Integrated Border Enforcement Team was allotted $590 million, which will be reassessed after five years. This funding was earmarked for all of the IBET's across the country, taking into account the manpower, education and technological improvement such as the Secure Criminal Information System (SCIS), which is a databank that contains top-secret information pertaining to national security issues.

Within the CBSA the operating budget has not changed since its inception in December 2003 (the CBSA did not exist pre 9/11), although, the undertaking of special

initiatives can affect the budget. While the CISNS has not received any budgetary increases, it is being negotiated at present and will require increased funding compensatory with any new expected duties as seems to be the case. While Immigration and Passport will be receiving extra manpower, they will be withdrawn from existing programs from other regions in Canada as regional sections are being created in an effort to achieve "critical mass." Of the remaining four agencies funding has either been frozen or reduced. Both the CCG and CIC have noted a decrease in funding, while NCIU and NSIS have noted a freeze. In the case of NSIS there has been no additional funding since 1998. Overall, it appears increased security responsibilities have not translated into increased financing.

In essence, the distribution of mandates within this security assemblage encompasses a myriad of responsibilities in the public and private sectors, including support roles and immigration and border integrity. Intertwined within this security response resides the issue of overlap. To a certain extent this issue is being addressed through the creation of Joint Force Operations, which serve to amalgamate and better deploy resources. However, some disconnect can be identified among the cross elements of mandates.

Since the events of 9/11 certain provisions have been implemented in a vigilant effort to tighten security measures. 9/11 has had a significant impact on mandates and priorities for some. It has resulted in the reorganization, expansion and arguably the extent of resources dedicated to national security efforts. Such changes can be observed on a functional basis in the manner in which day-to-day operations are conducted. It is also suggested by the member from the CBSA, there is greater access to information. Although, in this particular instance improved access to information might be the result

of three agencies being incorporated into one newly created super agency. This amalgamation and subsequent creation might speak to the validity of the networked model and characteristics concerning the capacity to expand and in some situations exclude "nodes." Changes in policy post 9/11 stems from a shift in personal and institutional philosophies as well as the newly developed federal legislation. Only two respondents indicated no changes since that fateful day in September, 2001, however, there was unanimous consensus changes are likely forthcoming in the form of increased JFO's and emphasis on national security matters.

The dedication of time and resources were consistent with the priority placed on the national security initiative. Those in a support role spent little time or resources directly designated to that function, as involvement was tertiary and incorporated during the operation of their respective other mandated activities. However, involvement in national security efforts was and is paramount when involved in current or ongoing operation. Nonetheless, the expansion and pluralization of policing activities does appear to be in motion. In addition, the dedication of time and resources speak directly to the concept of "switchers" within this assemblage. Recall, networks are composed of nodes some of which are primary nodes, thus designated the term "switchers" as they are the "power holders" within the network (Castells, 2000a, 15). As power holders they possess the social capital emanating from being denizens within other networks (Shearing and Wood, 2003a, 6). The relative weight of these switchers is derived "from their ability to be trusted by the network with an extra share of information. Castells notes, in this sense, the main nodes are not centers, but switchers following a networking logic, rather than a command logic" (2000a, 15).

Finally, the connection between the dedication to security resources and budgetary factors naturally mitigate and/ or aggravate the efficiency of this response. Seven of the ten respondents indicated a freeze or cut back on federal financing. With the creation of the CBSA it can be said that resources in some circumstances has been redistributed. However, perceptions at the local level reflected on the pontification circulated by federal officials. Therefore, from a local perspective, promised resources have not yet been realized.[7]

Operational Activities

Since the tragic events of 9/11 there have been some changes in the way operational activities are conducted. Consistent with literature on post - modern policing, there has been a pluralization of responsibilities as well as the necessity to adhere to the specialization qualities attributed networks. The range of functions that are required to properly address the needs of an effective and efficient security response are multiple. As previously noted, every attempt has been made to sufficiently represent these various components of a modern security and policing assemblage. Five (5) fundamental security related activities have been identified in an effort to discover who does what within the overall response (Table 3.2). Respondents were asked to categorize their individual agencies security activities on a scale of "1" to "5", "1" being a primary function and "5" being a marginal component.

Intelligence

The role of intelligence gathering within national security operations represents the core element of security risk management. It stands apart from the other functions in that

it provides the basis on which the remaining agencies functions are directed. As is readily observable in Table 3.2, intelligence was a significant aspect of all agencies with the exceptions of the CIC, who lost most of their security functions with the creation of the

Table3.2: Operational Activities

Agency	Intelligence	Enforcement	Policy	Strategic	Tactical
CBSA	1	1	1	1	1
IBET	1	2	1	1	1
HPA	N/A	1	1	1	1
I & P	1	2	4	1-2	1-2
NSIS	1	1	5	2	2
CISNS	1	5	1	1	5
NCIU	1	5	4	3	1-2
CCG	4	5	4	3	4
DFO	1	5	5	5	5
CIC	4	5	4	4-5	4-5

CBSA. While the Canadian Coast Guard's, role is largely of a supportive nature and the Halifax Port Authority, (while a "key proponent of the CBSA and RCMP," intelligence initiative) have no intelligence function at this juncture, changes might occur in this evolving security effort. The Acting Director of Operational Services with the CCG noted that they "are the only government sea vessels in the Canadian Arctic…[as such they are] the eyes and ears" in that capacity.

Approximately ten percent of CIC intelligence work is spent looking at pieces of applications and should a more labour intensive investigation be warranted it could be passed on to another agency.

Intelligence activities in this evolving apparatus are quintessential for efficient operations. Of those agencies responding affirmative to an intelligence-gathering mandate some interesting insights were discussed. The respondent from the IBET team

expressed "everything is based on intelligence...strategy is based on intelligence led policing...intelligence will determine how to investigate." The respondent from CISNS noted that more agencies want to join the Criminal Intelligence Service Canada. He stated, "They see it as a network...intelligence is shared." Prior to the events of 9/11, the issue of terrorism was a designated RCMP and CSIS responsibility. "But now, since 9/11 we're looking at quite a lot'" stated the respondent from the CBSA. He went on to note "We do more pre-arrival examination of traveler and commercial information now. This way *(sic)* we can better decide who and what we want to examine."

Enforcement

Enforcement related activities encompass the execution of arrests, detentions of persons and interdiction or disruption of cargo that could possibly pose a threat to national security. The enforcement distribution outcome in Table 3.2 among this security assemblage illustrates an even split, half with an enforcement mandate and half with little to no enforcement responsibilities. With the exception of the CBSA, those agencies designated a high enforcement function were composed of RCMP or Halifax Regional Police units. Since its inception, the CBSA has maintained the designated roles of Canada Customs; the "enforcement" functions of Citizenship and Immigration Canada; as well as those duties previously assigned the Canadian Food and Inspection Agency. Such activities include but are not limited to: the investigation of goods and travelers, issuing detentions, holding hearings, enforcing removals, surveillance and bio-security measures, inspections at border entry points of passengers, baggage and products.

On the other side of the enforcement spectrum the CISNS Bureau Director articulated his agency has no enforcement responsibilities whatsoever. Like the NCIU, they are an intelligence agency only and pass along information to relevant interested enforcement agencies. Consistent with expectations, the enforcement capacity of CCG, DFO and CIC also reflects their role as support agencies. With respect to DFO and CCG, they provide the means by which intelligence and enforcement functions are conducted. However, in and of them selves, lack the mandate to pursue operations on their own volition. Whether or not this will remain as such is in question as the Acting director with the CCG expressed that the "Senate Committee on National Security and the Standing Committee on Fisheries and Oceans want to see a stronger role" for the Coast Guard. Such a shift in mandates equates to an enforcement function, as the previously unarmed department would take on an armed response. In addition, the Acting Director of the CCG also articulated such a change would require a "shift in funding…and culture."

Strategic & Tactical Security Activities

Strategic activities can be more easily identified with long-term planning. It is distinguishable from tactical planning as it reflects general overall directions for national security initiatives and areas of greatest interest where a more concerted effort is required. Tactical planning is more closely associated with specifically designated operations. They are less policy driven and tailored for targeted operations. Unlike strategic security activities, which coincide with long – term risk management, tactical activities are tailored to meet the needs of a unique and specific security threat.

Upon examining strategic and tactical activities the Criminal Intelligence Service Nova Scotia stands apart from the rest of the sample. The general overall pattern showed some correlation between these two activities; however, quite the opposite was the case with CISNS. While the bureau has a significant interest in developing strategy to combat organized crime and by default, terrorist activity, they have no role from a tactical perspective.

Once again, CCG, CIC and DFO had less input into the development of these activities. However, CCG does differentiate itself from the group in that they have a moderate role in respect to strategic activities. To this extent, the respondent simply noted, "yes, policy and strategy has increased." The reasoning for these changes can likely be explained through the inclusion in the MSOC.

On the opposite side of the equation is NCIU who has significant input in tactical operations, but moderate input with respect to strategic activities. Though, this anomaly could be attributed to departmental language and culture. From the NCIU perspective, tactical activities are divided into two categories: "Operational Strategic", which concerns departmental activities and "Grand Strategic", which refers to governmental focus.

The activities of Immigration and Passport in reference to strategic and tactical operations are profound. Consistent with literature on the topic of "Risk Analysis" (Ericson & Haggarty, 1997; MacGuire, 2000), the NCO for the Atlantic Region commented that strategic planning allows them to forecast a plan and provides the ability to predict 10 – 15 years ahead. Through an "Environmental Scan", an analysis of the risks is completed with recommendations to mitigate the risk." Tactical intelligence is

"operation specific" to this region and takes into account its impact on a national and international scale.

Tactical and strategic operations with the Halifax Port Authority also provide some insight into the complexity of this apparatus. As an agency responsible to shareholders and under the auspices of federal regulations, the HPA is in an interesting situation. At a tactical level they have contracted Halifax Regional Police. However, with respect to the MSOC, concern is focused on the East Coast of Canada. This shift in emphasis corresponds to strategic level intelligence and involves Public Safety and Emergency Preparedness Canada,[8] which is the portfolio responsible for the overall national security response. The port operates under conditions whereby there are 3 possible levels of security threats. MAR SEC I represents the normal operational procedures. MAR SEC II coincides with the notion of a "potential threat. And MAR SEC III is categorized as an "imminent threat. Conversely, from a strategic perspective the port operations are taken into consideration with other ports across Canada. Thus, strategic functions are determined by way of Ottawa.

Summary

Basically the range of operational activities among the agencies in this local security network encompasses the spectrum of security possibilities. Security related activities included intelligence, enforcement, policy, strategic and tactical functions and/or a combination to various degrees of many or all functions. General response patterns are consistent with the expansion or the possibility of expanding roles in the security sector with respect to policing activities. This is aligned with arguments suggesting there has

been a pluralization of policing activities. The security intelligence component appears to be the core priority among most of these agencies and there is some indication this might expand to other agencies previously devoid of such activities.

Enforcement activities have largely been entrusted to select organizations with a traditional police function; however, the CBSA is also entrusted with enforcement responsibilities. Furthermore, in the case of the Canadian Coast Guard, changes might be forthcoming. Again, as might be expected, those agencies serving a support function exhibit little in the way of strategic or tactical decision - making. However, in the case of the CCG, further exclusion from this activity is in question.

Perhaps the most appropriate characterization of operational activities would be to describe it in a state of expansion and development. While many activities remained the same, greater emphasis and importance on security related matters has occurred, thereby resulting in the need to coordinate with others. This necessity has impacted the core of many agencies resulting in the creation of more joint force operations in various incarnations. Only one agency (CIC) has experienced a decrease in security related activities.

It can be said with some certainty that this local security network is composed of a number of specialized agencies, which is consistent with networked expectations. Each agency contributes something of necessity to the overall response. However, there remains a significant degree of overlap within this response as well. Despite this fact, compliance to networked qualities must be taken into consideration with the conceptualization of network theory or any theory for that matter. Theories represent an ideal, thus are seldom fully realized.

CHAPTER 4

SECURITY NETWORKS: ORGANIZATIONAL STRUCTURE

This thesis is an exploration of the network qualities of a local security organization. Organizations are rational systems designed specifically to function in concert with fellow people/agencies to achieve a mutually desired goal. Perrow (1967, 195) noted that organizations "are seen primarily as systems for getting work done, for applying techniques to the problem of altering raw materials - whether the materials be people, symbols or things." Networked structures have expanded to encompass a nexus whereby "individuals not only [interact] with individuals as before, they also [interact] with organizations and organizations [interact] with other organizations (Vaughan, 1999, 272). The extent of success with which a given task is realized is impacted by the organizational structure of each member node. Given this necessity as a backdrop, and the functional imperative to have compatibility within and between nodes, it is essential to explore this organizational structure by considering to what extent this local security response adheres to specific network qualities. This task entails assessing the features attributed network models and those historically associated with traditional models. By virtue of the literature on networks certain characteristics can be extrapolated and clearly defined.

Unlike traditional bureaucratically functioning models, which emphasize formality, operate in a centralized manner, function in a hierarchical fashion and are insular, networks tend to manifest features that are **informal**, **decentralized**, **lateral** and **open** (Lebkowsky, 2000; Castells, 2000b). These qualities more readily allow for an unobstructed interconnectedness. Table 4.1 illustrates the results as expressed by

individual respondents with respect to these key structural components relating to network and traditional models. Respondents were asked to rate their respective organizations on a scale designed to indicate to what extent that organization adheres to traditionally oriented models and network oriented models, based on the aforementioned four (4) qualities. The scale ranged from "0" = Completely traditional qualities to "4" = completely network qualities

Table 4.1: Traditional vs. Network Characteristics

Agency	(Formal=0) *vs* (Informal=4)	(Centralized=0) *vs* (Decentralized=4)	(Hierarchical=0) *vs* (Lateral=4)	(Insular=0) *vs* (0pen=4)	Network Score
CIC	2	2	3	3	**10/16**
CISNS	2	2	3	3	**10/16**
CCG	2	2	3*	3	**10/16**
DFO	0	0	4	4	**8/16**
IBET	1	0	3*	4	**8/16**
NCIU	0	3*	0	3	**6/16**
CBSA	0	0	1	4	**5/16**
I & P	0	2	0	2	**4/16**
NSIS	1	0	0	3*	**4/16**
HPA	0	0	0	2	**2/16**
Total	**8/40**	**11/40**	**17/40**	**31/40**	**67/160**

* For purposes of classification, responses indicating a rating between 2 and 3 under a single criteria were issued a "3" score. This occurred 4 times in total.

** Values were re-assigned during the calculation phase to better represent "no" adherence to networked characteristics.

Comparisons were made between Formal and Informal, Centralized and Decentralized, Hierarchical and Lateral, and finally Insular and Open characteristics. The rational for this continuum of comparisons hinges on the network theory assertion that such assemblages manifest characteristics, which are informal, decentralized, lateral, and open.

Formal vs. Informal

Networks are recognized for the informal fashion in which member nodes correspond with one another. Respondents who ambivalently characterized their agencies level of formality had a few interesting and significant comments with respect to this issue and the level of integrity of any security response lacking in formality. The representative from the CCG stated "everything [is] pushing", "moving" and "shifting towards formal." He expressed concern that "too much was happening" and "too much information is lost...if done informally." CISNS bureau director emphasized, "In the intelligence community it depends on urgency, nature and source...Third party rules have to be followed."

The responses indicate 50 percent of the agencies in the sample continue to have aspects strongly attributed to formal organizations. This distribution runs counter to what one might expect in a network model. Of the agencies that responded with a somewhat formal response, the representative from the IBET noted:

> Exchange of information is done formally...The Arar case will have a definite impact on this...it is governed by 3rd party rules... If you are going to use information, let me know what you are going to do with it.

That is, despite the fact two agencies might be functioning out of the same office, if one agency wishes to do something with a piece of information they are required to go through formal channels to do so. The overall score in the formal/ informal comparison was 8/ 40, which suggests at least at this point in time a strong correlation with traditional bureaucratic qualities.

Centralized vs Decentralized

In addition to the informal manner networks function, they are also characterized as behaving in a decentralized fashion. An analysis of the data in the present formulation demonstrated a closer association to the traditional bureaucratic model than a network model, as the total score under this quality was 11/40. . The lone notable exception to this general pattern was found with the NCIU who, while not totally in opposition to the rest of the sample, indicated that there was "centralized control, but decentralized execution." NCIU was keeping in line with the typical military organizational structure. Excluding the position of NCIU, a large proportion (4) of the sample responded ambivalently to this question. However, given the evolving nature of this arrangement, it seems more likely that it will continue to move towards a centralized model. Acting Director of Operational Services CCG articulated that the CCG has evolved from a decentralized agency two years ago, is semi-centralized/semi-decentralized now, and will likely be centralized in two years. The respondent from CISNS acknowledged that they have a "common law relationship" with the Criminal Intelligence Service Canada (CISC) and to that extent it is centralized, however, they do "have some control at the provincial level.

The remaining agencies have expressed a rather strict adherence to the centralized model. However, there remain some differences in respect to interpretation and culture. The respondent from the CBSA noted, "Ottawa has to know…but they might not control it", referring to the dissemination of information. This evaluation stems from terms consistent with the prior remarks expressed by the respondent from NCIU, however, were categorized differently by that respondent. In some instances there was no ambivalence whatsoever. The NCO i/c H Division NSIS commented:

> As we are centrally run from Ottawa, all our reports are forwarded to Ottawa for the ultimate information of the Commissioner through the Criminal Intelligence Directorate. We also advise the Commanding Officer of Nova Scotia through the Division Intelligence Officer of all investigations in Nova Scotia that require his notification.

The general sense of this feature suggests a closer link to traditionally oriented organizations. Of the total responses to this criterion the only un-ambivalent comments emanated from those participants that strictly adhered to a centralized approach. Conversely, there were no instances of strict adherence to a decentralized response.

Hierarchical vs. Lateral Communication

Perhaps the most indeterminate category was found in the hierarchical/lateral comparison due to situational dependent issues and the nature of the information being disseminated. The sum of the ratings amounted to a score of 17/40. Complicating this analysis were the responses provided by the representatives from the CCG and IBET. The difficulty experienced in categorizing these agencies resulted from the range of possible scenarios. In the case of the CCG the location of the particular scenario is a factor. Operational matters, which take place on a ship, are more hierarchical in nature than ashore in an office setting whereby information flows laterally. Interestingly, the respondent noted, "Things don't get done that way." At face value, this appears to run in opposition to the literature on networks. The hierarchical/lateral dichotomy and analysis is further complicated by the IBET experience, as determining the flow of information is heavily dependent on the nature of the information itself. Information of a sensitive nature involving a terrorist organization is "sent off [to Ottawa, then the U.S.]... through channels to make certain everything is done properly." Conversely, if they are simply

seeking information about a boat in Yarmouth and there is uncertainty as to its purpose for being there, the lateral distribution of information is the more common course of action.

The agencies that function primarily in the latter manner are DFO and to a lesser extent CISNS and CIC. Given the operational activity it is of no surprise DFO operates laterally since the intelligence gathered through their Air Surveillance program gets distributed automatically "without being asked and it is used as seen fit." This information is distributed directly from databases located on the plane. With regards to CISNS there are strict guidelines to be adhered, which have been agreed upon in the Memorandum of Understanding (MOU). Thus, as CISNS Bureau director articulated, "the access to certain data cannot be brought back to home agencies." However, as an integrated unit composed of the RCMP, DND, HRP and the CBSA the flow of information within those walls is lateral in nature and the way it operates is through equal partnership. As a policing agency, CISNS as with all policing agencies must adhere to the "Police Act" that restricts the dissemination of information to non-traditional policing agencies.

Hierarchical characteristics can be situation dependent within the CBSA, but they are nonetheless hierarchically managed. The respondent from the CBSA expressed the existence of some "leeway" with respect to the delegation of authority, however, "there is still a need to report." Again, as would be expected the NCIU, I & P and NSIS all expressed characteristics consistent with the bureaucratically oriented hierarchical model.

Classifying the hierarchical/lateral component of this analysis is thus problematic. At best support for network theory rests on the transient nature of this criterion within the

IBET and CCG. Therefore, the overall sense is suggestive that this feature is most closely associated with traditional bureaucratic models. This assessment, as was the case with the previous criterion, is supported by the frequency of strict adherence to traditional organizations.

Insular vs. Open

Of the four qualities discussed, the open manner with which this assemblage functions most closely resembles that of a network. The collective rating of the respondents summed to 30/40. Unlike the isolated, detached operational characteristics associated with bureaucracies, networks are characterized as possessing open qualities. A rating of 21/40 would suggest a greater adherence to network qualities than traditional qualities. Therefore the collective rating of respondents on this quality is significant. Nonetheless, this effort still encounters barriers with the "need to know" philosophy, which plays a significant role in many respects. In numerous interviews respondents referred to the need to know component. The respondent from NSIS articulated,

> NSIS does provide intelligence reports to our partner agencies and other sections in the RCMP if the information or investigation dictates they need to know.

The respondent from the CBSA reiterated this,

> Communication is open within the agency, but there is a need to know basis...security clearance [is considered, as are] third party rules.

The integrated nature of the IBET tells an even more detailed account of the insular versus open attribute,

> We deal with national security issues and go to each detachment...We are visible...[They] give talks...check in at corner stores and hotels...share information directly [with detachment members]...[but] they don't need to know all of the details.

While the representative from the HPA noted they "have to be very transparent", and seek a "proactive" approach with respect to public consultation, the manner in which they are required to operate through the "Smart Port" agreement and the Halifax Marine Advisory Committee mitigates this approach. The committee is a formal organization with informal platforms, thus, while policy is formal, issues can be handled on a one-on-one basis, or in the case of a port wide issue "en massé."

Network Dynamics

Not only does this comparative data speak to the nature of the network as a whole and how member agencies operate with respect to one another, it also provides some sense as to how these agencies function as separate, distinct nodes. Referring back to Table 4.1, complete adherence to network theory would require individual agency responses to achieve a cumulative score of 16/16. Conversely, an agency that reflected absolutely no networked characteristics would result in a cumulative score of 0/16. The overall distribution illustrates five (5) of the ten agencies representatives rated their qualities as 50% or more in line with network characteristics. Interestingly, those agencies within this category are by and large tertiary agencies and function primarily in a support manner. Surprisingly, the functional nature of the IBET thus far does not manifest stronger networked characteristics. Given its designation as an integrated unit, expectations would suggest (in accordance to network ideology) closer reflection to these characteristics. If we begin with the premise that already exists, then these findings provide only limited support for the emergence of network theory in this milieu – at least not at face value. It could be that we need to reexamine our starting point and manage

expectations as to the face of this phenomenon. This point will be addressed in the final chapter.

Summary

If one assumes that the agencies within this local security response were previously all standard bureaucracies, then the identification of even some evidence of a presence of network qualities suggests a significant change. As a network, these agencies manifest features, which are formal, centralized, hierarchical and open. Based on these four components as itemized in Table 4.1, taken as separate units this local security assemblage partially resembles what might be characterized as a "network."

According to the literature on network theory, fully developed networks are decentralized, informal, lateral and open. These results were only partially realized in this sampling. The benefits attributed these characteristics results in the seamless flow of information and intelligence. However, within this assemblage there still remains considerable reviewing and filtering of information (See Appendix A for a more detailed explanation). This finding does not completely coincide with the seamless flow of information that is ideally characterized by "pure" networks. Nonetheless, there appears to be some indication of a transformation in process. Therefore, given the aforementioned criteria, perhaps the best description of this response is a network in the early stages of development. Again, any absolute determination as to the description of this local security network must be considered in conjunction with the knowledge that network theory represents an ideal, and not necessarily an achievable reality.

CHAPTER 5

NETWORK RELATIONSHIPS: IMPORTANCE & PRIORITIES

Power and influence dynamics are inherent features in any organizational model. Castells (2000a, 16) argues, "Networks are value free or neutral." Therefore, at their core they are programmed for a specific task. However, questions still persist as to who defines the goals of the network. This results in a struggle to assign network goals (Castells, 2000a, 16). Understanding the dynamics of inter-agency relationships is critical for developing an appreciation of network models of organization and organizational integration. This chapter identifies and describes the nature of primary relationships and categorizes the importance of these relationships. Understanding the situational dynamics of these relationships includes identifying the exercise of inter-agency power and priority setting abilities, asserting one's relative influence and power vis-à-vis other security agencies in the network. As Castells points out, "while there are still power relationships in society, the bypassing of centers by flows of information circulating in networks creates a new, fundamental hierarchy: the power of flows takes precedence over the flow of power (2000a, 20).

Agency Importance: The Big Three

Networks are characterized by a set of interconnected nodes that function in a lateral rather than a hierarchical manner. Among this mix of nodes are switchers or power holders (Castells, 2000a) whose weight and relative importance are determined by their compatibility to other nodes and association with other networks as well as the capacity and ability to be "trusted with an extra share of information (16)." Given these network

characteristics, it is logical to assume the frequency of reference to established relationships with individual agencies would highlight the importance of certain agencies (nodes) within this assemblage. In this context, respondents were asked to list the foremost nine (9) departments/ agencies with which their agency has an ongoing relationship (See Appendix B). In addition respondents were asked to categorize the purpose of this relationship and discuss in greater detail their respective three primary relationships.

While the intent was to identify the most important three relationships, four agencies stand apart from the group as representing an integral aspect to the overall security initiative (Table 5.1). Paramount among respondents was relationships with the RCMP or sections/agencies headed by the RCMP.

Table 5.1: Top 3 Relationships and Type by Agency and Activity

Role	Sample	Top 3 Relationships & Activity		
Support	DFO	RCMP (I/L)	DND (I)	Other (I)
	CCG	CBSA (S)	RCMP (S)	DND (L)
	CIC	CBSA (L)	CSIS (I)	RCMP (IN)
	CISNS	CBSA (I)	RCMP (I)	HRP (I)
Other	CBSA	CSIS (I)	RCMP (I)	DND (I)
	HPA	CBSA (L)	HRP (L)	TC (L)
	IBET	DFO (I)	DND (S)	Other (I&E)
	I&P	CBSA (E)	CIC (IN)	Passport (IN)
	NCIU	CSIS (I)	RCMP (I)	DND (I/IN)
	NSIS	IBET (I)	I&P (I)	CSIS (I)

Key
E = Enforcement
I = Intelligence
IN = Investigation
S = Support

An ongoing relationship with the RCMP or an integrated unit lead by or consisting of an RCMP representative was acknowledged eight times. Of the eight references, six were of a direct referral to the RCMP in general, while two were made in reference to specific

sections/units (IBET and I & P). Special mention should be forthcoming with respect to the IBET and the CISNS. As integrated sub units composed of numerous agencies from the national and international community, it is logical the RCMP would be heavily involved with these units, particularly given RCMP preeminence in national security matters. The core agencies in the Nova Scotia IBET are: RCMP, CBSA, Immigration and Customs Enforcement (U.S.), United States Customs and Border Enforcement and the United States Coast Guard. CISNS operates in a similar fashion since HRP, CBSA and the RCMP are core agencies in the bureau. At the core of these relationships are the exchanges of security information and intelligence.

The relationship CIC shares with the RCMP are by and large of an investigative nature, delving into section 29 investigations[9] or other Immigration and Refugee Protection Act (IRPA) violations. Immigration officers might not feel comfortable with a file; thus, refer it to the RCMP under such circumstances. However, it is customary at this point in time for anything of significance to go to the CBSA enforcement unit until the investigation is concluded. Immigration and Passport (I & P) has a relationship with CBSA based on secondment, whereby at this point in time a regional intelligence officer from CBSA meets once a week with the unit. This activity involves the "administration and enforcement of the Immigration and Refugee Protection Act (IRPA).[10]

Second on the list of most notable agencies was the Canada Border Service Agency (CBSA), which was listed among the top three relationships by seven different agency respondents. As was the case with the RCMP (see above), the CBSA is a core agency within the IBET and CISNS. Thus, reference to the CBSA was by way of association as contributors in an integrated security initiative. Similarly, the respondent from DFO

passively indicated a relationship with the CBSA as one of the three top agencies with which such a relationship exists. In this capacity the CBSA retrieves information via RCMP liaison assigned to DFO. While not expressed as one of the top three relationships by the respondent at CBSA, the existence of the relationship between the CBSA and HPA is worthy of description. For lack of a better characterization, this relationship is through a liaison position. This activity entails liaising and interaction on matters concerning terminal security. The CBSA has primary jurisdiction to identify and inspect ship manifests, thus has free access to every terminal. Relations between HPA and NPET were categorized as nearly as important as relations between the HPA and CBSA.

Both CSIS and DND were referred to five times by this sample grouping as being among the three top agencies with which a relationship exists. Since NCIU is represented in this sample, I will confine my discussion to that agency in its capacity as a DND resource. Given its mandate at home and abroad, NCIU serves a pivotal function for the Department of National Defence and for Canadian national security within ports. As a branch of the Department of National Defence, NCIU operates as an intelligence and Investigative arm for DND (Its Host agency), providing advice through the "collection of intelligence," identifying security risks through "proactive programs," and the conduction of "investigations and operations," hence, becoming aware of internal and external threats. Providing "up front information" has become paramount and occupies a much "higher profile" since the "U.S.S. Cole" incident. DND also Liaise with CCG and functions as a vessel support agency for the IBET in conducting patrols.

As previously discussed, CSIS receives information via the RCMP emanating from DFO. There is a mutual exchange of information between NCIU and CSIS, as is the case

with NSIS and CBSA. However, the respondent from the CBSA noted, the Privacy Act and third party restrictions[11] could impede the sharing of information on individuals.

Coordination

The mechanisms in place designed to manage the coordination of this security arrangement have multiple manifestations. The basic methods can be broken down into formal and informal components. Examples of the informal means of coordinating security efforts can be witnessed in the way the IBET utilizes the Offshore Aerial Surveillance program employed by the DFO. The NCO i/c NS IBET noted,

> They set up flights and we get on board out to the U.S/Canada Border...They know what the IBET is...They set the guidelines of where we are flying.

Similar arrangements between the IBET and DND exist,

> Given the resources of DND, ie; vessels, we can and have utilized them to assist in coastal patrols.

Thus, the basic informal process undertaken in this relationship is simply to "hop on board."

In a similar vein the respondent from Immigration and Passport Section articulated a less formal arrangement with certain agencies. The NCO for the Atlantic Region expressed they had "excellent coordination" with both Passport Canada and CIC. Cases are referred and discussed "over a cup of coffee." Much the same could be said with respect to the arrangement between NCIU and CSIS or the RCMP. The NCIU Regional Counter Intelligence Officer noted that no formal relationship existed between NCIU and those agencies, but that the sharing of information taking place is based on professional judgment. Such examples are consistent with expectations attributed networked approaches to security initiatives. However, there also exists a more formal element to

this relationship among the same agencies (Interview 1, Interview 2). Formal means of coordination can take the form of Memorandums of Understanding (MOU) or be subject to legislative and institutional policy. The relationship between the CBSA and I&P illustrates this point as agency coordination is based on secondment.

The creation of MOU's and predetermined guidelines as developed within the operational policies of the IBET and CISNS for example and the inclusion of the "need to know" provision all mitigate the effectiveness of this cooperative effort. The means of coordination are dictated at the regional or central level through Service Level Agreements (SLA), which are national in nature and Memorandums of Understanding (MOU's) that contribute significantly to Canadian Coast Guard (CCG) operations. At the moment, relations with the RCMP and thus by virtue of its mandate, IBET, is on an informal basis. However, The Acting Director of Operational Services with the CCG indicated in a year's time this arrangement will likely become more formal and more interaction would take place. In the case of CISNS coordination is dictated by "the laws of the country and " the need to know."

Essentially, coordination is based upon formal agreements and informal relationships or a combination to a varying degree of both. To a certain extent these attributes raises some issues concerning accountability. It raises questions with respect to responsibility and the distribution thereof. This coincides with the assertion that networks are better able to disperse organizational responsibility more evenly among member nodes (Dupont, 2004, 78). Conversely, this arrangement also inhibits the optimal effectiveness of the response. In combination with legislative and other formal procedures and policies, professional judgment can also result in the hampering security efforts.

Autonomy

Bayley and Shearing (2001) has coined the concept of a multi-lateralization of activities and responsibilities to reflect the fracturing of traditionally designated departmental practices and resulting practice of governance through a variety of nodes. Consistent with this fundamental shift is a shift from relationships characterized by features of autonomy to one based on collaboration. In an effort to isolate and identify this network characteristic in this local security network, respondents were asked to identify if the issue of agency autonomy has changed since the events of 9/11.

The variation in responses to agency autonomy varied, lacking any unilaterally agreed upon characteristic. Nonetheless, respondents did indicate more often than not an autonomous association with most other agencies. As would be expected, the issue of agency autonomy was related to the issue of cooperation. The correlation between those agencies that are entered into an MOU coincides with those whose autonomy depended on MOU's as part of a Joint Force Operation (JFO). That is, the terms of the MOU dictate the degree of autonomy. This dynamic highlights the importance of MOU's in determining the degree of collaboration, which more accurately reflects networked qualities, but detracts from suggestions that this shift is all encompassing to include departments at large. Wood (2000) might characterize this revelation as "the ongoing reinvention of governance [that] occurs more through waves of change rather than a dramatic ideological or structural shift (5)."

Overwhelmingly, respondents noted that there are "no less" important relationships within this mix. There is a general consensus suggesting relationship importance is situational dependent. But, as articulated by the representative from the IBET, in the case

of integrated units, core relationships are most important. He expressed " other agencies might be less important today, but more important tomorrow." The respondent from NCIU reiterated this point focusing on the unique circumstances of a potential threat, agency expertise and the primacy of roles. To buttress this comment the representative from NSIS stated, "All of our partners could be important in an investigation and the lead role could change depending on the incident." More profound was the response from the representative from the CBSA who articulated, "All relationships are very important...the only way intelligence works is through the exchange of information...you can't squeeze them out." These comments are consistent with the networked principle of specialization (Shearing, 2005, 59), as well as the necessity to respond to "perceived challenges and objectives (Wood, 2000, 5)."

By and large, the issue of importance in the present security grouping is a non-issue. This is depicted above with respect to relationships among the top three cooperative efforts as well as in the assessment of possible least important relationships. This characteristic is in keeping with network relationships whereby all relationships are important to the network. This pattern also resembles network expectations surrounding "switchers," which suggest certain nodes are core to this response. The data clearly identifies the RCMP, CBSA, CSIS and DND as significant actors in this assemblage. It also follows that these agencies belong to other networks beyond those here in Nova Scotia. These are findings indicative and consistent with the expectations found in the literature on networks as relating to switchers being members of multiple networks (Castells, sept2000b, 697). However, it has also been argued if one node fails to contribute to the overall response, then the others would subsequently function in an

automated network fashion and force the negligent node out of the grouping. Granted, nodes might be replaced, but under certain circumstances an effective and efficient response would be compromised. Furthermore, core logistical tools are not easily replaced.

It might be the case that qualities inherent in the traditional organizational model still persist, whereby agency power and status is still dictated by the importance of any given agency. This is not the case where networks are concerned, as all agencies are vital to its optimal functioning. Thus, the current assemblage might be marked by remnants of a lumbering bureaucratic model as well as features attributed networked models. Once again, the general response pattern provides mixed results, which is consistent with the evolution of a network unfolding through what Wood described as "waves of change (2000, 5)."

Priority Setting

Possible scenarios resulting from the above mentioned contingencies appear to be limitless. Again, considering the literature on networks certain expectations exist with respect to membership in other networks and the concept of primary nodes described as "switchers." Recall switchers are "power holders" (Castells, 2000a, 16) largely due to their compatibility and ability to be entrusted with greater information. In addition, amongst network theory, there still remains no clear sense as to how goals are determined and arrived. In an effort to assess the validity of this point it is necessary to consider if and how one agency influences the priorities of another. In this section respondents were

asked to discuss to what extent, if any, they had influence over the priorities of other agencies or were influenced by other agencies. The results are listed in Table 5.2.

Table 5.2: Network Qualities – Open & Closed.

Agency	CISNS	I&P	NSIS	CCG	DFO	NCIU	CBSA	CIC	HPA	IBET
Influence	N	N	N	Y	Y	Y	Y	N	N	Y
Influenced BY	N	N	N	Y	Y	Y	N	Y	Y	N

As the table illustrates, responses varied in the degree with which agencies identified with a network orientation based on the issue of influence. Three (CCG, DFO and NCIU) agencies representatives responded affirmatively in both categories. Therefore, those agencies are characterized as possessing more open qualities, which implies greater subjectivity to external influence. The remaining four agencies demonstrated a variation of mixed qualities. Of these, two (CBSA and IBET) respondents articulated their respective agencies were more likely to influence other agencies/ departments than be influenced by any other department, while the remaining two (CIC and HPA) agencies representatives indicated just the opposite. Three (CISNS, I & P and NSIS) of the ten agency representatives replied that they neither influenced nor were influenced by any other agency within this network. This finding would suggest these respective agencies are more closed. This mix of responses implies qualities reminiscent of a network in the early stages of development.

According to respondents, five of the ten agencies have an affirmative influence on at least one other security agency's priorities. Given the "typical military operational structure" as manifested in the traditional bureaucratic chain of command approach and the anticipated "centralized control" of the NCIU, it is expected in its capacity as the

Department of National Defence's information and intelligence unit, it would have a certain degree of influence over other agencies within that host department. However, the impact on priority setting differs when it comes to the remaining four agencies, as influence is not engineered through host departments, but rather on different departments.

The Department of Fisheries and Oceans and the Canada Coast Guard both possess a certain degree of influence over the RCMP. DFO Director for the Maritime Region articulated, "I think our air information is more important to the RCMP...What we see has more influence on what they do." By the same token, Acting Director of Operational Services with the Canada Coast Guard expressed that they are also a support agency and if the RCMP did not access CCG's ships, "where are they going to go."

Intertwined in this complex equation is the role of the IBET, as it is primarily the IBET that would access the aforementioned agencies services. The NCO i/c NS IBET looked at the internal components of this integrated unit and believed the unit influenced the only other Canadian member of the unit (other than the RCMP), that being the CBSA. Interestingly enough, the respondent from the CBSA was of the opinion that his agency influenced the priorities of the IBET and other JFO's due to its "contacts abroad." Again this reflected the internal operations inherent in an integrated unit. Beyond the confines of the JFO, the respondent did not acknowledge any other influential positioning.

While the Halifax Port Authority does not influence Transport Canada and the CBSA directly, it does work with and attempt to influence these agencies in terms of policy implementation. This is not an indicator of power, rather an effort to facilitate port operations in such a fashion, which takes into consideration the economic and security obligations assigned the HPA.

The power to influence is synonymous with the power to be influenced. In terms of national security matters, among those agencies whose representatives acknowledged a predisposition to be influenced, the predominant sentiment was where security is an issue; it would take priority over any other mandate. As such, the RCMP (being the lead agency on national security matters) was cited most often as possessing the ability to influence priorities. Having said this, all of the respondents indicated that there has yet to be any significant difficulties with respect to competing priorities. One respondent indicated, "Where it concerns national security...No brainer (Interview 3)." Another noted priorities would be determined based on the operation, they would "try to accommodate...[but in the end they] are going to do it (Interview 6)." However, this conciliatory approach might not always be the case as one respondent indicated, "if they want us to do something on their behalf, we have to consider the practicality...We have to deal with our priorities...It depends on the need (Interview 4)." In addition, regulations are in place that impedes the automatic acquiescence to requests. There are certain practices that are followed that resist any derivation thereof. Evidence of this came from the representative from the CBSA who noted when interviewing people crossing the border,

> If CSIS wants us to ask certain questions, we can't ask those... We have a set of questions to ask. If they answer them correctly then we can't ask the other questions (Interview 2).

As might be expected, the influential relationship that exists between NCIU and the host agency The Department of National Defence is a reciprocal one. Should an issue arise whereby NCIU can accommodate a request under its current mandate it will endeavor to do so on an informal basis. Otherwise a formal request would have to be pursued, thus having the priorities changed by senior officials.

Keeping with the matter of influence as it relates to this study in the context of national security in Nova Scotia, special attention should be granted the National Security Investigation Section. While there is no organization, which directly influences the priorities of NSIS, its priorities are dictated by the priorities as set down by the RCMP "National Security Priorities" in Ottawa after consultation with "O" Division (Ontario), "C" Division, (Quebec), "E" Division (B.C.) and Ottawa. Therefore, the particular issues in the Atlantic region have a negligible impact on the determination of priorities.

Summary

Evidence of an operating security network has come to bear in this sample. The frequency of interaction between certain agencies within this sample of organizations clearly suggests a ranking of importance in the overall response. Chief players were units directed by the RCMP and the CBSA. Surprisingly, the role of the Canadian Security Intelligence Service (not represented in this sample) ranked third, of similar significance to the Department of National Defence. In addition, the most frequent purpose for interaction is the sharing of information. Given the federally designated nature of these primary agencies and the connection between them and parallel units located elsewhere within the country, some evidence exists in support of network model characteristics. These three or four units could be characterized as switchers.

The coordination of these agencies and the activities they share is managed through a mixture of formal and informal relationships. The issue of autonomy is a non-issue as each agency operates beyond the influence of one another. So long as they perform the role they are assigned, they have a place in the network.

Finally, the ability to influence or be influenced by other agencies within the confines of this grouping leaves one with the impression that there is no standard pattern, since responses were mixed and ambivalent. However, influence is determined by specific situational requirements. Since most agencies specialize in certain fields, their respective roles are essential for efficient operations and cannot be duplicated easily by confederate agencies. Consistent with network conditions, these agencies operate in an interdependent manner, whereby collaboration and cooperation is a necessary component in the overall shared security exercise. Beyond these niches, there still remains significant overlap in other functions. Agencies with tertiary roles discussed the unique and indispensable function they contribute to the mix. Primary actors reflected upon the influence they possessed over other primary actors. Regardless of these observations, where a threat to national security is a real concern, the ability to influence is irrelevant and of no consequence as acute threats to national security trumps all other operations.

CHAPTER 6

NETWORK GOVERNANCE: DYNAMICS AND DECISION MAKING

Among its distinctive qualities, discourse on Network Theory evolves around the **decentralized** operation and **lateral** communications. That is to say, the command and control structure is more reflective of a decentralized organizational response (Kempa et al., 1999). But analysis that limits its focus on "local" nodes in a network, and neglect the role of senior organizational and/ or political authorities is incomplete. In this chapter the intent is to verify whether or not this developing security network is consistent with these networked characteristics of decision-making. This description and analysis is accomplished by first exploring key reporting protocol attributed to this security nexus. This exploration entails considering a number of quintessential operational features, including 1) reporting protocols, and 2) decision – making practices. Reporting protocols describe formal the means by which decisions are arrived in relation to central authorities.

A). Reporting Dynamics

Traditional bureaucratic organizations are characterized by the necessity to report operational activities to senior institutional authorities. This is necessitated by the hierarchical manner in which they operate. Unlike the cumbersome procedural systems, commonly associated with bureaucracies, networks claim to have the capacity to bypass micro-managerial procedures through a flatter organizational hierarchy and integrative approach. The integrative strategy of joining nodes on a common task more readily lends to the unimpeded sharing of information. This allows agencies to be better-equipped and

able to access and provide information in a seamless and lateral manner (Castells, Sept, 2000, 695). An integrated approach by its very nature implies the practice of reporting to multiple or joint authorities. The extent of agency integration has a fundamental role in determining the fluidity of this exercise. Table 6.1 illustrates the nature of these relationships in this particular local security network. Respondents were asked to comment on the types of authority and to whom they are required to report.

Table 6.1: Reporting (Joint, Internal and External Authorities)

Authority	CCG	CISNS	IBET	CBSA	I&P	DFO	CIC	HPA	NCIU	NSIS
Joint	Y	Y	Y	Y	Y	N	N	N	N	N
Internal	Y	Y	Y	Y	Y	N	N	Y	Y	Y
External	?	N	N	Y	Y	N	N	Y	Y	Y

The distribution of responses coincides with some consistency to a proposed network model. Five of the ten agencies identified some reporting to a joint authority. Eight agencies reported to internal departments, while five also reported to external organizations. This reporting pattern is significant in that networks would be marked by an increased reporting pattern to external and joint authorities. By and large, the distribution of reporting patterns was not exclusionary. Of the eight agencies that reported to internal authorities, five reported to a joint authority and five reported to an external authority.[12]

The representative from the CBSA responded affirmatively to joint, internal and external authorities. As a member of a JFO, the CBSA reports to the Director of the JFO. Such is the case with regards to the CBSA membership within CISNS. Internally the

CBSA reports in the typical hierarchical fashion to the Director, Regional Director, Vice President and President of the CBSA. As a member of Public Safety and Emergency Preparedness Canada (PSEPC), the CBSA ultimately reports to an external agency as well. This reporting pattern coincides with the image of an agency undergoing change. It suggests some adherence to network qualities as well as the traditional organizational behavior.

As previously discussed, the Integrated Border Enforcement Team is composed of several entities representing both Canadian and American Contingencies. As such, the IBET reports to the Integrated Joint Management Team (IJMT), which will ensure all of the agencies are receiving the proper reports as defined under the regulations within that policy framework. In true fashion to the hierarchical framework of the RCMP and in a similar fashion as the I & P section, the IBET also reports internally to the Border Integrity Officer, who in tern reports to the Provincial Federal Policing Officer and so forth until it finally reaches the Assistant Commissioner (Federal Intelligence Officer). While this unit does not report externally to any agency, it might on occasion send reports to the Canadian Security Intelligence Service (CSIS). Again, these mixed reporting patterns are indicative of an effort in transition.

The remaining agency for which a respondent identified a necessity to report to some joint authority was the Canada Coast Guard. As a member of the Maritime Security Operations Centre (MSOC) a DND lead initiative, CCG is required to report to the lead agency in relation to security matters. Like the IBET, the MSOC is a multi-agency operation and is engineered in such a way that it resembles an integrated approach to problem solving. Again, adhering to traditional models of organizational operations, the

CCG reports up the chain of command to the Regional Director, the Commission and finally to the Assistant Deputy Minister.

To what extent Immigration and Passport (I & P) is required to report to a joint authority is a matter of debate. This is primarily due to the joint authority with whom they report being an internal mechanism within the RCMP. Nonetheless, the nature with which this reporting occurs shares many characteristics associated with the joint authority protocol. I & P is part of the "Border Integrity" initiative and as such reports to the NCO Border Integrity, to the Federal Policing Officer, then to the Criminal Operations Officer (CROPS), who in turn reports to the I & P Atlantic Region CROPS Counsel on a bi-monthly basis.

Reporting patterns of the National Security Investigation Section (RCMP) is also worth noting as it entails requirements indicative of other RCMP directed units. This unit reports simultaneously to the "H" Division head quarters (Nova Scotia) as well as HQ in Ottawa. Internally, this unit has a Performance Agreement with the Division Intelligence Office and Balanced Scorecard report, stipulating how the unit will accomplish its goals, due every sixty days. In addition, NSIS reports externally to the Attorney General as mandated by the Terrorism Section in the Criminal Code of Canada.

In summary and in accordance with the proposed security network organizational model, a network shift in reporting styles should reflect a more integrated and/ or external reporting protocol. Rhodes and Marsh (1992) have emphasized this assertion referring to the necessity to focus on other network features such as integration. In practice, the best way for agencies to exchange classified information and circumvent legislative and jurisdictional barriers is through joint efforts. Although integration could still be subject

to challenges, the amalgamation of resources and interests represent a quintessential feature of any security network. In essence, this should result in the improved flow of information between security agencies. In this particular local security network there is a real indication of increasing integration and agency collaboration. However, the mix suggests a mix of reporting styles. Reporting requirements to some extent still force some agencies to remain silo like, but others lean more in the direction of network models. Perhaps the clearest examples of this shift can be identified in the creation of the MSOC and the IBET, which epitomize the engineering of nodal networks. These respective operations provide a working example of integration between separate and distinct nodes. Due to the way they are engineered and the merging of mandates, they encounter less frequent problems with respect to legislative limitations and the provision of a "need to know."

B). Internal Organizational and Political Decision Making

The networked qualities of decentralization and lateralization were previously discussed in the reporting context. The nature and extent of decentralized decision – making taken into consideration with the network emphasis on local knowledge (Shearing and Wood, 2003a) provides a further indicator of networked characteristics. Security networks and networks in general emphasize local knowledge and flexibility, however, flexibility and the emphasis on local knowledge can hinge on the extent of the involvement of traditional command and control operational decision making practices. The degree and extent of senior organizational and political influence in this local response reflects the extent in which this network conforms to the theoretical local ideal.

Thus, addressing the nexus between front line operatives and senior officials determines the role of local authorities in defining their respective operational direction, which has direct relevance to the network attribute of decentralization.

In a pure networked model of security organization, the expectations would be that senior organizational and political officials would have a limited hands – on role in routine decision – making, especially with respect to short – term planning. Table 6.2 outlines the degree of influence that senior organizational and political officials have in determining the local needs and priorities of security and policing network, both from a short-term and long-term perspective. Respondents were asked to rate the role of senior organizational and political officials in respect to decision – making on a scale from "1" being "significant", to "5" meaning "not at all."

Table 6.2: Senior Organizational and Political Influence

Agency	Senior Organizational		Political	
	Long Term	Short Term	Long Term	Short Term
CBSA	1	1	3	3
NSIS	1	1	3	3
HPA	1	1	1	1
I & P	2	2	1 – 2	1 – 2
CISNS	1	1 - 5	1	4
IBET	1	4	1	5
CCG	2 – 3	4	1	5
CIC	2	3	2	4
DFO	3	3	?	?
NCIU	4	4	4	4

Key
1 = Significant
5 = Not at all

In describing the pattern of influence from organizational officials there are a number of patterns worth discussing. The first and primary pattern to note is the manner in which senior organizational officials tend to assert a

moderately high degree of influence over the long-term priorities of this network. Of the ten agencies within the scope of this study, five (CBSA, NSIS, HPA, CISNS and IBET) respondents indicated senior internal organizational officials had a significant degree of influence over their agencies long-term priorities, two (I & P and CIC) articulated unambiguously denoting a high – moderate degree of influence, one (CCG) wavered between high-moderate and moderate and one (DFO) indicated a moderate degree of influence. The only representative to express minimal internal senior organizational influence was that of the National Counter Intelligence Unit (NCIU). This overall response pattern is perhaps not surprising as strategic issues tend to be driven by central and national concerns.

With respect to short-term priorities this distribution changed somewhat in favor of a network pattern. In two agencies there was some shift away from senior involvement. The shift with the CIC was slight as short-term priorities tended to be only moderately affected by senior officials. However, the change within the CCG is more significant in that the influence on short-term priorities shifted from moderate to minimal. Short-term issues and operations require more emphasis on local activities and knowledge, thereby, could explain this shift. This shift better represents the operations attributed to networked model expectations. Command and control activities appear to function in a decentralized manner; Reliance on local knowledge seems to be unfettered; and from an organizational standpoint, the overall response pattern on short – term operations seem to benefit from an apparent more hands – off approach, thereby allowing for greater flexibility.

As might be expected, the overall political impact on this assemblage as a single entity where long-term priorities are concerned mirrors that of senior organizational officials. On an individual basis there is some deviation as experienced by the CBSA and NSIS in particular. Since the minister in charge of Public Safety and Emergency Preparedness Canada (PSEPC) manages the Threat Assessment Group (TAG),[13] makes decisions thereof and the implementation of the TAG is situation dependent for the province, it stands to reason that political officials would occupy a moderate degree of influence with this agency. In relation to NSIS, political influence declined to a moderate level from that of a significant degree attributed senior political officials.

The most striking features in this distribution were located in the drop of political influence experienced between long-term and short-term priorities within CIC, CISNS and most particularly the CCG and the IBET. Political clout within the long-term operations of the CIC is moderately high, however, this influence declines to a marginal level where short-term priorities are a concern. Similarly, though to a greater extent, operations within CISNS are less influenced by political officials where short-term priorities are at issue.

In general, political influence is limited over short-term priorities and never exceeds the influence applied in long-term priorities. Thus, operational, short-term components of these agencies are left to be managed at the local level. Therefore, local operations tend not to be subjected to political micro – managing.[14]

If we begin with the assumption that this response was previously characterized by those indicative of a traditional bureaucratic approach, then there can be no question that a shift in governance is underway. This assessment is particularly significant in terms of

short – term practices as illustrated in the absence of micro managing. As such there is a certain degree of greater flexibility on behalf of local agencies. However, it should also be pointed out that this pattern is slightly less convincing wherein internal organizational officials are concerned. This leeway is less evident with respect to long-term priorities as they remain primarily determined from a central authority. Essentially, as a network, priority setting differs between the establishment and administration of long-term and short-term priorities.

This response pattern suggests that organizational and administrative limitations will likely persist with network approaches in national security matters. Ultimately, the real test of network theory in this regard, is to what extent local matters are determined at the national level.

Establishing Local Priorities

The next logical step in this process is to take into consideration the role of these local security agencies in determining their own priorities and requirements (See Table 6.3). Responses to this line of inquiry will both verify and support the previous findings, thus substantiating the capacity for organizational flexibility inherent in this local network. To accomplish this task, respective agency representatives were asked to rate their level of influence in determining their own resource requirements and identifying their operational priorities as marginal, extensive, or some place in the middle. Adherence to networking qualities would be exemplified by extensive influence over these two elements. This issue prompted an eclectic range of responses. Only one agency representative had indicated that they had extensive influence over their own local

Table 6.3: Agency Influence

Influence	IBET	CISNS	DFO	CBSA	HPA	I&P	CCG	CIC	NCIU	NSIS
Extensive	x									
Marginal							x	x	x	x
Other		x	x	x	x	x				

*The "Other" category reflects responses, which fit into neither extreme, but were based on a number of multiple and/ or mitigating contingencies.

activities. The respondent from the Integrated Border Enforcement Team stated,

> Extensive...who's to know better than me what is required to do the job and what is down here.

Four other representatives suggest that they have marginal influence in determining their resource requirements and priorities. Five of the ten respondents could not provide a clear concise response to this question. For example, the respondent from the Department of Fisheries and Oceans based his response on what he would be able to accomplish, provided a specified amount of resources are in place. The DFO Director noted that they establish their priorities and resource requirements up front by stipulating what that organization can accomplish with a designated amount of resources. Such a response is suggestive that this agency retains a certain degree of control over its own operations. They identified the capabilities with the current resources available and leave it to senior officials to decide if they wish to expand on these operations. If so, they must provide more funding. This response suggests that among some agencies, the extent of security provided lies squarely in the hands of senior central figures and what they are willing to spend.

With respect to resources and thus possessing the capacity to properly carry out its local priorities, the Bureau Director of CISNS articulated

> That doesn't really affect me... we are always on secondment... [Employees] are begged and borrowed... there is a need for analysts and intelligence investigators, not operational investigators.

This response highlights resource deficiencies and a lack of understanding on behalf of senior managerial and political authorities for the necessary requirements to perform a given task. However, this response also points to the flexible nature of the unit despite such resource deficiencies, thereby demonstrating characteristics indicative of networks.

The CIC director of operations thought they were "on par" with other agencies and the majority of their influence was derived by way of "inventory reduction." He expressed,

> We don't always get what we want... there is a difference between what we need and what we get.

This latter comment raises a concern which is the primary factor plaguing the remainder of the respondents. There is a direct and logical nexus between determining priorities and administrating the performance of those priorities. This is inextricably tied to funding and the role of the Treasury Board to supply adequate resources to fulfill the defined objectives.[15] In this regard, the NCO for Immigration and Passport Atlantic Region pointed out, there are a number of "push and pull factors" that come into play in making such a determination. The occurrence of some unexpected incident such as the Swiss-Air disaster would take precedence on the list of priorities for all agencies. It would appear that the struggle for inclusion on the resource gravy train is universal. Requests can be forwarded to Ottawa from the Regional CBSA operation itemizing a "priority" to be involved in a particular JFO and involvement depends on how much the Treasury Board wants to dedicate to that initiative. This scenario plays out with the CCG, and NCIU as well. In the case of NCIU, they have complete control of the resources once it is dedicated to the unit; however, they are given little voice in the development of the

budget and are required to adjust their activities in accordance with the budget. By default, budgetary restrictions have an impact on local priority setting. This arrangement has clear impediments to regional activities inherently affecting the full possible extent of security operations. The situation with respect to NSIS provides a bleaker image. The NCO i/c "H" Division noted,

> Nova Scotia has very little influence on the National Scale of resource allocation.

Reflecting back upon the comments of the respondent from the IBET as noted above, the designation of local expertise in needs and priority assessments do not appear to be a universal characteristic among all of these agencies. Centralized funding for local security networks still effects and directs strategic activities. Through knee jerk reactions, these central decision – making authorities are creating a murky security environment whereby there is no clear direction and new policy is being implemented without the necessary provision of ways and means to actually implement this policy (Interview 5).

In Chapter five the manner and extent in which other agencies or "nodes" impact on one another's ability to make decisions was examined. This chapter has expanded on this assessment taking into consideration senior organizational and political leadership's influence in determining future agendas and the course of direction. With few exceptions, senior organizational officials still retain influence on long-term and short-term priorities of local security agencies. However, this influence appears to be less prevalent where short – term operations are at issue. Nonetheless, in terms of efficiency and possibly effectiveness, this revelation is somewhat disconcerting given the level of possible disconnect between the political jostling occurring centrally among senior officials and the "ground beaters" (Interview 1) regionally situated attempting to perform a specific

task. The retention of centralized power and decision – making response detracts from local efforts to properly vet what they perceive to be matters of concern and employ strategies best able to address these concerns.

In a similar pattern, though to a lesser extent, political influence also sets the agenda for local and regional operations. Influence from political sources comes in the form of policy and long-term funding, thus limiting the extent and scope of operations. However, short-term, active initiatives tend to be immune from political interference.

Determining priorities is largely a product of senior organizational and political officials. The one and only exception to this rule can be located with the increasing utilization and importance of the IBET and the "Smart Border Agreement" with the United States. Thus, given this unit is governed by an International Joint Management Team, its autonomy could be by virtue of the existing integrated relationship with the United States and at the behest of the same.

In Summary, significant remnants of the traditional bureaucratic model of operations still exist within this local security response. Local efforts still remain reliant on federal purse strings, which in turn can either impede or advance the capacity to be adaptable. Nonetheless, there are also clear indications that a networked shift in organizational practices is emerging.

Summary

This chapter was developed to explore the scope and parameters of how this local security network determines its own priorities and decision-making abilities. The research findings generally suggest a transformation in organizational models is

underway. The increased establishment of ad hoc joint force operations, creation of the Maritime Security Operations Centre and Integrated Border Enforcement Teams all represent a shift in traditional operational dynamics. This emerging shift is reflected in the evidence of a decentralized command and control structure, where authority is increasingly shared in joint activities and mechanisms with other security While traditional vertical command and control structures still remain in place, it often operates in conjunction with others, rather than in complete isolation of others..

While general and long-term decision-making and priority setting still remain under the auspices of senior organizational and political authorities, there is evidence suggestive of a slight shift in local influence within this process. Restrictions or limitations placed on this local security effort do not appear to be concerning a threat to local knowledge, but rather one of budgetary restrictions. Agencies are required to justify their presence in joint force operations and find themselves limited in the scope of their operations by resources and circumstances or events that take priority over security initiatives, thereby utilizing financial resources that might have otherwise been designated for such purposes.

CHAPTER 7

NETWORKING CHARACTERISTICS: ADVANTAGES, DISADVANTAGES AND PROBLEMS

Organizational theorists, policy analysts and managers have portrayed networked organizations as a necessary and advantageous form of organizational structure in the management of security threats. Networks are seen as being much more compatible and appropriate than the cumbersome traditional bureaucratic response largely as a result of their inherent flexible nature. Castell's (2000, b) has argued that networks possess the flexibility and adaptability required to respond to security threats in the current global environment. Newly developing information and communication capabilities have minimized impediments to its successful implementation. Shearing and Wood (2003a) and Lebkowsky (2000) have further commented on the advantages attributed networks to focus on "local" capacity and knowledge. However, given the lack of empirical research in the national security environment as acknowledged by Dupont (2004), concerns still exist as to whether pre-existing traditional organizational limitations that have plagued developing networks in the past have been resolved. Historically, concerns about networks have emanated from the complexity of a multi-agency, inter-connected effort and the subsequent inability to provide effective leadership. This is problematic due to the diffused manner in which they operate, devoid of a central command and control mentality (Dupont, 2004, 78). Concerns exist which are also connected to such complex organizational arrangements and the capacity or willingness to cooperate and coordinate efforts, focus shared resources and manage complex tasks (Castells, 2000a; Lebkowsky, 2000).

In an effort to further determine and verify the validity that security and policing operations have undergone a fundamental transformation from a traditionally organized model to a post-modern networked model of security provision, attention will now be focussed on the perceived advantages and disadvantages associated with networks as a model of organizational operations. This is addressed by first considering specific attributes ascribed networks and then allowing for more generalized comments.

Perceived Advantages and Disadvantages of Networked Organizations

Closed Questions

Network Advantages

As previously mentioned, networks possess the inherent qualities of adaptability, greater effectiveness and tends to emphasize local knowledge. It is through the flexible nature of networks that greater effectiveness is achieved and therefore better equipped to address the perceived perpetual evolution of security threats. Emphasis on local knowledge provides a significant contribution to securing societies from security threats as events unfold on a local stage. Through the collection of local knowledge from multiple localities a more comprehensive picture or assessment can be developed. This is the nature and purpose of intelligence gathering and risk management.

Respondents were asked direct and specific questions relating to these advantageous characteristics specifically ascribed networks in relation to their respective experience. This line of questioning had a dual purpose. First, it tested claims of a shift in network qualities. Second, it provides a basis onto which the current local assemblage adheres to this network re-conceptualization. The results were mixed, but nonetheless moderately

consistent to what might be expected from a networked model of organization in an evolutionary stage. Responses were based on the perceived significance of local knowledge, organizational adaptability and effectiveness.

Table 7.1: Network Advantages (n = 10).

Advantages		
Local Knowledge		
Important	Less Important	Other
10	0	0
Adaptable		
Yes	No	Other
5	4	1
Effective		
Yes	No	Other
8	1	1

Local Knowledge

All ten respondents were in agreement with respect to the criteria of local knowledge. It was deemed as being a very important aspect to the respective agencies day-to-day operations. The respondent from the IBET articulated,

> This is a small province here. Local knowledge, that's where it all starts, a guy can be standing down on the wharf and see something suspicious... Locals are more familiar with what is out of place.

The importance of local knowledge is further heralded by the respondent from DFO who noted, "Something that may seem totally out of whack, locally, we can say, well that's not unusual... We can understand why something is happening instead of pushing the panic button." Another respondent simply stated, "You have to know the players who pose a threat (Interview 8)."

While there was unanimous consensus with respect to the importance of local knowledge, some qualifications were discussed. The well - spoken respondent from HPA likened the comparison to one of tactical and strategic problem solving, commenting,

> One can't operate without the other... Bush fires can be put out tactically (local). Forrest fires are strategic (national).

This characterization is consistent with a comment forwarded by the representative from the Canada Coast Guard who stated, "We are not an intelligence organization... Intelligence flows through others and is national for operations." This characterization functions to differentiate the intelligence component of the security response from the other elements.

Adaptability

It is suggested post-modern network models have a better capacity to adapt in changing environments and situations (Castells, 2000 a, 695). Responses from this sample illustrates 50 percent of the representatives were in agreement with this assertion. Of the other five respondents, four were of the opinion it was not more adaptable, while one was uncertain. Of the five in agreement about the present security organization being more adaptable than previous efforts, attention was dedicated to the virtues equated with integration and equality. For example, the representative from the IBET commented,

> Before the IBET's the RCMP tried to do it all themselves... [Now], if I can't do it, this guy over here can.[16]

Another respondent expressed satisfaction with the notion that "more plans have been put into place now" and are no longer collecting dust (Interview 2).

But this assertion would be challenged by the comments offered by two other representatives who contend that there is much pontification being manifested. The overwhelming consensus among the naysayers evolved around the principle that there is a capacity to be more adaptable, but this has not materialized as of yet. Unrelated to the aforementioned, the respondent from NSIS remarked,

> In some cases it may be [more adaptable], but we are still mainly reacting to incidents as they occur.

The undecided participant simply noted that he did not know enough about the internal mechanisms involved in this elaborate process, but remarked adaptability is negatively affected by the proliferation of internal feuding still existing in the security community (Interview1).

Effectiveness

Due to the qualities of networked models and the manner in which information is disseminated, it is contended they are more effective then traditionally oriented organizations at mitigating or circumventing threats to national security (Shearing and Wood, 2003a; Dupont, 2004). As illustrated in Table 5.1 there is a slightly higher agreement ratio to this criterion than the previous one. Six of the ten respondents believed the present apparatus is more effective than previous initiatives. While there is significant agreement among participants that this initiative is more effective, some respondents in agreement still voiced some reservations. One person qualified his support by noting,

> Things are working very well with other agency counterparts, [but we] can do better without question... Nobody is throwing up roadblocks... We are working together to achieve universal goals (Interview 5).

Another tempered his enthusiasm by stating,

> Yeah, [people are] more willing to talk... [They] always did talk at the upper levels... [They] did at the local level too, but it has been streamlined... [But there still remains] problems with institution to institution [communication] (Interview 8).

This respondent cited institutional "clicks", institutional barriers, cultural barriers and the "need to justify [their] existence and worth. The respondent who was ambivalent about the effectiveness of the present initiative expressed concern with respect to the continued dedication to work together. Immediately following the events of 9/11 the representative from CIC noted

> There was a greater degree of receptivity to work together... It is starting to diminish a bit now.

One respondent was disenchanted with the present effectiveness citing concerns with legislation,

> I think it is less effective... The Privacy Act and Access to Information causes conflict... Information should be more available to those protecting the country... Canadian society has to determine what they want - there is a cost (Interview 8).[17]

There is some indication from the various comments that a shift in models has indeed occurred – at least where network advantages are concerned. This is born in the pattern of responses to these network advantages. Nonetheless, concerns still exist among some representatives with respect to the capacity of this security grouping to adapt and maximize its effectiveness. This suggested feature could be explored further by considering the disadvantages historically attributed networks.

Network Disadvantages

In conjunction with inherent advantages, networks have been described as being accompanied by inherent specific disadvantages. Many disadvantages associated with networks are remnants inherited from previous network models. However, not all

disadvantages should be categorized in a similar way in part due to the possibility that some are more accurately reflective of problems that can be overcome, rather than negative bi-products, which are inherent and permanent. Disadvantages or problems traditionally associated with networks are outlined as follows; 1) they are complicated with no clear direction, 2) they have ineffective leadership, 3) suffer from difficulty in coordinating various agencies and functions, and 4) experience difficulty focusing resources and managing complex tasks (Shearing and Wood, 2003a; Castells, 2000a).

Table 7.2: Network Disadvantages (n = 10)

Disadvantages/ Problems		
Complicated		
Yes	No	Other
6	4	0
Effective Leadership		
Yes	No	Other
4	1	5
Coordination		
Yes	No	Other
5	4	1
Focusing Resources		
Yes	No	Other
6	4	0
Managing Complex Tasks		
Yes	No	Other
6	2	2

Again, respondents were posed direct questions about these specific characteristics. While these results were mixed and the correlation is not overwhelming, they are nonetheless suggestive of a network in transition.

Complexity

Six of the ten respondents were of the belief the present network arrangement is more complicated and could benefit from a more clear direction. One respondent voiced concern regarding the lack of formality and direction from the government to make the sharing of information mandatory (Interview 8). In a similar vein, another addressed the necessity to consider the security population as a whole (Interview 1). This is particularly relevant if we begin with the premise that national security cannot be decentralized. Still another referred to the ongoing changes with the MSOC's and growing pains experienced in that context (Interview 7). The same respondent raised concerns with respect to the expeditious manner in which the apparatus was developed. Perhaps the most significant comment was raised by the representative from I & P who articulated the need for the "harmonization of mandates and priorities." This comment encapsulates the gist of the concerns as a whole.

Comments to the contrary, depicting the present climate as not being complicated generally described the process as evolving at a good pace. The only exception was with the National Security Investigation Section (RCMP), which receives "plenty of direction" from Ottawa. This comment demonstrates the continuing adherence to traditional bureaucratic models.

Effective Leadership

Ascertaining a sense as to effective leadership is possible under the current security effort prompted a myriad of non-committal responses. The only representative questioning the assemblage's capacity to provide effective leadership did so half

heartedly by stating it was "not necessarily" possible to do so. From his own unique position he noted, "We are clear where we are going" as it was decided by a single governing body (Interview 7). Notwithstanding this minor anomaly, representatives could definitely foresee the possibility for effective leadership, though difficult to accomplish with competing cultures, priorities and the ever-present turf wars (Interview 4). Other limitations emphasized a limited capacity to accomplish this task due to the size of the response. The preponderance of responses that occupy the "Other" category was of the opinion that the overall response was not really decentralized. The respondent from the Criminal Intelligence Service Nova Scotia summed it up best by noting, "security matters cannot be decentralized." Given this pattern of responses, effective leadership or lack thereof, might better be characterized as a problem rather than a disadvantage.

Coordination

According to network theory, the task of coordinating the efforts of multiple agencies can be both difficult and cumbersome. Within the scope of this sample five of the ten representatives characterized this present initiative as having properties, which are difficult to coordinate.

Of those in disagreement with the idea that the present arrangement is difficult to coordinate were CCG and DFO. As these agencies see themselves as having a supportive function and for the most are carrying on their respective daily activities it should be of little surprise that they see no problems in this respect. The other two dissenting agencies are RCMP lead units and have previously characterized their respective operations as centrally coordinated. In response to the question one respondent noted,

> From where I am sitting and who we deal with I think it works rather smoothly... It works even better with the secondment of a CBSA person on strength to our section (Interview 9).

Of mixed opinion was the respondent from the Integrated Border Enforcement Team (also RCMP lead) who acknowledged some problems with coordination, however qualified it by noting, DND, DFO and the CCG "are going through some major changes... [But} the RCMP is running as well as it can be."

The remaining five agency representatives expressed concerns with government regulations, mandates, resources and priorities. The NCIU representative discussed problems relating to resources, time constraints and differing priorities. Ranking priorities differs from one agency to the next. The representative from the HPA who suggested in order to meet the same goals you need consistent and compatible regulations buttressed this sentiment. In a similar fashion the CISNS Bureau Director voiced concerns about mixed mandates, overlap and long-term strategies.

The comment voiced by the respondent from the CBSA cautions any pre-designation of coordination as a disadvantage. Instead, criticisms of coordination would better be described as problems, which can be resolved. He noted, "coordination is always a little difficult, but you can get it done." Interestingly enough, this remark is qualified further by the representative in relation to the focusing of resources.

Focusing Resources

From a historical context, networks have encountered difficulties focusing resources "around centrally defined goals, achieved through the implementation of tasks in rationalized vertical chains of command and control (Castells, 2000a, 15)." The issues

addressed by the six respondents expressing concerns with focusing resources fell into one or both of two categories, 1) Patterns of Dissemination and/or, 2). Priorities and Mandates

As described in the previous section, one agency representative shared some concerns he had with the distribution of resources:

> It is difficult to focus resources because it is to one group... [He emphasized] but that is part of our job, where is our money... [The] Mounties set up groups, invite us in, but we have to pay to have a man there (Interview 2).

Another respondent emphasized the inability to focus time and resources on any one area for an extended period of time due to the vast scope of the agency's responsibility in comparison to the capability associated with the exhaustive stretching of resources (Interview 8).

The other impediment to effective resource management is once again related to priorities and mandates. The representative from Citizenship and Immigration Canada perhaps summed it up best by commenting,

> Yes, [it is difficult to focus resources] because of competing priorities... We are living in a very fluid, ever changing environment... [Therefore], what is a priority today is not necessarily a priority tomorrow... It could also be a case of priority overload.

Incorporated in this quagmire of obfuscation is the balance of competing objectives in this apparently fragmented initiative. Reconciling conflicting mandates and the lack of any sense of an overall strategic goal results in the blind disbursement of resources to no apparent end. One respondent spoke to this concern referring to the "quantum gap" that exists between federal policy and what the real threat actually is (Interview 5). Another respondent reflected upon conflicting mandates with no overall strategic goals. He noted that money was being spent, but questioned where it was being spent (Interview 1).

However, there is hope that this shortcoming can be resolved as another respondent suggested that they could benefit from clearer direction but there might be a "harmonization of mandates and priorities" in the future (Interview 9).

Managing Complex Tasks

The final disadvantageous characteristic directly attributed network models are the innate lack of ability to manage complex tasks beyond a certain size (Castells, 2000a). Results from the data are marginally consistent with this characterization in the case study before us. Impediments to efficiently and effectively managing this task are related to resource allocation, personal attributes and organizational perspective.

In the instance of the latter qualification, complex tasks represent a problem rather than a characteristic. The representative from Immigration and Passport noted "everybody has their limitations," but such matters can be resolved "through integration" and tackling it as an organization and not "program specific." The respondent from the Halifax Port Authority credited the challenge to one of managerial and leadership qualities. Metaphorically likening the task to a "web of interconnectedness," he commented,

> If you don't have the skills you won't do it... You are either the right person or not... you need to be able to deal with personalities and mandates... Have to be able to deal with new security agencies... Have to deal with everybody's issues.

Finally resources are at the forefront once again on the list of factors contributing to the inefficient managing of complex tasks. The representatives from the Canada Border Service Agency, Citizenship and Immigration, Criminal Intelligence Service Nova Scotia and the National Counter Intelligence Unit reflected on such concerns as inadequate

training, resource allocation, budgets and changing philosophies. The number of agencies involved in an initiative and lack of resources can complicate, drop or shelve some well - intentioned projects. Many agencies find themselves requiring an infusion of resources to manage current responsibilities, thus by default also competing for a larger share of the security pie.

As might have been expected given the pattern of responses to network advantages, so too was the response pattern mixed with respect to corresponding disadvantages. This further lends some support to the argument that security efforts are undergoing some transformation. However, it is also suggestive that some historical characteristics of networks still persist in the present arrangement. Having said this, it is important to recognize that some of these disadvantages are not necessarily disadvantages at all, rather problems that can be overcome. The notion of disadvantages implies an omnipresent feature, however, as noted above, some shortcomings can be managed and rectified with due diligence. As one representative noted even the distribution of resources could be resolved through the art of "compromise and negotiation" (Interview 8).

Open Ended Questions

Dupont (2004, 77) has argued the transition to a "decentralized, horizontal, networked society...[has] been instrumental in the collapse of all sorts of barriers that previously corseted institutions, organizations, communities and individuals...." At the outset of this section I hoped to discover whether or not the positive and negative characteristics attributed networks as described by Dupont were actually consistent with the present day dynamic. To this end, respondents were asked open-ended general

questions on the advantages and disadvantages associated with working in the security environment, as it presently exists. Responses could be classified in one of two general categories that I have identified and categorized: 1) "functional" advantages or disadvantages/ problems associated with cooperative efforts or 2) personal advantages or disadvantages/ problems associated with cooperative efforts.

Functional Advantages

The mix of **advantages** described by respondents varied extensively. The nature of these benefits incorporated such critical elements as maximizing functional and personal components in the overall response. Topping the list of benefits associated with the present day arrangement is the belief that under the present arrangement that resources are better utilized. One respondent noted that an integrated approach allows for a concentration of resources towards a common task (Interview 1). In this vein, the respondent from the CBSA added, "Integrated teams work on one issue...[thereby allowing for better] targeting." This approach eliminates the "duplication and triplication" of time, resources and effort. Another respondent noted in addition this "allows deployment of resources to other issues (Interview 10)."

The second major advantage cited by respondents was the idea of having mutually compatible training. Officials from various agencies and societies are often better able to understand each other's regulations when they use similar and compatible training. The respondent from Immigration and Passport (I & P) articulated "problem solving techniques sensitizes others to the problems we face." This is a reciprocal relationship as officials visit other countries such as China and Australia in an effort to appreciate the

hurdles faced by their counterparts abroad. In the end these problem-solving techniques results in the promotion of "best practices."

It has also been contended the present network arrangement is more conducive to the sharing of information. Section 8.2, paragraph "E" of the Privacy Act refers to the "Consistent Use" clause as utilized on matters concerning common tasks. This allows for ready access to necessary information. The respondent from NSIS also referred to the benefits of working in an integrated fashion resulting in the "better exchange of information." Encapsulating the core tenets was the comment from the IBET respondent, who noted,

> [They have] access to a wealth of information you normally wouldn't have... Kind of makes everything seamless... There are five agencies instead of one... [There are more resources and information as a result, which makes it possible to do more.

Functional Disadvantages

While the present security arrangement has its advantages, these are often accompanied by **disadvantages**. It was previously noted; working on a common task lends itself to the better utilization of resources. However, concerns have been expressed with respect to the distribution of resources. One respondent noted,

> The feds (sic) are trying to recuperate...budgets are being reduced... [they want] more for less... When you collaborate you draw efficiencies, but they will only go so far... When you see how the pot is divided up and who is in charge of it... I'm not too sure it was well thought out (Interview 4).

The primary concern in this situation seems to be focused on who is provided the financial resources as they relate to JFO's and how these resources are utilized and dispersed among member agencies. Other resource concerns relate to long-standing habitual practices. One respondent stated,

> You can throw money at a problem, but you have to be willing to do things differently (Interview 4).

The respondent proceeded to pose some interesting considerations when assessing integrated intelligence and enforcement efforts. Included among these concerns were questions related to how successful and effective they are? Do they constitute and actual improvement, and what are the actual relationships (Interview 4)? These questions instill a sense that more work is required to develop a better understanding of the benefits with emerging trends. They also underline the fact that this kind of research has until this point escaped any empirical and networked examination.

The remaining significant issue expressed by respondents is the nature of Federal legislation. Several respondents noted the impact the Access to Information Act, Customs Act and the Privacy Act has on security operations. Of primary concern is the way in which these acts impede and prohibit the dissemination of information. For example, one respondent noted the Privacy Act post 9/11 interferes with voluntary releasing of information to other agencies (Interview 2). Instead of providing the whole file, certain agencies are now required to limit what they release to the specifically requested information (Interview 2). The result is that certain information of relevance might go unidentified. This could feasibly pose some problems, as certain details might appear inconsequential unless taken into context with other information with other information that only one party is privy. Thus, common practice is to suggest, "Maybe we should work together." This inhibiting feature challenges the network principle of a seamless flow of information. The sharing of information remains hindered by legislation prohibiting its free exchange.

Personal Relationships: Advantages

Networks are based on the philosophies of communication, openness, collaboration, effectiveness and inclusion in the shaping of the process. Rather then proceeding through traditional hierarchical formal channels, information is hypothesized to occur by way of an informal interconnected process or mechanism (Shearing and Wood, 2003a; Dupont, 2004; Castells, 2003a). As such, personal considerations and attributes of this network security response mitigate and/ or aggravate its efficiency, thereby representing a quintessential concept in this analysis. For example, one respondent had noted that the present effort is contingent on building personal relationships and they are in the "people business" (Interview 8).

Developing and maintaining inter-personal relationships with other network participants is a necessary factor in establishing an efficient and effective security response. Through the process of working in conjunction with other agencies on a common task there is a greater capacity to develop broader personal networks and reinforce existing knowledge bases. The DFO Director of Maritimes Region noted,

> The whole networking... getting to know people, putting a face to the name... it is nice to have a forum where you can begin to understand the security agenda.

In a similar fashion another respondent thought the process was more conducive to developing new contacts and learning new ways of doing things; seeing how other agencies go about their respective operations (Interview 2). This personalized quality lends itself to the building of stronger foundations with other agencies, or at least certain individuals within these agencies.

Broader systemic advantageous features exist as well. Advantages stem from the ability to express agency concerns in relation to its position and abilities vis-à-vis the

overall security agenda. In the broadest sense, the respondent from Citizenship and Immigration Canada (CIC) noted this coordinated approach allowed for a better understanding of departments, individuals, mandates, objectives and specific projects. Furthermore, options are built upon due to the stream of ideas coming to the table (Interview 1). Building upon this comment, benefits are realized with the participatory nature of early "sign-ons" to government programs, thus providing a voice and opportunity to assist in lessening the impact and frustration resulting from evolving government policies. Early involvement lends itself to the ability to "proactively communicate why policy is developed and implemented" as well as provides an opportunity to "change government perspectives" about the industry (Interview 5). A strong and informed understanding of the overall initiative from the onset better assists in lowering resistance to change. The DFO Director commented,

> If we had to change our priorities it is easier if we understand the priorities as part of a team... [Thereby providing the opportunity to] better understand what is important... and how we as an organization can better fit into the agenda.

Key to the concept of networks is the element of informality since information is transferred from one node to the next in a seamless fashion. Positive comments stemmed from the integrated nature of operations. The respondent from IBET remarked,

> Mine is unique, it is integrated... My agency is part of an integrated team... everybody else has an equal say at the table... The stolen boat mentioned in the news recently... if there was no contact here it would not have been identified.

The informal protocol established within this integrated team proved to be essential for this incident to be resolved in an efficient and effective manner. It further illustrates the equal footing member nodes enjoy as part of this response, thereby suggesting adherence to network qualities.

Personal Relationships: Disadvantages

While personal qualities can assist in nurturing and building greater cooperative efforts, they can also hinder or limit an efficient security response. One respondent stated,

> Personality can sometimes be a problem... I have seen trust dismantled (Interview 1).

The respondent from the IBET reiterated this concern,

> Sometimes people (1 or 2) in other agencies do not put the importance on the relationship itself... [They] don't want other people treading on their territory.

This comment highlights two problematic characteristics of the current network. First, it speaks to the omnipresence of institutional turf wars. Second, it suggests that this limitation is not department wide, but present in the psyche of particular persons.

The development of new policing and security agencies can create conflicts from an organizational standpoint even within the confines of one parental department. In discussing difficulties in establishing his unit, one respondent cited a lack of understanding as to individual agencies functions stemming from insufficient or total omission of "higher ups" to properly educate other agencies and units as to operational activities of his unit and those of confederate security agencies (Interview 7).

Organizational and cultural factors can impede efficiency of security networks. A number of comments were directed towards organizational cultural matters and the historically pervasive concept of the struggle for perceived power. The respondent from NSIS clearly and concisely articulated,

> Some organizations believe information is power and are reluctant to exchange the information and risk losing this power.

Such remarks are highly suggestive that the present network incarnation has not entirely resolved this pre-existing problem associated with earlier networked models. Individual

agency goals and priorities still continue to persist. It is reminiscent of an individualized approach rather than a one built on consensus. Another respondent cited cultural biases and philosophies, as being a detriment to a concerted effort as the mentality lends itself more readily to thoughts of superiority in the task at hand (Interview 8). This counter productive approach is more in line with "closed" organizations and a thought process indicative of a "we can do it best philosophy."

Informality can also be accompanied by concerns related to personal and organizational distrust and the proliferation of power struggles. One respondent noted,

> Agencies are still looking after themselves... we use information for our selves... All the agencies do that...(Interview 2)

The respondent elaborated further noting,

> We were hoping all information would come together (following 9/11)... Ask any intelligence agency around the world, they would say you need all intelligence under one agency... We don't take information at face value. We do an investigation into the information (Interview 2).

Perhaps the most significant negative feature associated with the issue of formality emanates from the option to forego cooperation in its entirety. An informal process by its very nature lacks formal regulations. One respondent expressed concern with the fact that this informal process leaves the decision to cooperate up to the individual representative (Interview 8). They are not required to share information.

In summary, general open-ended questions elicited a mixed bag of responses. While some respondents discussed functional attributes such as the ability to focus resources, synthesize training and share information as proving to be extremely beneficial to security efforts, others have referred to budgetary and legislative impediments hindering such efforts. In addition, personal and organizational characteristics resulted in no consensus. The informality of networks was classified as a benefit and a weakness.

Priorities and turf wars still permeate throughout the overall response. However, understanding ones role in the overall response was seen as a possible attribute.

It has been suggested that networks have undergone a transformation wherein many of the historical problems attributed this form of organization have been resolved (Shearing and Wood, 2003a). While general comments pertaining to the operation of the present national security apparatus manifests some consistency with networked expectations, the suggestion that previous network problems have been overcome might be premature. Similarly, advantages might be overstated. As has been the case with the other networked characteristics discussed in this chapter and previous ones, the results have been mixed.

Table 7.3: Summary table as response to perceived advantages & disadvantages of network organizations

Advantages	Disadvantages
Functional	
- Utilization of Resources	- Distribution of Resources
- Eliminates Duplication	- Too many agencies (Fuzzy objectives) – Overly complex
- Compatible Training	
- Sensitizing and Understanding	- Legislation
- Access to Information	
- Improved Targeting	
Personal	
- Building Relationships - Cooperation	- Informal = Not forced to share
- Changes Perspectives	- Cultural biases/ philosophies
- Optimal Positioning	- Trust Issues
- Provides a voice	- Information is power
- Less Formal	- Personal Relationships
	- Competition

Summary

The purpose of this chapter was to identify and describe the advantages and disadvantages experienced by respondents in a local security network. This was

accomplished by first asking participants to consider more directly relevant considerations associated with the network paradigm, then providing participants with an opportunity to reflect on general open-ended questions regarding the perceived advantages and disadvantages of the local apparatus. The combination of these two probing methods of inquiry has highlighted two critical points. First, responses have indicated that the bifurcated definition of advantages and disadvantages is too simplistic. In reality, as expressed by respondents, some disadvantages are simply problems that can be alleviated and not disadvantages, which imply a state of perpetuity. Second, this chapter has demonstrated that participants in this local security network perceive their organization and operations in some instances as functioning in the ideological network fashion, but at other times perceive it to be more consistent with the traditional paradigm – fragmented and in conflict.

From a theoretical perspective, the advantages attributed network models paralleled the responses with the exception of adaptability, which resulted in greater ambivalence. . There is a general overall sense among respondents that the present arrangement is more effective and emphasizes the importance of local knowledge. However, given prior comments concerning the local lack of influence in determining local priorities, the significance or bearing of local knowledge is tempered. This reality reflects previous comments suggesting many security matters are centralized (ie: Interview 1; Interview10).

Consistency among disadvantages is less convincing, though still manifesting characteristics attributed early impediments of networked organizations. This is suggestive that such shortcomings are not easily overcome in this competitive and

evolving security response. However, patterns of responses coupled with the general ambivalence and specific references to a capacity to overcome or circumvent certain impediments speaks to the utility of a networked approach void of the lumbering knee jerk reaction indicative the bureaucratic approach.

From a practical perspective general comments provide a useful tool for the practitioner. Advantages, disadvantages and problems varied and in some instances occupied a place on both sides of the argument. Relationships have been built and nurtured among this grouping, but they have also been dismantled. Resources have been better utilized, disposing of overlap, but they have also been a source of discontent in the manner they are distributed. The less formal manner in which this grouping functions has made the sharing of information more seamless, however, simultaneously, concerns have emerged with respect to the fact this informality leaves the sharing of information up to the individual.

Essentially, there is a lack of consistency and a predominant ambivalence among this response pattern. In addition, long - standing traditional organizational hic-ups remain as prevalent today as they were prior to the events of 9/11. There still remains significant traditional organizational cultural biases; the "information is power" mentality still permeates in the minds of people and agencies; The inescapable reality of personal characteristics are also voiced; And, supposed better access to information is impeded by legislation, the "need to know", and 3rd party rules. These vexing factors, whether remnants from previous networked initiatives or features of the traditional bureaucratic model, has not hedged or hindered current efforts completely. Greater opportunity exists to learn from other agencies within this arrangement and develop a new perspective and

appreciation of each other's roles, attributes, capabilities and concerns. Thus, the role of dialogue is a quintessential factor in the overall response. After all is said and done, these mixed responses suggest that the local security network does not operate in strict adherence to the hypothesized models as described by Castells, Dupont or Shearing and Wood but is most likely still in a transitional stage of maturity.

CHAPTER 8: CONCLUSION

Confronted by an increasingly sophisticated and ever evolving terrorist threat, security and policing agencies have been forced to respond in a more efficient, effective and flexible manner. It has been hypothesized this reform has created a change in the way security organizations function, distinguishing themselves from a traditionally based bureaucratic approach to one of networked governance. This research has set out to test the salience of this hypothesis by examining network qualities of a local security complex. During the course of this study, key features attributed to networked operations with respect to national security departments/ agencies/ units have been examined. This study represents one of the first empirically based academic examinations of security networks and tests the potential consistency or inconsistency of network theory.

By examining the established key network qualities through the perspective of local security representatives, this analysis substantiates claims that a networked model of governance is emerging in the security environment. However, this verification must be accompanied and tempered by a degree of caution. While this analysis has indicated a "shift" in the organizational characteristics of a local security and policing practice from traditional to networked qualities, such a claim might be premature when attempting to apply this argument in broad, generalized sweeping brush strokes. The results of this study are indicative of a shift in its initial stages, its final incarnation is yet unknown.

This final chapter is dedicated to revisiting the salience of network theory as suggested through the perceptions of those representatives within a local security and policing network. This section will summarize the findings and identify the key qualities that define this local security network, how it is structured, its respective activities,

relationships, network advantages and disadvantages and network governance. The current state of postmodern policing will be examined as it relates to a unique security and policing milieu. Finally, directions for future academic endeavors are explored. This will highlight limitations to this study and emphasize a strategy of "best practices" in future research.

The Utility of Network Theories

Current discourse on security initiatives suggests there has been a radical transition or shifting in the way efforts are organized and conducted. If we begin with the assumption that previous efforts were characterized by traditionally bureaucratic qualities, then, this case study indicates that there is a transition in motion. Nonetheless, it is also true that this security response is also characterized by the more traditionally based organizational structures and practices.

This local security network is characterized by increased joint activities among and between the ten various agencies surveyed. Integrated activities possess the inherent capacity to be more receptive to the network qualities discussed in the preceding chapters. However, the extent to which this transition will come to dominate the organizational structure of this local security network and operational activities of the nodes within this network remains unknown at this early stage of development. By highlighting certain key qualities that assist in defining this local security network, we will be in a better position to determine what stage in this transitional process has been achieved.

Mandates & Activities

Understanding security mandates is a binary process. At one end of the spectrum, one must understand what is mandated. On the other end, one must understand and appreciate what is not mandated. Within the operations of this local security network, there is some evidence of overlap and disconnect where mandates and activities are concerned. For example, as the central actor in the Canadian national security arsenal wherein domestic matters are concerned, the RCMP dedicates manpower and expertise to many local, regional, national and international initiatives. Within the operations of these separate initiatives there is evidence of a fundamental disconnect with respect to the understanding of mandates. The inception of the Integrated Border Enforcement Team is a case in point. As a RCMP lead operation, the IBET found itself in competition with another RCMP lead initiative - NSIS. This internal confusion resulted as a bi-product of the infancy of the IBET program and the lack of oversight by senior organizational officials to properly educate pre-existing units/ agencies. Such growing pains are inherent and to be expected within newly developing organizations. It was incumbent on the NCO of the IBET to educate and seek out potential partners for that integrated unit and sell the virtues of membership.

The distribution of activities and the sheer size of the overall response are still in a transitional period and under pressure to respond to evolving gaps in the security structure. One such gap still persisting is the necessity to securitize waterways. For example, the Canadian Coast Guard possesses the logistical resources to secure Canada's waterways. However, changing the present activities would require changing CCG's mandate by arming and retraining personnel. This multilateralization of policing

activities will require the reallocation of responsibilities, receiving fewer resources or redirecting current resources, thereby detracting from pre-existing, mandated operations. In addition, the shift in mandates and activities are complicated due to the possible reluctance of personnel to embrace the dramatic change in responsibilities. These revelations strongly support a networked shift, but raise concerns that have consequences for the development of an effective networked response.

The IBET epitomizes the concept of nodal governance as increased permanent joint activities and ad hoc joint force operations have the capacity to overcome such security impediments as outdated legislation, third party rules and the need to know.. These initiatives speak directly to a network's capacity to expand in a fluid, seamless fashion. The capacity to expand and adapt is a hallmark feature of networks and is buttressed by comments from the bureau director of CISNS who noted the expressed desire on behalf of other agencies to become a member of the local Bureau and the parent organization - The Criminal Intelligence Service Canada (CISC).

To some extent security efforts have embarked on an age of diversity whereby the multilateralization of auspices has occurred. However, due to the infancy of this initiative, concerns still plague security efforts as crossover and mandates remain points of confusion and territorial contentions. Resolving these matters might prove to be a formidable challenge for local security agencies that find themselves to be marginal members in a larger group of networks. This is in keeping with the characteristics identified within networked models and discourse on security and policing (Shearing, 2005) of organizational structures. It is not enough to understand ones own mandate and

capabilities; one also has to develop an appreciation for the mandates, capabilities, impediments and vulnerabilities of the other members in this effort.

Structure

Structural characteristics provide a significant basis in determining how well this group adheres to the principles of nodal networks. Strict adherence to a network would manifest characteristics such as informal communications, decentralized decision-making, lateral relationships and open to external influence. Such an organizational model in theory is devoid of attributed limitations of traditionally based bureaucratic organizational models. The structural characteristics exhibited in this local security sample appear to be consistent with a network in the early stages of development.

At first glance, the responses to various organizational questions appear to present this consortium as still being centralized, formal and hierarchical. But, elements of a centralized response seem to be an appropriate and inescapable component where national security initiatives are a concern since those agencies with a "primary role" in the effort has characterized national security as a centralized matter. However, the ratio of network responses to traditional bureaucratic responses suggests a shift in structure.

The finding on formality least resemble networked expectations. The degree of formality is subject to 3rd party rules, need to know principles, legislation and the occurrence of operational mistakes. From a practical perspective, the lack of formality can potentially result in a loss, or misuse of information. In addition, by communicating in an informal manner, the decision to share information is left entirely to the discretion of the individual. As a result the already complicated situation is exacerbated by the

introduction of personal bias and attitudes. These findings were suggested on several occasions within this study. Given the sheer size, respective mandates, cultural divide and competition for resources the issue of a transition to an informal structure would appear to be insurmountable. In addition, changing nameplates, make it difficult to establish and maintain relationships and develop trust. Therefore, individual likeability, trustworthiness, professionalism and capacity to trust all factor into the extent of the formal or informal nature and capacity of this process.

On the other hand, the fact that one respondent had identified this issue as one requiring legislative intervention, thereby forcing agencies and departments to share information is troublesome. Clearly frustration resulting from a lack of valued interpersonal communications as identified above has come to fruition. One respondent had noted an expectation that exchanges of information would be more fluid (Interview2). This has indeed transpired to some extent, but has not materialized in some areas. Legislative intervention should be considered with some caution, as resentment can result if agencies are required by law to share information (Interview 1) and legislation can be so vague that it is open to different interpretations. In such instances it might be an option to initiate a joint force operation and work together on an ad hoc issue.

While this security network more readily identifies with centralized organizations, it is somewhat more reflective of a network in its early stages with respect to its lateral relationships. Again, if one assumes the traditional bureaucratic model previously characterized this security effort, these findings would represent some shift in organizational structure. It is significant to take notice that strict adherence to a hierarchical process was most common among core agencies identified in chapter three.

The "open" manner in which this network operates provides the strongest indication that an inevitable shift is underway. At first glance it appears to be inconsistent with the findings of the previous three characteristics. Nonetheless, openness of these agencies is limited to the release of general information as it relates to operations and restricted by the necessity for security clearance, third party rules and the need to know.

Knee jerk reactions as a result of 9/11 had a short - term impact on the way local security networks function. However, as Wood (2005) suggests, this postmodern shift will occur through "waves" of change. While events such as the Maher Arar case has had significantly more influence and has functioned to temporarily suspend the transition as it is presently conceived, a shift still seems to be in motion.

Relationships: Importance and Power

Power dynamics are a defining feature in all forms of organizations. Nodal networks are no exception. With respect to the national security initiative as portrayed in this local security network, clear evidence exists suggesting the primary actors or possible "switchers" among this network are the Royal Canadian Mounted Police and the Canada Border Service Agency respectively.[18] Given that the RCMP still represents the bastion of security operations by way of its Federal Policing functions and the CBSA is the preeminent authority at border crossings these designations make sense.

Network theorists have struggled to uncover who is responsible for defining network goals. Network theory posits if a node does not perform a given task and/ or threatens the functioning or existence of the network it can be shut down and its functions taken over by another node. These network features might cause one to ponder the role of switchers

in these processes. The 2004 Auditor General Report[19] regarding the role of the IBET triggers questions concerning the role of switchers in the network. Were comments made in that report a catalyst for a retaliatory act?

According to respondents, no agency is supposed to be of any less importance and each might perform the function as lead in a given circumstance resolved this issue. Each agency contributes its own operational specialization to the overall response. Replacing these agency contributions would be a lengthy and cumbersome task. In this respect, the literature seams to be circular. Resolving problems by this means would only serve to create new problems thus culminating in an act of futility. Nonetheless, there is consistency with Castells' assertion while "some nodes are more important than others...they all need each other as long as they are within the network... [Furthermore], no nodal domination is systemic" (2000,15).

Perhaps the most credible support for the concept of switchers can be found in the time and resources dedicated to security initiatives, membership in other networks, its size and jurisdiction. Again, the preeminence of the RCMP as one of the main security agencies and the primary mandate of the CBSA to control the flow of goods and people across the border stand apart from the fold. The primary functions of these agencies, the size of the respective overall organizations and links to other regional and federal responses are indicative of features indicative of networks.

While results were mixed, based on the assumption that this network was previously marked by traditional bureaucratic characteristics, protocol is changing. The ability to influence or be influenced was largely determined by a specific operational necessity and actors were autonomous entities. But, some respondents expressed other agencies were

dependent on their agencies abilities. Other respondents noted the ability to influence other primary players in the overall response.

Governance

The primary consideration when analyzing the feature of governance in this local security network is the role and extent of senior organizational and political influence exercised over the significance of local knowledge vis-à-vis priority setting and determining network goals. This question is essential to identifying to what extent this network is decentralized.

On the issue of short-term operations senior political officials have little impact on operations. Much the same can be said with respect to senior organizational officials. However, with the exception of the Integrated Border Enforcement Team where a shift in international (U.S – Canada) efforts are underway, it is the powers that be in the political and senior organizational echelons that control policy, direction and the purse strings. In some instances it is other regions of the country that dictate direction. This development possibly suggests the existence of superior or primary networks among a group of networks or it might simply depict the reality as one of those regions occupying a more vulnerable state of threat. Regardless how one chooses to identify this position, local agencies have little control over their respective operations with respect to long-term strategizing and goal setting.

These findings highlight a pervasive problem. Senior Bureaucrats centrally located are making decisions about the importance and direction of local security networks. Senior organizational officials are charged with the task to maneuver within the politics

of national security, yet are disconnected from grass root operations and the "ground beaters" mandated to carry out local operations. There is a constant need to submit 'Score Cards" and other operational performance reports. Therefore, there is overlap in this respect as well. It would seem the process has become increasingly complicated. While there has been a shift to some integrated units, such integration has not resulted in the dismantling of reporting protocol; it has primarily created new joint authorities with which to report. Clearly, many of the disadvantages identified with previous network approaches have not been completely resolved.

Resources have been a point of contention prior to 9/11 and will continue to plague security efforts for some time to come. Concerns are raised about membership in operations, who is responsible for distributing resources and how they are distributed. Other concerns are raised with respect to mandates and the right to receive resources. Some of these issues could be addressed through increased education and open, honest dialogue.

Agencies are still feeling their way through this process, which is slowly, but steadily realizing the benefits of joint efforts. However, political leadership factors into this mix as there is no overall long – term strategy or policy in place to effectively alleviate the uncertainty with respect to direction and goals. Political efforts, though well intentioned, have been bogged down by knee jerk reactionary responses. The problem is three pronged. There is a fundamental disconnect between incorporating policy with resources. There is disconnection between mandates and resources. And there is disconnect between policy and mandates.

Advantages & Disadvantages of Networks

Prior to the events of 9/11 a sense existed whereby the status quo was good enough in the area of national security. The need to accelerate security initiatives was thrust upon officials in a very short period of time. As efforts evolve to new demands, certain advantages and disadvantages emerge.

As a collective, the current security network is believed to be more effective than previous efforts. Yet, concerns were raised as to how adaptable it is. This is a perplexing phenomenon, as presumably an effective security response in a fluid ever-evolving terrorist environment requires the ability to evolve and adapt with greater ease. This confusion can likely be attributed to the necessity to approach problems in a networked coordinated fashion accompanied by pre-existing archaic legislation, third party rules and cultural biases. The network emphasis on local knowledge is fundamental in addressing risk as security threats occur locally. However, due to the global environment with which we live, local knowledge figures into security concerns across the country and in fact the world. This feature has its advantages in that relevant information can be shared with relative ease. But, it also figures into assigning priorities and the subsequent distribution to address concerns.

Overall, patterns of disadvantages/ problems are mixed. Responses to theorized network disadvantages were slightly more conducive with networked expectations; however, on certain characteristics there was some acknowledgement that these issues were resolvable. While it might appear that the disadvantages attributed networks out number their advantages, there might exist a need to re-categorize disadvantages as problems. Disadvantages imply a constant state of being. In the present context the

characteristics identified by network theories as disadvantages do not necessarily imply a state of constancy. Thus, some characteristics might be better referred to as problems.

Overall, there appears to be some indication a transformation in this local security response is underway. But, the extent and veracity of this shift needs to be re-conceptualized and taken in conjunction with the timing and infancy of this process. The problem was and remains a lack of consultation with those mandated to carry out security operations. At present, efforts are still evolving and communication disconnects still remain a prominent feature in the current security landscape. But, by re-categorizing concepts, thereby shifting the point of reference, a different picture begins to emerge.

Future Security and Policing Trends and Implications

From the outset of this study the intention was to provide an empirical understanding of a local, functioning, post-modern security and policing apparatus. This undertaking was an attempt to define and explore the definitional characteristics of this response in an effort to validate or rebut claims present day security and policing efforts have undergone a transition from a traditionally based bureaucratic model to a networked response. To some extent, this study has supported such claims. Despite the lack of unanimous agreement or consensus on the matter of strict adherence to network qualities, an organizational shift still appears to be underway. However, our current understanding to this point of the network "framework" impedes and constrains our vision of this phenomenon..

Research on network theory is incomplete. We are conditioned to view the practical application of networks as an all-encompassing effort consisting of agencies, departments

and units as one of many nodes of a local initiative. This local initiative in turn is but one aspect of a larger group of networks. While this remains the proper starting point in defining networks, it provides little in understanding the tangible description of overall networks. Only by viewing each of these network nodes as possible members in much smaller manifestations of joint force operations, ad hoc initiatives or multilateral agreements can a better understanding of networks be accomplished. In other words, our understanding of network theory needs to start small - local and then branch out nationally. This study has illustrated that smaller integrated arrangements most readily lend themselves to the characteristics attributed networks. They are better able to circumvent the legislative and cultural impediments plaguing the realization of a true network as they provide a catalyst for integration. The integrated approach is supported by the creation of such units as the Integrated Border Enforcement Team (IBET), Maritime Security Operations Centre (MSOC), the Criminal Intelligence Service Nova Scotia (CISNS) and other integrated approaches. Thus, in order to develop a true appreciation for the face of a network, we must narrow our focus, rather than thinking in broad abstract terms.

When prompted to provide their opinions on future incarnations of security efforts, respondents tended to allude to greater emphasis on integration in the form of JFO's, which focus primarily on specific issues, rather than a general response. When queried about the evolution of security efforts, many respondents articulated that future security and policing initiatives either will or should be characterized by an integrated approach (Interview 1, 4, 7 and 9). One respondent noted;

> Everything is integrated now ... I think that is the right way to go ... We were secretive ... We thought we could do it all ourselves ... We

> thought we were the best ... That's not the way we do it anymore (Interview 7)

A second representative was of the belief that future initiatives would be characterized by "more agencies wanting to network" (Interview 1). He suggested that these efforts would be marked by concerns with respect to mixed mandates and the Privacy Act, but a common intelligence bank should be a matter of "legislation" and more joint force operations should be developed and maintained by new funding, rather than diverting resources from pre-existing units. The redirecting of funds was a concern identified by all of the respondents, appearing to be a ubiquitous problem.

If we are to accept the theory that present and future security operations are or will be characterized by those inherent in networks, we must give serious consideration to the notion of networks as being synonymous with the principles of integration. As one respondent had noted;

> I believe in integration, true integration ... when you come to the table you come as equal partners ... Integration is the way of the future ... Equal partners in all capacities (Interview 1).

The Debate on Pluralization

Shearing (2005, 57) argues, "A new paradigm of policing has emerged." Similar comments have been subject of discussion for some time now (Shearing, 1996; Murphy, 1998; Bayley and Shearing, 2001; Hermer *et al.*, 2002; Shearing and Wood, 2003b; Crawford and Lister, 2003) Functions traditionally assigned police organizations have also been incorporated into the organizational activities of other public and private agencies. This case study adds credence to this argument, not due to the pluralization of responsibilities, rather, the extent in which these organizations are incorporated into the fold. Since the events of 9/11 greater attention and a heightened awareness exists in the

national security industry to risk assessments. Emerging from this impetus is the momentum to formulate joint force operations and create an environment where there is at least the perception of a multi-lateralization of mandates. The problem with this reaction stems from the fact that mandates as defined federally have not evolved in kind to reflect this transition. Throughout this research one common impediment to effective integration has emerged in the way decision - makers at the federal level have reacted slowly to the new reality and imperatives. The inability of centralized officials to respond in a timely and appropriate decentralized manner in step with current and evolving local threats weakens the effectiveness of security networks. While respondents had indicated that the ability to adapt was lagging in this response, I would argue certain steps have been taken by these agencies to function despite the restrictive limitations encountered on an ongoing basis.

Shearing (2005, 59) has accurately pointed out the police "simply do not monopolize policing (assuming they ever did) any longer." Thus, our traditionally rooted concept of policing is in need of a broader, more inclusive conceptualization. Within this nexus of diversity the police represent but one node among an arsenal of nodes dedicated to combating internal and external threats to national security. He (Shearing) has suggested police organizations can be "beneficiaries... or casualties of the age of nodal security (2005, 60)." Shearing argues the status of this evolution depends on whether or not police policy makers opt to react in a "swift, flexible and innovative" manner, or in a manner he characterized as the "ostrich response - head firmly in the sand, bum in the air (2005, 60)."

It would be difficult to rebut this assessment forwarded by Shearing. However, in this case study the argument does not exist in isolation as one unique to traditionally characterized police organizations. Nor does it accurately depict the reality of grass-root policing in the broadest sense of the concept. Within the present context many agencies could be accused of sticking their heads in the proverbial sand. Reasons for this response are the result of outdated legislation and personal or institutional attitudes. For example, Section 107 of the Customs Act, Section 4 and 8 of the Privacy Act and the fumbling of institutional mandates all have a role in impeding efficient and seamless integration and exchange of information. Present and future initiatives must and will adhere to strict guidelines resulting from such legislation, the need to know policy and third party rules as dictated in multilateral agreements. The manner in which the Maher Arar case was managed might serve to muddy the waters even further. On the other hand, the opposite might be true as rules and regulations might resolve the extent of uncertainty as to mandates, responsibilities and the exchange of information.

Institutional barriers have not been shed in the aftermath of the events of 9/11. Each node is still attempting to justify their own unique place in the network. Each node is still struggling to acquire resources to carry out their respective tasks, mandates or individually interpreted mandates. In the meantime the powers that be within the Treasury Board and at Ministerial levels continue to indulge in the act of pontification.

Cultural and personal factors have also proven to be a difficult challenge to overcome in the pluralization debate. As noted above, the sense that knowledge is power still flourishes in the minds of many. Again, in this case study this phenomenon is not unique to policing agencies. To utilize a rhetorical technique made famous by Donald

Rumsfeld, Does this mean they are immune to such knowledge is power tactics? Of course not. But the police are not the only agency indulging in this practice. Such a technique is ubiquitous in its application as each institution is attempting to justify its place and pre-eminence in certain activities.

In the final analysis, security efforts are subject to the values and fabric of Canadian Society. While the general population grapples with privacy concerns, agencies are challenged to juggle security needs and simultaneously manage expectations.

Doing Security Research: Methodological Considerations

Attempts to investigate this supposed paradigm shift in the security and policing environment will be contingent on a number of factors - some related to those practitioners in the environment, yet others within the academic community.

Researchers need to come to terms with the sensitive nature of the community they wish to study. They need to be sensitive to the possibility of compromising the integrity of the organization and the repercussions when this integrity is compromised. Therefore, researchers must subscribe to the notion that the threat is real. The events of 9/11 seemed to project some sense of an anomaly. Critics of policing activities were skeptical that any similar event could ever occur. However, recent events in Spain and the United Kingdom should function as a reminder that real security threats still exist.

Second, researchers must come to grips with the issue of trust. Throughout this research I have referred to trust within and between agencies mandated a security role. If trust is an issue in that environment, it most certainly is an issue for introduction in academic research.

In concert with developing and maintaining trust, researchers would benefit from understanding and appreciating the culture of the various representative agencies and impediments they are required to overcome. Throughout this process I have been struck by the forthright honesty of the participants. No "punches were pulled" as I echoed the sentiments of a few respondents, the dedication and adherence to "open and honest" communication. Future endeavors should focus on maintaining a critical perspective without criticizing and embarking on an exercise of "finger pointing."

From the practitioner's behalf, departments' and/ or agencies should be more receptive to being researched from an academic perspective. Much criticism of these agencies within institutions of higher learning is derived from resistance to such efforts. If we are to trust those in the national security milieu to safeguard the Canadian public against terrorist threats, then they should possess a level of sophistication able to discern the difference between the release of information that could compromise efforts and those that are legitimate exercises in research and public knowledge.

I am not making the claim that this research represents the panacea of how to approach such studies. Nor do I claim that this current study is the final word on the issues. This study is designed to provide the first of what I hope are future research efforts to understand and assist in describing a newly developing security network phenomenon. It represents one of many stepping-stones in this academic journey.

As the first study of its kind, I did encounter some limitations and resistance. Perhaps this resistance on behalf of certain departments was the result of concern in regards to becoming the objects of a microscopic academic evaluation during the developmental stage of a hasty response. The fact that many respondents reflected on the “knee jerk”

reactions to such events supports this assessment. Security concerns might have also prompted reluctance. However, given that potential respondents were provided the same copies of the interview guide as those who agreed to participate, such concerns seem unlikely. Nonetheless, certain key departments did not wish to take part in the research. As I had identified in Chapter one, the Canadian Security Intelligence Service (CSIS) is Canada's foremost intelligence gathering organization. Having its cooperation would have been beneficial and desirable. Having said this, the absence of CSIS by no means negates the validity of this research. The inclusion of such agencies as the National Security Investigation Section (NSIS), the Integrated Border Enforcement Team (IBET), National Counter Intelligence Unit and others provide a sound basis for the arguments discussed. A similar argument applies with respect to the absence of Transport Canada. Furthermore, if time and resources permitted a more complete and comprehensive study could have been conducted that would have incorporated not only all departments involved in this local contingency, but also members of networks beyond this local contingency. This would have permitted an opportunity to examine inter-network operations.

In the final analysis, this study does provide empirically based evidence that an organizational transition is occurring, from the traditional bureaucratic approach of security and policing to a networked approach. However, this transition is only in the early stages of development. There still remains significant resistance to this movement. Regardless of expectations, the shift is a process or journey and not an end point or destination. It might be the case that a complete network transition never occurs. Expectations to this event should be tempered by the acknowledgement that theory is

based on an absolute ideal, rather than an achievable reality. In that event, theorists might have to go back to the drawing board and re-examine the true nature of a network model. It may be that the Theory of Networks will need to be redefined by the more complex realities of organizational limits in the real world of security agencies, taking into consideration the complex and changing mandates and core societal values.

Endnotes

[1] Transport Canada oversees Air transportation security matters including the Canadian Aviation Transportation Safety Authority. CSIS is Canada's principle advisor in security related matters conducting investigations, analyzing information and providing risk assessments to various government departments.

[2] The HPA is a "self sufficient, economically driven crown agency regulated by the federal government, but not funded by the government."

[3] The official Internet site notes, "this is a Provincial Bureau of the Canadian Intelligence Service...Staff work on a number of all encompassing projects, including eco-terrorism, terrorism...."

[4] The Smart Border Agreement predated the events of 9/11

[5] "Responsibilities include: any threat to the security of Canada as defined by section 2, *Canadian Security Intelligence Service Act*; any offence where the victim is an internationally protected person (IPP) as defined in section 2 CC, or a person designated as a protected person in PRPM Ch. 2; the unlawful release of sensitive or classified information dealing with national security...; related terrorist activities as defined in the anti-terrorism provisions in the CC [criminal code].

[6] The Manager of Marine Security indicated that the creation of his position was due to the ISPS and 75% of the time was dedicated to policy development and security. This figure could be a matter of splitting hairs.

[7] Since conducting the initial interview, the Bureau director from CISNS noted provincial involvement in that agencies operation has resulted in extra resources coming to fruition.

[8] PSEPC portfolio agencies include the following agencies: CBSA, Canada Firearms Centre, CSIS, Correctional Services Canada, National Parole Board and the RCMP.

[9] Section 29 investigations concern fraudulently gained citizenship.

[10] Aside from this, the Halifax Port Authority did not refer to the RCMP as one of the top three agencies with which they interact. This is surprising given the recent creation of the National Ports Enforcement Team (NPET) located in the Port of Halifax. Thus, the nature of this relationship remains unknown. It could be that policing issues are addressed through HRP. While not an agency represented in this research, as a unit, the NPET has a similar mandate to that of the IBET

[11] If a recipient of a piece of information intends to in some way act on that information they will personally have to check with the author of the same.

[12] Of these eight agencies, two reported to joint, internal and external authorities.

[13] The Threat Assessment Group is a Provincial Group consisting of the RCMP, DND and the CBSA. It is primarily called into action in acute threat to security instances.

[14] Notable exceptions to this rule are illustrated with RCMP Immigration and Passport (I & P) and the Halifax Port Authority (HPA), wherein political influence, while remaining consistent in terms of short-term and long-term influence, is still significant.

[15] One respondent noted that there is no long-term strategic focus... they are throwing in money, but what are we going to get out of this? Mis-directions are becoming more confounded... 9/11 has made this misdirection worse... The government has been reactionary to incidents or perceived incidents (Interview 1).

[16] The NCO i/c for the Nova Scotia IBET noted through the El Paso Intelligence Center all he had to do was enter a password and he had access to any and all information concerning any boats, sail boats and the people associated with these vessels. All policing agencies in the United States utilize this system.

[17] This respondent followed up by expressing concerns that he did not want to see efforts circumvent personal rights and that there should be some course of regress.

[18] CSIS and DND are also major departments/ nodes in this network.

[19] In the 2004 Report of the Auditor General, officials from CIC cited the lack of participation in IBET;s was due to (in their view), the IBET's primary focus being drugs and contraband. They dismissed any suggestion of national security.

References

Acharya, Amitav (2002). Security and Security Studies After September 11: Some Preliminary Reflections. Institute of Defence and Strategic Studies [Online]. Available: www.911investigations.net/IMG/pdf/doc.1401.pdf

Alkire, Sabina (2002). Conceptual Framework for Human Security. [Online]. Available: www.humansecurity-chs.org/doc/frame.html

Bayley, D.H. & Shearing, C (2001). The New Structure of Policing: Description, Conceptualization, and Research Agenda. National Institute of Justice, Washington, D.C.

Booth, Ken (1991). Security and Emancipation; Security in Anarchy; Utopian Realism in Theory and Practice. International Affairs, 67, 3, 527-545.

Buzan, Barry (1991). People, States and Fear: An Agenda for International Security Studiesin the Post-Cold War Era. 2(ed). Hemel Hempstead: Harvester Wheatsheaf.

Campbell, David (1992). Writing Security: United States Foreign Policy and the Politics of Identity, Manchester: Manchester University Press.

Castells, Manuel (2000a). Materials for an Exploratory Theory of the Network Society. British Journal of Sociology. 51, 1, 5-24.

Castells, Manuel (2000b) Toward a Sociology of the Network Society. Contemporary Sociology. 29, 5, 693-699.

Crawford, A & Lister, S. (2003). Integrated Local Security Quilts or Frayed, Fragmented and Fragile Tangled Webs? The Patchwork Shape of Reassurance Policing in England and Whales. Paper presented at In search of security: An international conference on policing and security, hosted by the Law Commission of Canada , Montreal, February.

Der Derian, James (2001). 911: Before, After and In Between. [Online]. Available: http://www.ssrc.org/sept11/essays/der_derian.htm

Dupont, Benoit (2004). Security in the Age of Networks. Policing and Society. 14, 1, 76- 91

Erickson, Richard and Haggarty, Kevin (1997). Policing the Risk Society. Toronto: University of Toronto

Farrell, Catherine & Morris, Jonathan (2003) The Neo-Bureaucratic State: Professionals, Managers and Professional Managers in Schools, General Practices and Social Work. Organization. 10, 1, 129-156.

Freedman, L (1992). The Concept of Security. In Hawkesworth and Kogan (eds). Encyclopedia of Government and Politics, 2. (730-741). London: Routledge

Gallie, W.B. (1956). Essentially Contested Concepts. Proceedings of the Aristotelian Society. 56, 167-198.

Garland, David (2001). The New Culture of Crime Control. In The Culture of Control: Crime and Social Order in Contemporary Society (167-192). Chicago: University of Chicago Press.

Hermer, et al. (2002). Policing in Canada in the 21st Century: Discretion for Law Reform: Report to the Law Commission of Canada, Law Commission of Canada, Ottawa

HRP (2004). Special Enforcement Section. [Online]. Available: www.police.halifax.ns.ca/Services/specialenforcement.htm

Johnston, L (1992) The Return of Private Policing. London: Routledge.

Kahn, Muqtedar (2001). Terrorism and Globalization. [Online]. Available: http://www.glocaleye.org/terglo.htm

Kempa, Michael, Carrier, Ryan, Wood, Jennifer, and Shearing, Clifford (1999) Reflections on the Evolving Concept of Private Policing. European Journal on Criminal Policy and Research. 7, 2, 197-224.

Klein, Bradly (1994). Strategic Studies and World Order: The Global Politics of Deterence. Cambridge: Cambridge University Press.

Kraus, Keith and Micheal Williams (1996). Broadening the Agenda of Security Studies, Politics and Methods. Mershon International Studies Review. 40, 229-254.

Kraus, Keith and Micheal Williams (1997). Critical Security Studies. Minneapolis: University of Minneapolis Press.

Lebkowsky, Jon (2000). Nodal Politics. In Mindjack Magazine [Online] Available: www.mindjack.com/feature/nodal.html

Maguire, Mike (2000) Policing by Risks and Targets: Some Dimensions and Implications of Intelligence-Led Crime Control. Policing and Society, , 9, 4, 315-336.

Mansfield, Roger (1973) Bureaucracy and Centralization: An Examination of Organizational Structure. Administrative Science Quarterly, 18, 4, 477-488.

Murphy, Chris (1998). Policing Postmodern Canada. Canadian Journal of Law and Society. 13, 2, 1-25.

Office of the Auditor General of Canada. (2004). Report of the Auditor General of Canada to the House of Commons: Chapter 3, National Security in Canada – The 2001 Anti-Terrorism Initiative, (Cat. No. FA1-2004/1-3E). Ottawa: Minister of Public Works and Government Services Canada

Perrow, Charles (1967) A Framework for the Comparative Analysis of Organizations. American Sociological Review. 32, 2, 194-208.

Perrucci, R and Potter, R (1989). The Collective Actor in Organizational Analysis. In Networks of Power: Actors at the National, Corporate and Community Levels. NY: Aldine de Gruyter

PSEPSE (2006) Who We Are [Online]. Available: http://www.psepc-sppcc.gc.ca/abt/wwa/index-en.asp

Privy Council Office (2004). Securing an Open Society: Canada's National Security Policy. [Online]. Available: www.pco-bcp.gc.ca

Rhodes, R.A.W and Marsh, R. (1992) Policy Networks in British Politics. In, Marsh, R. and Rhodes, R.A.W. (eds.). Policy Networks in British Government. Oxford: Clarendon Press.

Shearing, Clifford (1996). Reinventing Policing: Policing as Governance. In Otwin Marewin (ED), Policing Change, Changing Police, International Perspectives NY: Garland Publishing Inc.

Shearing, Clifford (2000). A New Beginning for Policing. Journal of Law and Society. 27, 3, 386-393.

Shearing, Clifford & Wood, Jennifer (2003a). Nodal Governance, Democracy and the New Denizens: Challenging the Westphalian Ideal. (DRAFT)

Shearing, Clifford & Wood, Jennifer (2003b). Governing Security for Common Goods. International Journal of the Sociology of Law. 31, 3, 205-225.

Shearing, Clifford (2005) Nodal Security. Police Quarterly, 8, 1, 57-63.

Smith, Steve (2002). The Contested Concept of Security. Institute of Defence and Strategic Studies [Online]. Available: www.911investigations.net/IMG/pdf/doc.1401.pdf

Urry, John (2002). The Global Complexities of September 11th. Theory, Culture and Society, 19 (4). PP.57-69

Vaughan, Diane (Aug 1999) THE DARK SIDE OF ORGANIZATIONS: Mistake, Misconduct, and Disaster. In Annual Review of Sociology, Vol. 25, pp. 271-305 http://web.mit.edu/gtmarx/www/garyhome.html#Online

Weber, Max (1946) From Max Weber, H.H. Gerth and C. Wright Mills, eds. London: Routledge and Kegan Paul.

Wood, Jennifer (2000) Reinventing Governance: A Case Study of Transformations in the Ontario Provincial Police. Centre of Criminology. Toronto: University of Toronto

Zedner, Lucia (2002). The Concept of Security: An Agenda for Comparative Analysis. In Globalization and Security Readings, C. Murphy (ed). 62-90.

Appendix A: Dissemination of Information

Agency	Direction		
	Hierarchical	Lateral	Both
CCG		X	
DFO		X	
IBET		X	
CBSA			X
CISNS			X
HPA			X
I & P			X
NSIS	X		
CIC	*	*	*
NCIU	*	*	*

Agency	Reviewed and Filtered	
	Reviewed	Filtered
NSIS	N	N
DFO	N	N
CISNS	Y	N
HPA	Y	N
CBSA	Y	Y
CCG	Y	Y
I & P	Y	Y
NCIU	Y	Y
IBET	Y	*
CIC	*	*

* Denotes missing data or no response.

** These tables provide a more detailed illustration of how information is disseminated and exceed what is required to confirm the existence or absence of a seamless flow of information Lebkowsky (2000, para. 5) associates with networks. A "purely" networked organizational model would result in the lateral dissemination of information or perhaps both. Conversely, strict adherence to a bureaucratic structure would be Hierarchical. In addition, if the flow of information is seamless, expectations would be minimal that the information would be filtered. Therefore, these results show some, though mixed consistency with network qualities.

Appendix B: Sample Relationships

	CBSA	CCG	CIC	CISNS	DFO	HPA	IBET	I&P	NCIU	NSIS
	Top 3 Relationships									
1	CSIS	RCMP	RCMP	RCMP	RCMP	HRP	DFO	CBSA	DND	CSIS
2	RCMP	DND	CSIS	HRP	DND	TC	DND	PP	CSIS	I&P
3	DND	CBSA	CBSA	CBSA	CS/CB	CBSA	Core	CIC	RCMP	IBET
	Supplementary									
4	CIC	CSIS	DFAIT	DND	CCG	RCMP	TC	CSIS	CBSA	DND
5	HPA	CIC		Police		CSIS	CCG	CISNS	TC	CBSA
6		HC		L&F		CCG	CSIS	CISNS	DFO	HRP
7		USCG		CIC		DND	NSIS	DND	CCG	
8						DFO		CCG	CIC	
9						USC		DFO	Police	

* Core – Core Agencies in IBET
* CS/CB – Canadian Security Intelligence Service/ Canada Border Service Agency
* HRP – Halifax Regional Police
* DFAIT – Department of Foreign Affairs and International Trade
* HC – Health Canada
* L & F – Lands & Forrest
* PP – Passport
* TC – Transport Canada
* USCG – United States Coast Guard
* USC – United States Customs

Appendix C: Interview Guide

MAPPING SECURITY: A NETWORK ANALYSIS

INTRODUCTION

I invite you to take part in a research study being conducted by myself (Darryl MacPherson), a graduate student at Dalhousie University. This study is being conducted as partial fulfillment for a Masters in Sociology. Your participation in this study is voluntary and you may choose to withdraw from the study at any time. The study is described below. This description will provide you with an understanding of the risks or inconvenience that you might experience as a result of your participation. It is unlikely that you will benefit from taking part in this study, however, the information you provide will assist others in understanding the environment with which you work.

PURPOSE

The new security environment has created new forms of organizations, communities and collaborations. The primary objective of this study is to develop a better understanding of the national security networks in the Province of Nova Scotia. Through the documentation, description and analysis of security networks, I hope to develop a greater understanding of the roles, functions, activities and governance of departments and agencies in this environment. Your participation in this study is important as you represent an agency in this security network.

YOUR PARTICIPATION

As a participant in this study you will be asked to take part in a semi-structured interview lasting approximately one - two hours in length. You will be asked a number of prepared questions. Interviews will be conducted at a place of your choosing. If you are agreeable, your words might be quoted in the final copy of this research project. You are under no obligation to answer all of the questions posed and are free to withdraw from the interview at any time. Dependent upon your approval, the interview might be audio - taped, however, if at any time during the interview you wish to have the tape recorder turned off I will comply with those wishes.

As the principle investigator, I alone (Darryl MacPherson) will be conducting the interviews. Access to this raw information will be limited to myself, and my supervisor, Dr. Chris Murphy (Chair, Department of Sociology and Social Anthropology).

ANONYMITY/ CONFIDENTIALITY/ STORAGE

As a participant in this research you will not be identified by your name, but rather by your position. Therefore, there is no need to provide you with a false name (pseudonym). Only possibly my thesis supervisor and myself will know your name. The only place that your true identity will appear will be on the consent forms presented to you at the beginning of the interview. Any direct quotes will be attributed to your position. Nonetheless, others in this security network might be able to identify you through affiliations.

The storage of all raw materials will remain in a filing cabinet at my place of residence in a locked office. Outside of myself, the only other person that might be provided access to this material will be my supervisor. This material will remain in this location for the duration of my study. Following the completion of my thesis Dalhousie University policy on Research Integrity requires that this information remain with the institution for five (5) years. Tape recordings will be destroyed after they are transcribed.

POSSIBLE RISKS & BENEFITS

Every effort will be made to protect your personal identity. However, the potential still exists that you might be identifiable by others close to you in the policing and security network. While the subject matter of this research is benign, there exists the possibility that you might divulge sensitive information. Such information would be of a nature that would compromise ongoing security operations. I will contact you to discuss the transcriptions to ensure there is no ambiguities, misinterpretations or misrepresentations. In the unlikely event of this occurring I will exclude this material from my study and submit to an agreement so designated by your agency. Such an agreement would require me to sign an oath of confidentiality not to repeat or discuss the aforementioned sensitive material.

You will not be compensated for your involvement in this study. I do hope you will take satisfaction in knowing that your participation will enlighten others that traditionally theorize about this topic. This research will not only contribute to a better academic understanding of networked organizations, but will also assist networked organizations like yours by identifying concepts or characteristics that might positively or negatively impact your agencies operations.

QUESTIONS

If at any time you have questions about this study you can contact either myself (Darryl MacPherson) at (902) 435-9074, dsmacphe@dal.ca ; or Dr. Chris Murphy at (902) 494-2069, cmurphy4@dal.ca . Should there be any changes in this study that might impact your decision to participate you will be informed.

PROBLEMS or CONCERNS

In the event that you have any difficulties with, or wish to voice concern about, any aspect of your participation in this study, you may contact Patricia Lindley, Director of Dalhousie University's Office of Human Research Ethics Administration for assistance: (902) 494-1462, patricia.lindley@dal.ca

FOLLOW-UP

Following the completion of this research I would be pleased to provide you with a summary or complete copy of my thesis.

- ❑ I would like a complete copy of your thesis

- ❑ I would like a summary of your thesis
- ❑ I do not require a copy
- ❑ I would like an oral presentation

Consent

I have read the explanation about this study. I have been given the opportunity to discuss it and any questions I had have been answered to my satisfaction. I hereby consent to take part in this study. However, I realize that my participation is voluntary and that I may choose to withdraw from the study at any time. .

_____

Participants Name (printed)

_____ _____

Participants Signature **Date**

Yes, I would like a pseudonym _____ (Initial)
No, I do not require a pseudonym _____ (Initial)

Yes, I agree to be audio – taped _____ (Initial)
No, I do not agree to be audio – taped _____ (Initial)

Yes, I will permit direct quotes _____ (Initial)
No, I will not permit direct quotes_____ (Initial)

_____ _____

Researchers Signature **Date**

Interview Guide

Institutional History

Mandate:

(a) What is your agencies security mandate today?

(b) How has it changed since the events of 9/11?

(c) What percentage of your agencies time is dedicated to security initiatives?

(d) Where do security issues rank on your organizations list of priorities?

(e) What percentage of your agencies efforts and resources would you estimate are dedicated to security?

(0-25) (26-50) (51-75) (76-100)

(f) Has your budget increased in the last 3 years to accomplish this task? In what ways was it spent? List;

*Technology*_____

Manpower _____

*Other*_____

(g) Are new programs being developed to accomplish this task? List:

_____

_____

_____

_____

_____

Operational Activities:

(a) How would you categorize your agencies security activities in terms of priorities? "1" being primary, "5" being marginal

Intelligence	*1*	*2*	*3*	*4*	*5*
Enforcement	*1*	*2*	*3*	*4*	*5*
Policy	*1*	*2*	*3*	*4*	*5*
Strategic	*1*	*2*	*3*	*4*	*5*
Tactical	*1*	*2*	*3*	*4*	*5*
Other	*1*	*2*	*3*	*4*	*5*

(b) Has this mix changed since 9/11?

(c) How has it changed?

Organizational Structure:

(a) How would you describe your agency's organizational structure?

Formal	*1*	*2*	*3*	*4*	*5*	*Informal*
Centralized	*1*	*2*	*3*	*4*	*5*	*Decentralized*
Hierarchical	*1*	*2*	*3*	*4*	*5*	*Lateral*
Insular	*1*	*2*	*3*	*4*	*5*	*Open*

(b) What are the old and new sections within your agency that have a security function?

(c) What are their functions?

(d) Can you briefly walk me through the steps your agency takes in performing its security task

(e) How is information disseminated, hierarchically or directly to other low level tactical agencies?

(f) Is this information reviewed first and filtered?

(g) How does this unit, in your opinion, create support for the rest of your "host" organization?

Relationships With Other Security Agencies

Scope:

(a) Can you list other agencies or departments that you have a formal security relationship with?

*1*_____	*4*_____	*7*_____
*2*_____	*5*_____	*8*_____
*3*_____	*6*_____	*9*_____

(b) Can we briefly go through this list (top 3) so that you can tell me about the nature of your agencies relationship with these other agencies and organizations.

1 ***Nature***

Activity

Co-ordination

Autonomy

Power

Frequency Ann. Mon. Week Day Needed

Importance VI Imp NVI

2 ***Nature***
Activity

Co-ordination

Autonomy

Power

Frequency Ann. Mon. Week Day Needed

Importance VI Imp NVI

3 ***Nature***
Activity

Co-ordination

Autonomy

Power

Frequency Ann. Mon. Week Day Needed

Importance VI Imp NVI

(c) In general (Non-specific) terms, how would you assess the above criteria to agencies of less importance?
(d) When your agency encounters differences in priorities or assessments, with other agencies, how does your agency proceed with its task?
(e) How do these agencies influence your priorities?
(f) Which agencies influence your priorities the most?
(g) Do you have more freedom? Y N
(h) Do you have more autonomy? Y N
(i) Which relationships would you categorize as primarily informal? Which primarily formal?
(j) Which agencies does your agency influence the most?
(k) How would you have addressed these concerns before 9/11?

Advantages and Disadvantages of Networking
Advantages:
(a) What are some of the advantages of working with other agencies on a common task?

(b) *How does being a part of an integrated team assist you in the facilitation of your agencies work?*
(c) *Comparatively speaking, how does local knowledge and intelligence factor in to your operations as opposed to federal or international contributions?*
(d) *Do you believe the present security organization is more adaptable than previous initiatives? Better able to evolve and respond to the environment?*
(e) *Do you believe this collaboration is more effective?*

Disadvantages:

(a) *From your perspective, what are the problems (if any) with the present relationships?*
(b) *Did you have similar problems prior to the events of 9/11?*
(c) *Can you tell me about any concerns you might have concerning the following?*
    i. *Autonomy*
    ii. *Trust*
    iii. *Regional thinking*
    iv. *Resource allocation*
    v. *Political*
    vi. *Other factors that might have an impact on your agencies ability to maximize its effectiveness and efficiency?*

(d) *Do you find that this arrangement is complicated and could benefit from having a more clear direction?*
(e) *Do you believe effective leadership in the overall security response is possible with such a decentralized arrangement?*
(f) *Is it difficult and cumbersome to coordinate various agencies and their functions?*
(g) *Is it difficult to focus resources on specific goals?*
(h) *What are the problems associated with communications with other security agencies?*
(i) *Is it difficult to manage complex tasks beyond a certain size? How do you resolve these? How did you resolve them before?*
(j) *Do you encounter problems with respect to differing priorities with different agencies? How do you resolve these problems?*
(k) *How do you feel other agencies could function more effectively or contribute more to security concerns?*

(l) Has this sharing of security responsibilities negatively affected your agencies role? Power? Prestige?

Governance

(a) How are your department operations and activities managed and governed?
(b) Are there any joint authorities to whom your agency reports?
(c) Are there any internal departments with which you are required to report? How often is this required? Why?
(d) Are there any external departments with which your agency is required to report? How often does this occur? Why?
(e) On a scale of 1 (significant) to 5 (none at all), how much does senior organizational officials assist in determining your long-term priorities? Short-term priorities?

	Significant				*Not at all*
Long term	*1*	*2*	*3*	*4*	*5*
Short term	*1*	*2*	*3*	*4*	*5*

(f) On a scale of 1 (significant) to 5 (none at all), how much does senior political officials assist in determining your long-term priorities? Short-term priorities?

	Significant				*Not at all*
Long term	*1*	*2*	*3*	*4*	*5*
Short term	*1*	*2*	*3*	*4*	*5*

(g) How much influence does your agency have in determining resource requirements and priorities to accomplish your task?
(h) Who is ultimately responsible for the policies, decisions, actions, errors and successes of your agency?
(i) Who is ultimately responsible for the policies, decisions, actions, errors and successes of joint security operations in general?
(j) How would you characterize the distribution of resources, responsibilities and uncertainty in this security response?

	Minimal	*Moderate*	*Extensive*
Resources	*1*	*2*	*3*
Responsibility	*1*	*2*	*3*
Uncertainty	*1*	*2*	*3*

(k) How do you think the security apparatus will change in the future?
(l) How do you think the security apparatus should change?
(m) Do you have any concerns about the expansion of security agencies and networks in the future?