NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

CAPSTONE PROJECT

THE GLOBAL SPECIAL OPERATIONS FORCES NETWORK FROM A PARTNER-NATION PERSPECTIVE

by

Tom-Erik Kihl
Jonas Carling

December 2014

Thesis Advisor: Nancy Roberts
Second Reader: Kalev I. Sepp

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2014	Master's Capstone Project

4. TITLE AND SUBTITLE
THE GLOBAL SPECIAL OPERATIONS FORCES NETWORK FROM A PARTNER-NATION PERSPECTIVE

5. FUNDING NUMBERS

6. AUTHOR(S) Tom-Erik Kihl and Jonas Carling

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The purpose of this capstone project is to provide recommendations to Norwegian Special Operations Command (NORSOCOM) and Swedish Special Operations Command (SWESOCOM) on how to utilize and contribute to the U.S. Special Operations Command´s "Global Special Operations Forces Network" initiative. The project explains social network theory, analyzes the GSN, and suggests how NORSOCOM and SWESOCOM can manage their GSN membership. The research extends to include potential aspirations of a national network.

The GSN effort is a thoroughly well-thought-out concept nested in U.S. strategy. USSOCOM's leadership in the GSN can be described as informal, cooperative, and communicative with partner nations and agencies. The network has no alliance-like requirements, which makes membership for partner nations "low cost."

NORSOCOM and SWESOCOM have been forward-thinking, and are well positioned for an evolving GSN. However, from a network perspective, further actions are required to counter expected challenges and to utilize the membership more effectively. The national commands should inform national stakeholders to build support, establish national network managers, and participate in burden sharing. The GSN membership can provide the policy level with an alternative security cooperation forum that has access to information and resources. The GSN membership should be leveraged to enhance national networks.

14. SUBJECT TERMS	15. NUMBER OF PAGES
global SOF Network, GSN, USSOCOM, partner nations, network managers, networks, social networks, network performance, Special operations forces, national SOF networks, 21st threats, TSOC	155
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE GLOBAL SPECIAL OPERATIONS FORCES NETWORK FROM A PARTNER-NATION PERSPECTIVE

Tom-Erik Kihl
Captain, Norwegian Army
B.S., University of Hedmark, 2012

Jonas Carling
Major, Swedish Navy
B.S., Swedish National Defense College, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2014

Author: Tom-Erik Kihl
Jonas Carling

Approved by: Nancy Roberts
Thesis Advisor

Kalev I. Sepp
Second Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this capstone project is to provide recommendations to Norwegian Special Operations Command (NORSOCOM) and Swedish Special Operations Command (SWESOCOM) on how to utilize and contribute to the U.S. Special Operations Command´s "Global Special Operations Forces Network" initiative. The project explains social network theory, analyzes the GSN, and suggests how NORSOCOM and SWESOCOM can manage their GSN membership. The research extends to include potential aspirations of a national network.

The GSN effort is a thoroughly well-thought-out concept nested in U.S. strategy. USSOCOM's leadership in the GSN can be described as informal, cooperative, and communicative with partner nations and agencies. The network has no alliance-like requirements, which makes membership for partner nations "low cost."

NORSOCOM and SWESOCOM have been forward-thinking, and are well positioned for an evolving GSN. However, from a network perspective, further actions are required to counter expected challenges and to utilize the membership more effectively. The national commands should inform national stakeholders to build support, establish national network managers, and participate in burden sharing. The GSN membership can provide the policy level with an alternative security cooperation forum that has access to information and resources. The GSN membership should be leveraged to enhance national networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APAN	All Partners Access Network
AU	African Union
AOR	Area of Responsibility
BICES	Battlefield Information Collection and Exploitation Systems
C4I	Command, Control, Communication, Computers and Information
CANSOFCOM	Canadian Special Operations Forces Command
CENTCOM	Central Command
COA	Courses of Acton
COCOM	Combatant Command
COM	Chief of Mission
CONOP	Concept of Operations
COS	Chief of Staff
DOD	Department of Defense
EU	European Union
FCC	Functional Combatant Command
GCC	Geographical Combatant Command
GMSC	Global Mission Support Center
GSN	Global SOF Network
HQ	Headquarter
IA	Inter-Agency
ICT	Information and Communication Technology
ISCC	International Special Operations Coordination Center
ISOF Conference	International Special Operations Forces Conference
ISR	Intelligence Surveillance and Reconnaissance
JCS	Joint Chief of Staff
J3-I	J3 International
JSOC	Joint Special Operations Command
JSOU	Joint Special Operations University
LO	Liaison Officer
MA	Military Assistance

NAO	Network Administrative Organization
NATO	North Atlantic Treaty Organization
NORSOCOM	Norwegian Special Operations Command
NORSOF	Norwegian Special Operations Forces
NSCC	NATO SOF Coordination Center
NSHQ	NATO SOF Headquarters
OSCE	Organization for Security and Cooperation in Europe
PDC	Professional Development Center
PN	Partner Nation
POC	Point of Contact
QDR	Quadrennial Defense Review
R&D	Research and Development
RFS	Request for Support
RSCC	Regional SOF Coordination Center
SF	Special Forces
SIE	SOF Information Environment
SOCEUR	Special Operations Command Europe
SOCFWD	Special Operations Command Forward
SOCOM	Special Operations Command
SOF	Special Operations Forces
SOLO	Special Operations Liaison Officer
SWESOCOM	Swedish Special Operations Command
SWESOF	Swedish Special Operations Forces
TSOC	Theater Special Operations Command
TTP´s	Tactics, Technics, and Procedures
UN	United Nations
USG	United States Government
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USN	United States Navy
VTC	Video teleconference

ACKNOWLEDGMENTS

We would like to thank the Naval Postgraduate School Defense Analysis Department faculty who have created the well-thought-through curriculum harnessing the students' combat experience to enhance the discussions and broaden the analysis of emerging security threats on a strategic level.

Specific gratitude goes to our advisers, Dr. Nancy Roberts and Dr. Kalev I. Sepp, for their mentorship. Additional recognition goes to Dr. Keenan Yoho for assisting us by sharing his extensive knowledge of GSN history and possible future employment. Dr. Nancy Roberts inspired key elements of this work through discussions and lectures and shaped our thoughts about the power of networks in confronting future complex problems. Additionally, this work would not have been possible without the assistance provided by USSOCOM in general and the men and women in the J3-I in particular. Both the Norwegian and Swedish LO at USSOCOM have added valuable support during our research. We greatly appreciate the support and assistance provided by Admiral William H. McRaven with access to the quiet professionals within his command, so that they could participate in our discussions with open and candid arguments.

We would also want to thank both NORSOCOM and SWESOCOM for their support and dedication to this project. If it had not been for them, we would not have been able to participate in the discussions during the International SOF Conference 2014 in Tampa, Florida, which contributed greatly to our research.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> In the 21st century, we must build partnerships that enable us to better meet a wider range of challenges. To that end, I see us building networks that leverage our unique capabilities—and the unique strength of our allies and partners that share common interest—to confront the critical challenges of the future.
>
> —U.S. Secretary of Defense Panetta
> June 28, 2012
> U.S. Institute of Peace

A. THE NEW THREAT ENVIRONMENT

From the 20th to the 21st century, the world has moved from the Cold War paradigm toward an asymmetric threat environment. In the current global context, there is no such thing as a local problem. Local threats have become globally networked.[1] During a speech to the Special Operations Forces (SOF) community, then–U.S. Secretary of State Hillary Clinton made the following statement:

> Extremist networks squeezed in one country migrate to others. Terrorist propaganda from a cell in Yemen can incite attacks as far away as Detroit or Delhi. A flu in Macao can become an epidemic in Miami. Technology and globalization have made our countries and our communities interdependent and interconnected. And today's threats have become so complex, fast-moving, and cross-cutting that no one nation could ever hope to solve them alone.[2]

Another development with these new threats is that networks are diversifying their activity, which results in the convergence of threats that were once distinct,[3] as shown in Figure 1.

[1] USSOCOM, *SOF 2020, Global SOF Network*, Tampa, Florida, 2013. Information folder.

[2] U.S. Secretary of State Hillary Clinton (speech, ISOF Week, Tampa, Florida, May 2012); USSOCOM, *SOF 2020, Global SOF Network*.

[3] Ibid.

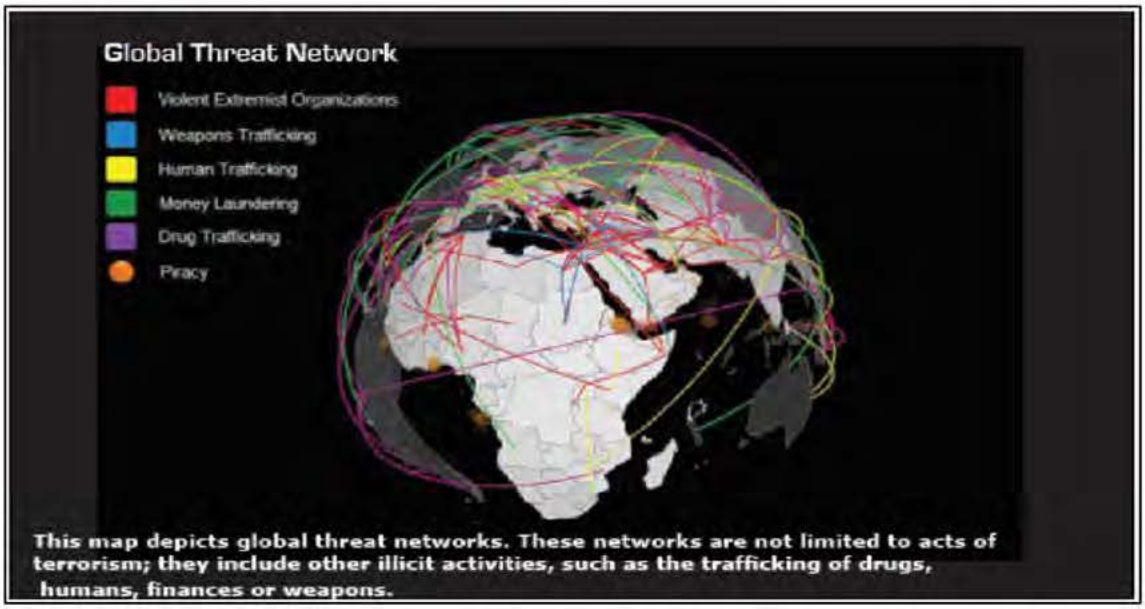

Figure 1. Global threat network.[4]

Admiral William McRaven articulated USSOCOM's awareness of the complex interdependence of today's national security issues:

> We live in a world in which the threats have become increasingly networked and pose complex and dynamic risks to U.S. interests around the world. These networks are diversifying their activities, resulting in the convergence of threats that were once linear. In today's environment, this convergence can have explosive and destabilizing effects—there is no such thing as a local problem.[5]

Based on these complex national security issues, the United States Special Operations Command (USSOCOM) has identified five key trends that are shaping the strategic security environment and present unique challenges for the global force:[6]

- The redistribution and diffusion of global power,
- The rising role of non-state actors,
- The easy access to advanced technology, to include information technology,

[4] USSOCOM, *SOF 2020, Global SOF Network*, 6.

[5] Admiral William McRaven, Posture Statement before 113th Congress, House Armed Services Committee, U.S. House of Representatives, March 6, 2013, 2.

[6] USSOCOM, "Senior Leader Guide" (ISOF Conference 2014, Tampa, Florida. 19–21 May 2014), 10.

- Shifting demographics, specifically the rapid, turbulent expansion of the urban environment, and
- The evolving, yet frail, economic health of the United States and its critical partners.

The national strategies of Norway, Sweden, and the United States describe corresponding security threats for the 21st century. All three nations focus on asymmetrical and cross-border threats:[7]

- Global terrorism,
- Proliferation of weapons of mass destruction,
- Trans-national illegal activities,
- Cyber attacks, and
- Regional armed conflicts.

Strategists agree that the 21st century promises to be a very complex environment requiring flexible and proactive crisis management. It is especially the case for European countries whose common borders and relatively easy access provide opportunities for globalized threats to spread throughout the region.[8] To counter these threats, the different security coalitions pursue similar strategies. The North Atlantic Treaty Organization (NATO), for example, focuses on: proliferation of nuclear weapons and other weapons of mass destruction; terrorism from extremist groups originating within the Alliance territory or from out-of-area regions; trans-national illegal activities such as trafficking in arms, narcotics, and people; and cyber attacks towards government administrations, businesses, economies, and critical infrastructures.[9] Similar threats are identified in the strategies of Norway, Sweden, the United States, the United Nations (UN), and the

[7] Forsvarsdepartementet [Ministry of Defense]. *Et forsvar til vern om Norges sikkerhet, interesser og verdier* [*A Defense for Protection of Norway's Security, Interests, and Resources*], Parliamentary Bill no. 48 (2007–2008) 2008; Forsvarsdepartementet [Ministry of Defense]. *Et forsvar for vår tid* [A Defense for Our Time]. Parliamentary Bill no. 73S (2011–2012). 2012; Forsvarsdepartementet [Ministry of Defense]. *Evne til Innsats: Strategisk konsept for Forsvaret* [Capability for Effort: Strategic Concept for the Norwegian Defense].

[8] Regjeringskansliet, Forsvarsdepartementet [Ministry of Defense] "Veivalg i en Globalisert Verden." [Choices in a Globalized World] (Stockholm, Sweden: Elander Sverige AB), 2013.

[9] North Atlantic Treaty Organization, *Strategic Concept: for the Defense and Security of the Members of the North Atlantic Treaty Organization* (Lisbon, Portugal: NATO, 2012), 11; President of the United States, "2010 National Security Strategy," U.S. Government Executive Branch (Washington, DC, May 2010); *President of the United States. 2011 National Strategy for Counterterrorism*, U.S. Government Executive Branch (Washington, DC, June 2011).

European Union (EU).[10] As author Anne Holohan summarizes "the UN, NATO, OSCE [Organization for Security and Cooperation in Europe], and other political and military bodies and alliances all have to adapt to a truly interdependent world where borders are no longer sacrosanct and the tasks are not rigidly divided into military, civil, and political."[11]

USSOCOM is supporting a whole of government approach to address the current threats. The Command is developing a global network of Special Operations Forces working together with government agencies, allies, non-state actors, alliances, and partner nations. USSOCOM describes the international environment as having a character of "persistent instability"—something that requires SOF "persistent presence" in the future.[12] In other words, USSOCOM's response to a whole of government approach is called the Global SOF Network (GSN).

1. USSOCOM's Call for a Global SOF Network

USSOCOM is developing the GSN concept to enhance its already global force by networking with its U.S. interagency counterparts, its foreign allies, and partners around the globe.[13] The GSN's primary goal is:

> A globally networked force of SOF, Interagency, Allies, and Partners able to rapidly and persistently address regional contingencies and threats to stability.[14]

---

[10] See the different security strategies: NATO, *Strategic Concept: for the Defense and Security of the Members of the North Atlantic Treaty Organization* (November 19–20, 2010), 10–13; Regeringskansliet [Ministry of Defense] *En strategi för Sveriges säkerhet* [A Strategy for Swedish Security] Ds 2006: 1, 16–17; European Union, *Internal Security Strategy for the European Union: Towards a European Security Model* (Brussels, Belgium: EU, February 23, 2010), 2–6; Justis og Beredskapsdepartementet [Ministry of Justice], *Terrorberedskap* [Terrorism preparedness], white paper no. 21 (2012–2013), 2013.

[11] Anne Holohan, *Networks of Democracy: Lessons from Kosovo for Afghanistan, Iraq, and Beyond* (Stanford, California: Stanford University Press, 2005), 175.

[12] USSOCOM, *Concept of Operations for the Global Special Operations Forces Network 2020 (GSN 2020)*, July 29, 2013, 2, 15.

[13] Admiral McRaven, Posture statement before 113th Congress.

[14] *The Role of the Global SOF Network in a Resource Constrained Environment* (Joint Special Operations University (JSOU) Report), ed. by Chuck Ricks (MacDill AFB, Florida: The JSOU Press, 2013), 2.

The GSN consists of interagency partners and international partners, and is intended to better support the Geographical Combatant Command (GCC) and Theater Special Operations Command (TSOC). The idea is that the network gains expanded situational awareness of emerging threats and opportunities by enabling small, persistent presence in critical locations and facilitating engagement where necessary or appropriate. The networked approach is very successful in NATO, with the establishment of the NATO SOF Headquarters (NSHQ). It allows the United States and partner nations to share information, improve interoperability, and, when necessary, work together abroad.[15] As Major General Michal Repass of Special Operations Command Europe (SOCEUR) noted, "No one nation can do it all, but every nation can do something."[16]

In his article "Global SOF and Interagency Collaboration," defense analyst Christopher Lamb highlights the imperative of multilateral and interagency collaboration to navigate the current threat environment effectively with not only a direct, but also a very robust indirect approach. Successful indirect operations require a high degree of interagency collaboration to create a holistic approach.[17]

Admiral McRaven, in his testimony to the U.S. Congress, stated that the SOF network represents a way to improve support for the GCCs and chiefs of mission (COM) and empower a global effort with capable allies and partners. Recognizing that actors need to learn from each other, SOF partners are expected to build mutual trust, foster enduring relationships, and provide new opportunities to effect shared challenges.[18]

Admiral McRaven´s successor as Commander of USSOCOM, General Joseph L. Votel confirmed the way ahead for the GSN effort in his congressional testimony.

> In order to thwart expanding trans-regional threat networks and violent extremist organizations, USSOCOM must outpace the growth of threat

---

[15] Admiral McRaven, Posture statement before 113th Congress.

[16] MG Michael Repass, "Panel Presentation: SOF and the Indirect Approach to Conflict Prevention" (speech, National Defense Industrial Association (NDIA) Special Operations/Low Intensity Conflict (SO/LIC) Symposium in Washington, DC, January 28–30, 2013).

[17] Christopher Lamb, "Global SOF and Interagency Collaboration," *Journal of Strategic Security 7*, no. 2 (2013).

[18] Admiral McRaven, Posture statement before 113th Congress.

> networks with *friendly networks across cultures … [to] continue to develop our global SOF network.* Investing in our network allows us to *share the burden* more appropriately. … Success in meeting these challenges demands unprecedented *levels of trust, confidence, and understanding built through persistent engagement.*[19]

2. Building the Network

The network's evolution started with General Stanley McChrystal and Admiral McRaven's experiences in Iraq and Afghanistan, where both commanders had seen the utility of networking within the Joint Special Operations Command (JSOC) organization. The idea of a globally networked SOF started to come to life on or about 2009. First the U.S. SOF community began connecting internally and with its interagency community to build a holistic approach to the new threats.[20] Once the internal U.S. community had started connecting, its next step was to start connecting with international allies and partners to make this a global network.

The theme for the 3rd International Special Operations Forces (ISOF) Conference in 2012 was "Building the Global SOF Network." In 2013, Joint Special Operations University (JSOU) together with Canadian Special Operations Forces Command (CANSOFCOM) Professional Development Center (PDC) hosted a symposium in Tampa, Florida, with the theme "The Role of the Global SOF Network in a Resource Constrained Environment."[21] The symposium included SOF personnel from Canada, the United States, and eight other countries. One theme that emerged early in the symposium and persisted throughout the sessions was the need to sustain and adapt existing mission-essential networks, while continuing to develop new ones during times of austerity.[22] The participants acknowledged that the realities of new and changing mission sets and declining resources called for critical thinking and innovation in order to deliver operational success and sustain the advances achieved over the past decade-plus of war.

---

[19] General Joseph L. Votel, Congressional testimony, July 2014; cited in USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief, September 15, 2014). Italics in original.

[20] Stanley A. McChrystal, *My Share of the Task: A Memoir* (New York: Portfolio/Penguin, 2013).

[21] Ricks, *Role of the Global SOF Network in a Resource Constrained Environment*, ix.

[22] Ricks, *Role of the Global SOF Network in a Resource Constrained Environment*, 2.

In May 2014, USSOCOM hosted the fourth ISOF Conference with participating SOF leaders from more than 80 countries. The conference theme, "Strengthening the Global SOF Network," surfaced a new issue not explored in any depth in any previous conferences. USSOCOM's network strategy, which emphasizes a comprehensive whole-of-government approach to coordinate agencies, departments, and partner SOF, did not fully explain how small nations like Sweden and Norway, as Global SOF Network members, were expected to contribute to and benefit from the Network.[23] The NATO SOF structure and communication network has enhanced the SOF capacity and interoperability amongst its members in the last decade, of which Norwegian Special Operations Forces (NORSOF) and Sweden's Special Operations Forces (SWESOF) are contributing members.[24] How does USSOCOM's global network initiative impact these relatively small SOF communities and their relationships in other security alliances?[25]

B. PROBLEM STATEMENT

USSOCOM's response to the new threat environment suggests networked forces conducting global long-term preventive actions within a whole-of-government approach. The austere situation requires the United States to focus on low footprint solutions. USSOCOM has touched upon the need for burden sharing among the expeditionary-capable SOF nations to be able to face the global threat networks.

Sweden and Norway are already active members of the NATO SOF network, and fill staff positions in the NATO SOF Headquarters. Further, these nations have liaison officers at USSOCOM in Tampa, which makes them also part of the newly established Global SOF Network.[26] But, beyond the charm of novelty, Sweden and Norway have to ascertain how they can utilize, benefit from, and contribute to the GSN.

---

[23] USSOCOM, *Global SOF Network*, White Paper, Tampa, Florida. April 22, 2013, 5.

[24] Jim Thomas and Chris Dougherty, *Beyond the Ramparts: The Future of U.S. Special Operations Forces* (Washington, DC: Center for Strategic and Budgetary Assessment (CSBA), 2013), 86.

[25] A symposium touching on these questions has been conducted. See the JSOU report edited by Chuck Ricks, *The Role of the Global SOF Network in a Resource Constrained Environment*, 6–9.

[26] Ewa Stenberg. "Sveriges hemliga krig" [Swedish Secret War], *Dagens Nyheter* [*Today´s News*], published January 25, 2014. http://www.dn.se/nyheter/sverige/sveriges-hemliga-krig/.

Creating partnerships and building trust enhances the potential to gain support when needed. However, being a contributing and active partner in the network may require expanding roles and missions for the national SOF, reallocating resources, generating political will, and strengthening interagency and inter-department cooperation within Norway and Sweden.

This leads to a key question: *How can NORSOCOM and SWESOCOM contribute to and utilize the Global SOF Network to enhance SOF collaboration as a way to respond to the 21st century threats?*

C. PURPOSE AND SCOPE

The overall purpose of this project is to introduce Swedish and Norwegian decision-makers (political and military) to the GSN concept as a potential new framework for SOF cooperation. The scope is limited to the respective SOF Commands of Norway and Sweden. The range of the research includes a network analysis of the GSN, followed by a descriptive analysis of NORSOCOM and SWESOCOM's management of their GSN membership. Also included is an analysis of NORSOCOM and SWESOCOM's leadership role in a potential national SOF network.

A motivating factor for the project was that the GSN concept potentially could provide Norway and Sweden new avenues to contribute to international collaboration in countering the 21st century threats.[27]

D. METHODOLOGY

The following methods are used in the project: Archival Research; Discussions; and Relational Analysis.

[27] For SOF as an integrator of interagency efforts, see Michael E. Gates, "Creating SOF Networks: The Role of NATO Special Operations as a Testing Ground for SOF Integration" (master's thesis, Naval Postgraduate School, June 2011), abstract, 16, 20–24. For SOF as optimal for long-term preventive indirect actions and "Phase Zero" operations, see Ricks, "General Themes and Thoughts," in *The Role of the Global SOF Network in a Resource Constrained Environment,* 74–75.

1. Archival Research

USSOCOM's official documents and other relevant literature (news articles and periodicals) are the sources from which we have gathered the data on the GSN. Most of the official USSOCOM documents have come from USSOCOM. Various articles have been identified through Internet searches, suggestions from colleagues and advisors, and through the different courses at NPS.

2. Discussions

Discussions with key USSOCOM personnel complement the archival data.[28] The purpose of the discussions has been to confirm and clarify the archival data, and to retrieve additional data on the GSN. Discussions with Norwegian and Swedish SOF personnel have been conducted to confirm the authors' understanding of the national context in relation to the GSN. The information gathering has employed an unstructured and informal approach during the discussions.[29]

The second purpose of the discussions with USSOCOM personnel has been to probe the Command's expectations for countries like Norway and Sweden. What is expected, or at least desired, from USSOCOM's perspective, from these nations concerning information sharing, burden sharing, and interagency effort?

3. Relational Analysis of the Overall GSN

Relational analysis is the third method utilized in this study. We first developed a sociogram, based on the archival research and the discussions with key stakeholders, to present a visual overview of the network, its participants, types of connections, and the network´s structure. We then described the network´s topography, coordination infrastructure, governance and leadership, roles, tasks, processes, and style. The

[28] The authors participated during the International SOF Conference in Tampa, May 19–22, 2014. Several discussions were conducted with USSOCOM leaders, staffers, and NORSOCOM and SWESOCOM commanders. On July 8, 2014, the authors conducted a VTC discussion with then Commander USSOCOM, Admiral McRaven.

[29] Louis Cohen, Lawrence Manion, and Keith Morrison, *Research Methods in Education*, 7th ed. (New York: Routledge, 2011), 412–413. Unstructured and informal conversation approach: Questions emerge from the immediate context and are asked in the natural course of things; there is no predetermination of question topics or wording.

descriptive section is the foundation for a following segment where the GSN is placed on Roberts' Design Continuum in order to develop an understanding of the network as a whole.

E. RESEARCH LIMITATIONS

The project has not covered all aspects of the GSN effort. Even if the authors have analyzed available documents and writings about the GSN, and discussed with GSN architects, USSOCOM leadership, as well as the commanders of NORSOCOM and SWESOCOM and their Liaison officers (LOs) at USSOCOM, there are probably challenges, benefits and potential recommendations that are not covered in this project. This is not because they are less important or relevant. Time for data collection including time available to conduct discussions with involved personnel was limited. Further, social networks are complicated and there are unique details in each case that the research has not been able to identify completely, either due to lack of time, limited access to information, or lack of knowledge and understanding of the situation at hand.

F. THE CAPSTONE PROJECT STRUCTURE

Chapter I describes the future threat environment and USSOCOM's strategic response as exemplified in the GSN. We then define the problem—the need for improved knowledge about the GSN in Norway and Sweden in order to contribute to the GSN.

Chapter II opens with a description of social networks, their evolution, design, and relevant factors when analyzing performance. It then lays out the theoretical framework for the analyses conducted throughout the project.

Chapter III is reliant on archival data and discussions with network members. This chapter describes and analyzes the GSN. In particular, it details the development and performance of the network, its "fit" with the environment, its design tensions, and its overall assessment of strength and weaknesses. Chapter III provides an understanding of the GSN in particular.

Chapter IV describes implications for NORSOCOM and SWESOCOM's contribution to and utilization of the GSN. The first part describes the challenges for

NORSOCOM and SWESOCOM when managing their GSN membership in the whole network. The second part describes NORSOCOM and SWESOCOM's internal management challenges when leading a national SOF network.

Chapter V summarizes the capstone project and offers our conclusions and recommendations. The chapter provides the main recommendations to NORSOCOM and SWESOCOM on how to manage their GSN membership as well as how to manage a potential national SOF network. Further, based on the analysis of the GSN in Chapter III, the project puts forward a few recommendations to USSOCOM on how to continue and enhance the evolution of the GSN into the near future.

To effectively contribute to the network as well as share the benefits of membership, Norway and Sweden need to understand the structure and critical aspects of networks in general and the GSN in particular. The next chapter provides the necessary framework of social network theory: What is a network? What is a social network? What is network design? How does one assess and analyze a network?

THIS PAGE INTENTIONALLY LEFT BLANK

II. SOCIAL NETWORKS

This chapter creates the theoretical framework for the analysis that follows in Chapter III and Chapter IV. The framework described in this chapter will give the reader a basic understanding of social networks and how we can design and analyze them to improve their performance.

A. THE FUNDAMENTALS OF SOCIAL NETWORKS

Networks are not a new phenomenon either in the civilian business environment or the military. Small networks have always existed—networks of family, friends, clubs, and co-workers. According to the network theorist Patti Anklam,

> We all use our networks every day. From the simplest transaction with a colleague to participating in complex multinational agreements, we are in webs of relationships that we tap into in order to accomplish something that we could not do by ourselves.[30]

However, today our growing interconnections and global reach are pushing us toward networks of increasing size and complexity. We are being challenged to understand large-scale networks and how to function and operate effectively within them. Although we have developed the social network analysis tools and methodology to analyze social networks, we still lack the basic understanding of social networks, how they are created and designed, how they are managed, and most importantly, how we conduct our "net work," within them.[31]

1. What Is a Social Network?

Social networks are made up of connections and relationships between humans. As Professor Nancy Roberts defines the term, a network is "two or more nodes that have

[30] Patti Anklam, *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World* (Amsterdam; Boston: Elsevier/Butterworth-Heinemann, 2007), xi.

[31] Anklam, *Net Work*, 1–2.

a sustained connection over time."[32] A node can be a person, group, organization, nation, etc., and exists inside the boundaries of a network.

Network connections or ties are the relationships between the human nodes that connect them. There can be different types of connections within social networks. For example, a network might have sub-networks of authority ties, information ties, advice ties, and trust ties. Each of these sub-networks (e.g., authority, information sharing, advice, and trust) when combined represents the network as a whole. For example, in a military organization authority ties represent the chain of command, but there are many other connections that unite military personnel.

2. Principles of Social Networks

There are many reasons for the turn towards networks: the constant and rapid change in the environment that favors quick and adaptive forms of organizing; the communication and information revolution; the desire to be more connected with stakeholders; and the desire to collaborate with others.

Patti Anklam puts forward eight fundamental principles to understand a network; see Table 1.[33] These principles will be referred to later in the chapter.

[32] Professor Nancy Roberts, Naval Postgraduate School, Monterey, California, 2014. Lecture in the network design course.

[33] Compiled from Anklam, *Net Work*, 4–7.

Table 1. Anklam's eight fundamental principles.[34]

Anklam´s 8 fundamentals:	Explanation:
Principle #1: If it's a network, you can draw it.	If you can see relationships between two or more people, groups, or organizations, and if you can identify something that they have in common, then it's a network and you can represent it by drawing dots and lines.
Principle #2: Every network has an underlying purpose, and every network creates value.	A collection of people and groups may be a potential network but will need a purpose to keep together. The purpose relates to the value that the network creates, which may not always be articulated, but can always be discovered.
Principle #3: Once we learn to distinguish and identify the unique and individual characteristics of networks we can create, examine, and shape their properties, boundaries, and environment.	Anklam categorizes the facets of a network in terms of *purpose, structure, style* and *value*. Within each facet are multiple elements and dimensions that illuminate choices in network design. The unique characteristics of any network determine how it creates value and just what that value is.
Principle #4: Because networks are systems of human relationships, we can best understand them using lessons from the study of complex adaptive systems.	A complex adaptive system is one that consists of elements, called *agents*, whose relationships may be changing all the time. Within the boundaries of a system, agents are capable of self-organizing, often following a simple set of rules.
Principle #5: Everyone in a network influences the relationships in and the outcomes of the network.	Any change, in a complex system, no matter how small, can have a far-reaching and potentially unexpected consequence.
Principle #6: A leader's work is to create and maintain the conditions that enable productive and innovative relationships.	Leaders may excel at traditional tasks of management, but they can never manage all the relationships in a network, nor direct all of its activities to predicable outcomes. Leaders must however, provide an environment in which relationships produce innovative and productive outcomes.
Principle #7: Successful networks are reflective and generative.	Networks are complex, not chaotic. Chaos occurs when all the existing patterns and norms have broken down. Networks engage in both creative and reflective activities that maintain self-awareness and provide boundaries within which the unknown and unexpected can be welcomed and managed.
Principle #8: (The Paradox). All networks are alike, and all networks are unique.	All networks have a purpose, a structure, a style, and value-producing mechanisms that are articulated or discoverable. But each network expresses those attributes in a unique and flexible combination.

[34] Anklam, *Net Work*, 4–7.

3. Level of Analysis

When studying and analyzing a social network it is important to be clear on what level of analysis is used. If the analysis is conducted at the individual level, it examines the network of person-to-person relationships. If the analysis is conducted at the group level, it examines the network of inter-group relationships. If the analysis is conducted at the organizational level, it examines the network of inter-organizational relationships, and so on. This project examines relations among the organizations participating in the GSN.

The term inter-organizational network has many different interpretations. Most note that they consist of multiple organizations that are legally autonomous, with connections based on cooperation and collaboration.[35] To define inter-organizational networks, the authors have used Professor Laurence J. O'Toole, Jr.'s definition of inter-organizational networks:

> Networks are structures of interdependence involving multiple organizations or parts thereof, where one unit is not merely the formal subordinate of the others in some larger hierarchical arrangement. Networks exhibit some structural stability by extending beyond formally established linkages and policy legitimated ties…. The institutional glue congealing networked ties may include authority bonds, exchange relations, and coalitions based on common interest, all within a single multi-unit structure.[36]

Within an inter-organizational network, one of the goals is to increase the *social capital*, social capital is

> [t]he stock of active connections among people; the trust, mutual understanding and shared values and behaviors that bind the members of human networks and communities and make cooperative action possible.[37]

The nodes in an inter-organizational network fill the function of bonding social capital within an organization, and/or bridging social capital between organizations. Social capital is created by making the skills, knowledge, and experience available to

---

[35] H. Brinton Milward and Keith G. Provan, *A Manager's Guide to Choosing and Using Collaborative Networks* (Washington, DC: IBM Center for The Business of Government, 2006).

[36] Milward and Provan, *A Manager´s Guide to Choosing and Using Collaborative Networks*, 9.

[37] Anklam, *Net Work*, 15.

anyone in the network at the point of need. The benefits of a networked organization then are the rapid access to information, knowledge, and experience when solving difficult tasks.[38] As Anklam notes, it is expected that understanding and using a networked approach could improve the organizations' resiliency, credibility, reach, diffusion of knowledge and innovation, collective intelligence, and individual and network performance.[39]

4. The Evolution of Social Networks

A network results from a conversation among individuals, groups, or organizations that see the potential for uniting in a common purpose to create value.[40] A network is created either by intent or through discovery. A network created by intent means that one or more constituents who have a clear purpose in mind create it intentionally. A network created through discovery means that the potential for a network is discovered when a shared interest or concern surfaces in a conversation.[41] Figure 2 shows Anklam's depiction of how a network is created and evolves over time.

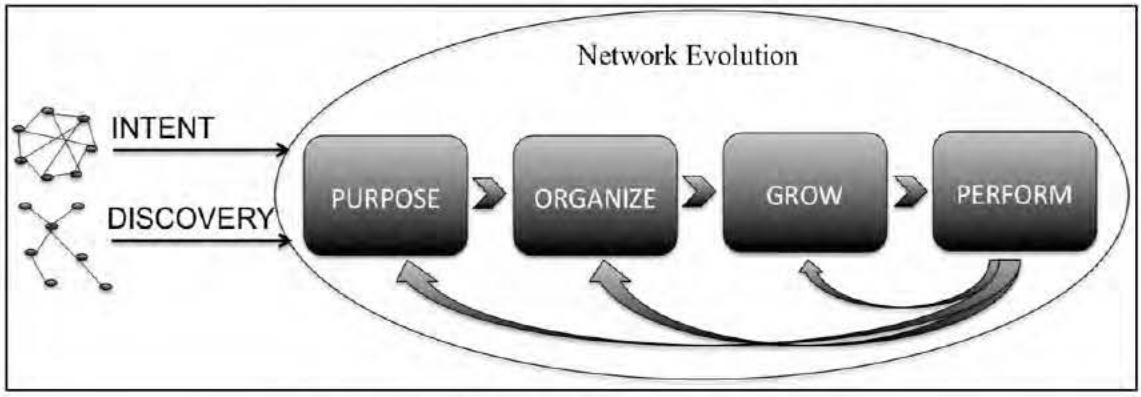

Figure 2. A network's evolution.[42]

[38] Anklam, *Net Work*, 25.

[39] Ibid., 26.

[40] Ibid., 132.

[41] Ibid., 132.

[42] The authors have changed the term *Design phase* to *Organize phase* to distinguish the phase from the overall network design as a whole. Anklam, *Net Work*, 133.

When the shared interest or common purpose has been identified, the network transitions into its *Organize phase*. During this phase, the activities are focused on establishing the network's purpose, identifying stakeholders, and initiating or strengthening relationships. Organizational tasks including establishing structure, style and a governance model, establishing norms for participation and defining the networks boundaries will have to be initiated in this phase as well.

During the *Growth phase*, the network continues building its capabilities, including structural, human, and relational capital, create new connections, and enhance its tensile strength as members work together toward the network´s purpose.[43]

During the *Performance phase,* the network maintains its momentum as members interact in value producing activities and conversations. The members are communicating across the network, managing problems, and responding to new possibilities and opportunities as they arise.[44]

These stages, especially the Growth phase, do not proceed in a linear pattern. There are setbacks and disruptions from both external and internal elements, as well as internal struggles and challenges that occur naturally over time. As depicted in Figure 2, the network will constantly have to examine how it is evolving and, if necessary, make changes to ensure that the network is performing well.

B. DESIGNING SOCIAL NETWORKS

As an organizing form, networks will never replace hierarchical structures or markets, but it is now clear that network forms (which vary) offer a range of choices for managing people, ideas, and work that were not previously available.[45] Depending on their purpose and tasks networks will have different designs. So to be able to understand the network and its elements it is important to understand the environment the network is operating in and how this influences the network and its performance. As stated by

[43] Anklam, *Net Work*, 133.

[44] Ibid.

[45] Ibid.

Anklam, the design of a network is one discussion point among the network's creators, organizers, developers, and stakeholders throughout the life of the network.[46]

1. Definition of Network Design

Professor Nancy Roberts proposes the following definition for network design:

> Network design is a constellation of a network's elements (e.g., its membership, purpose, interactions, structure, governance, etc.), which in combination describe the network as a whole.[47]

Designing a successful network requires that the constituents look for attractors that will draw people to the network; that they set boundaries for it; and design structures, events, and activities that they believe will forward the work of the network based on their knowledge and understanding of what brings people together. What needs to be reconciled is how to create networks in a way that acknowledges this complex property of emergence but also satisfies the need to provide direction and coherence.[48]

2. Components/Elements of Network Design

The following design aspects are important to consider when designing a network: *Purpose, Structure, Topography, Governance, Leadership,* and *Style/Culture*.

The *Purpose* is what prompts its members to care about the network and make them want to contribute to the network. The *Structure* is the network's "wiring diagram," the form and pattern of its connections among its nodes. *Topography* is the sum of all ties within the network. This gives insight into the resilience of the network. The topography gives the network its strength and weaknesses. *Governance* is the fine art and delicate practice of guiding and steering a network in a steady operational state. It is the function that keeps the network in balance and relationships intact. *Leadership* is the function that makes sure that the network is performing towards its purpose by creating and

---

[46] Anklam, *Net Work*, 141.

[47] Nancy Roberts, "Network Structure" (PowerPoint presentation, Network Design course, Naval Postgraduate School, Monterey, California, 2014).

[48] Anklam, *Net Work*, 160.

maintaining the conditions that enable relationships. The *Style* shows the nature of the network's interactions, its social climate, its culture, its core values, and norms.

a. Network Purpose

According to the authors Brinton Milward and Kevin Provan, "In order to know how to manage networks or to manage an organization operating within a network context, network managers must first understand the purpose of the network."[49] Anklam concurs in her *Principle #2: Every network has an underlying purpose, and every network creates value* (see Table 1).

The network's purpose statement or mission statement enables the network and its leadership to keep the network on track and ensure it is moving towards its proclaimed purpose.

Anklam notes that networks fulfill multiple purposes and she classifies them into five broad categories; *Mission, Business, Idea, Learning*, and *Personal*, as shown in Figure 3. It is important to note that a network can have more than one of these network purposes, for example, a combination of Mission, Idea, and Learning.

Figure 3. Main types of network purposes.[50]

[49] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 10.

[50] Anklam, *Net Work*, 31.

The shared purpose is one of the most important factors to enhance network collaboration. It is possible to have a network without clearly stated shared interest; however, network members need to be aware that divergent views on a network's purpose can create design tensions among network members (see the following discussion).

b. Network Structure

As Anklam has written, "The underlying structural pattern of a network is the most tangible of a network's properties: it is the aspect of the network that you can draw or visualize."[51] This statement relates back to Anklam's *Principle #1: If it's a network, you can draw it* (see Table 1).

One key aspect of social networks has been the identification of a distinct set of patterns that recur, and an understanding of how these patterns evolve over time, and insights into how a network's pattern predicts its performance. Figure 4 shows examples of the most common network structures.

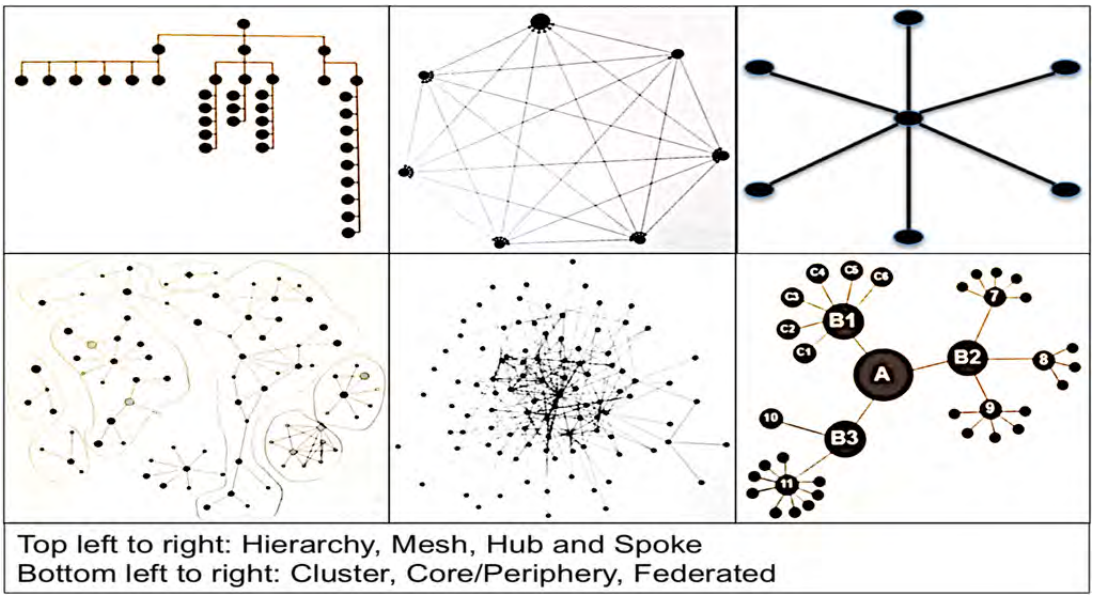

Figure 4. Main types of network structures.[52]

[51] Anklam, *Net Work*, 51.

[52] Anklam, *Net Work*, 53–67.

- *Hierarchy* is a network that propagates authority from a single person at the "top" through a structured series of subgroups. A common structure within government organizations.
- *Mesh*, also called *heterarchy*, is a network in which all members are equally connected to everyone else. A common structure within highly innovative focused, closed-knit teams in organizations.
- *Hub-and-Spoke* is a network where all the members are connected to one central hub. Typically, the hub holds the purpose of the network and sets the style.
- *Cluster* is usually a larger network that shows patterns of either connected or isolated groupings, or clusters, of nodes. This can reflect small groups of people who work together in the same geographic area. A common structure within a global cooperation that has offices around the world.
- *Core/Periphery* is a network with a "core," which is often a small number of people well known to each other, usually surrounded by a larger set of people on the periphery. A core set of people forms a hub, from which they connect to others.
- *Federated* is a network that has become a common structure when the network is spread geographically. The core network serves as the hub of multiple, relative autonomous hubs.

A network structure may look solid, hard-wired, and "objective." It is not. The structure is fluid and emergent, and its shapes are likely to change over time.[53]

As the environment and people change so will the network structures. Understanding how different structures are more or less suitable for different types of work is also important. For example, a hierarchical structure is less suitable in an environment focusing on innovation and creativity. Thus, there is no right structure for a network. Network structures are aligned with the environment, the type of work the network is doing, and the network´s purpose among other elements.

c. Multiple Structures

A key question in understanding social networks is to decide what relationships are important for the analysis. For example, trust, friendship, reporting, and information are all examples of different relationship types that can exist in a network. This means that relationship can create its own sub-structure. Together, these "sub structures" then form the "whole network structure." In other words, a network can have multiple sub-

[53] Roberts, "Network Structure."

networks with different structures and merged together these sub structures will produce a different overall structure for the whole network. One reason for conducting network analysis is to examine these relational patterns to illuminate how the network "really" works, such as finding informal hubs--the people whom others go to for information or who are best at communicating across boundaries in an organization.[54]

d. Network Topography/Texture

The people in a network are connected through ties that describe the nature of their relationships. From a structural standpoint, the sum of the ties—of any type—in a network gives it topography or texture.[55] There are many metrics related to the analysis of a network's topography. Four are most widely used: *density*, *distance*, *centrality*, and *open or closed*.[56]

- *Density* is the tightness of the structure. If everyone in the network were connected to everyone else, the network would have a density of 100 percent. The denser the network the greater resilience it will have. Density can also be correlated with the effectiveness of the network.
- *Distance* is a measure of how many people a piece of information needs to go through to get to everyone in the network. This is also called the "degrees of separation." This metric gives an indication of how quickly information can spread out across the network to reach all members. It also indicates how easy it is for any individual to reach the person who may be able to solve a specific problem.
- *Centrality* is a measure of how dependent a network is on one or two people or organizations.
- *Open or closed* is a measure of the balance within the network between external ties (those ties that people in the network go to for interaction outside of the network) and the internal ties (those ties among people within the network).

The topography of a network also can demonstrate the network's tensile strength, which is a network's ability to withstand stress and change without breaking down. The topography of the network depends largely on how easily ties are created, and the strength of the connections. It is also evidence of the mixture of strong and weak ties.

---

[54] Anklam, *Net Work*, 55.

[55] Ibid., 71.

[56] Anklam, *Net Work*, 72.

Strong ties are those between people who have known each other for a long time. Weak ties are ties that are not active, not used very much, or not shared by others in the network.[57]

e. Network Governance

All networks have some form of governance, explicit or assumed, which use a variety of levers to keep the network in balance and relationships intact. Governance is the fine art and delicate practice of guiding and steering a network in a steady operational state. It has to be flexible, attuned to the environment, and capable of change.[58] Anklam states that it is important, therefore, not to think of a governance model as an end-state but as an expression of increasing levels of coherence.[59]

Milward and Provan point out that inter-organizational networks have both network- and organization-level implications. Network-level managers have a major responsibility to ensure that all organizations that participate in a network are responsible for their share of network activities and are held accountable for their actions relative to the network-level purpose.[60] As *Managers of Networks,* their responsibilities are to coordinate overall network activities and ensure the successes of the network as a whole (see Table 2 which follows and Figure 16 in Chapter IV).[61]

Managers in Networks, in contrast, are individuals who represent their organization within the network. Their primary loyalty is to their organization, but they must work within a network context managing both the organization-level and network-level objectives to protect against split missions and split loyalties (see Table 2 which follows and Figure 16 in Chapter IV).[62]

---

[57] Anklam, *Net Work*, 72.

[58] Anklam, *Net Work*, 59.

[59] Ibid., 59.

[60] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks.*

[61] Ibid., 18.

[62] Ibid., 18.

Milward and Provan's concept of network management tasks (Table 2) is used as the analytical framework for describing the challenges for NORSOCOM and SWESOCOM as both Managers of Networks and Managers in Networks in Chapter IV.

Table 2. Management tasks in networks.[63]

Essential Network Management Tasks	Management *of* Networks	Management *in* Networks
Management of Accountability	• Determining who is responsible for which outcomes. • Rewarding and reinforcing compliance with network goals. • Monitoring and responding to network "free riders."	• Monitoring your organization's involvement in the network. • Ensuring that dedicated resources are actually used for network activities. • Ensuring that your organization gets credit for network contributions. • Resisting efforts to "free ride."
Management of Legitimacy	• Building and maintaining legitimacy of the network concept, network structures, and network involvement. • Attracting positive publicity, resources, new members, tangible successes, etc.	• Demonstrating to others (members, stakeholders) the value of network participation. • Legitimizing the role of the organization among other network members.
Management of Conflict	• Setting up mechanisms for conflict and dispute resolution. • Acting as a "good faith" broker. • Making decisions that reflect network-level goals and not the specific interests of members.	• Working at the dyad level to avoid and resolve problems with individual network members. • Working inside your organization to act as a "linking pin" to balance organization versus network demands and needs.
Management of Design (Governance Structure)	• Determining which structural governance forms would be most appropriate for network success. • Implementing and managing the structure. • Recognizing when structure should change based on network and participant needs.	• Working effectively with other network participants and with network-level management, based on the governance structure in place. • Accepting some loss of control over network-level decisions.
Management of Commitment	• Getting the "buy-in" of participants. • Working with participants to ensure they understand how network success can contribute to the organization's effectiveness. • Ensuring that network resources are distributed equitably to network participants based on network needs. • Ensuring that participants are well informed about network activities.	• Building commitment within the organization to network-level goals. • Institutionalizing network involvement so that support of network goals and participation goes beyond a single person in the organization.

[63] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 19.

Because networks are complex entities there is no one governance structure that fits all. The governance structure has to be aligned with the particular context of the network. The authors, Keith G. Provan and Patrick Kenis have identified three basic forms of network governance structures in inter-organizational networks: self-governance, lead-organization governance, and network administrative organization (NAO) governance (see Table 3 and Figure 5).

The most common form, self-governance, requires all network members to be active network managers. This form tends to be used when few organizations form a network. When more network members are involved, self-governance becomes too difficult, and they move toward more centralized network design, either with a lead organization form or a network administrative structure. The NAO structure means that member organizations of the network create a specific organization whose task is to manage the network as a whole.[64] Table 3 and Figure 5 provide a good overall explanation of the three structures and their differences.

Table 3. Network governance structures.[65]

Design Characteristics	Self-Governance	Lead Organization	Network Administrative Organization
Structure	No administrative entity, participation in network management by all members	Administrative entity (and network manager) is a major network member/service provider	Distinct administrative entity set up to manage the network (not a "service provider")—manager is hired
Optimal number of members	Few	Many	Many
Decision making	Decentralized	Centralized	Mixed
Advantages	Participation, commitment by members, ease of forming	Efficiency, clear network direction	Efficiency of day-to-day management, strategic involvement by key members, sustainable
Problems	Inefficient—frequent meetings, difficulty reaching consensus, no network "face"	Domination by lead organization, lack of commitment by members	Perception of hierarchy, cost of operation, complex administration

[64] Keith G. Provan and Patrick Kenis (2005) are cited in Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 7, 21–24.

[65] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 22.

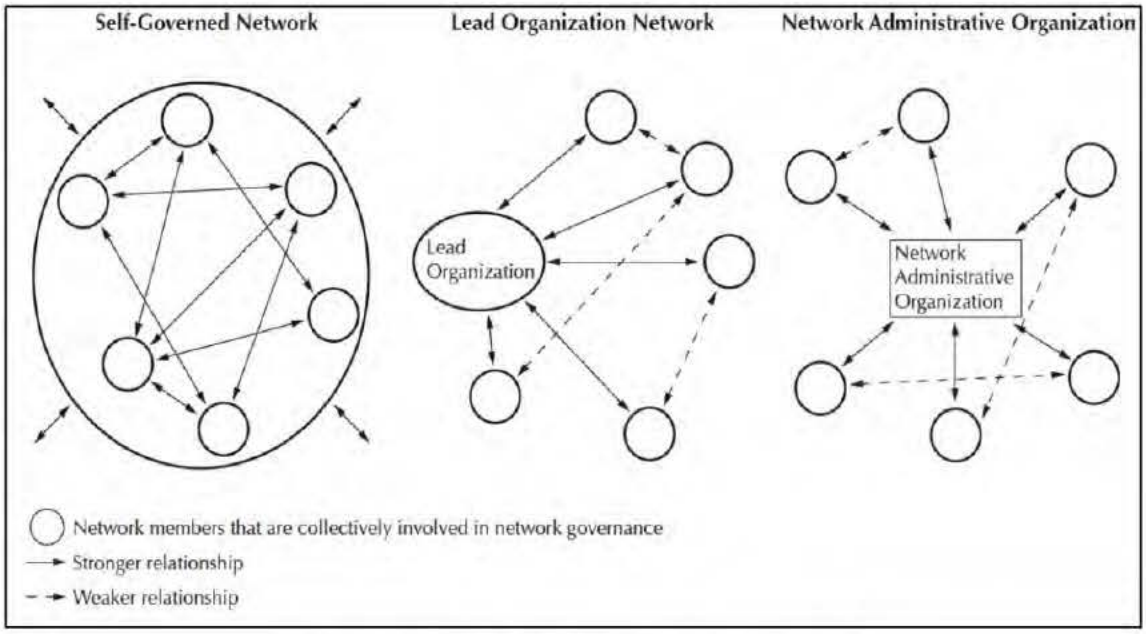

Figure 5. Network governance structures.[66]

Provan and Kenis' concept of inter-organizational network governance structures (Table 3 and Figure 5) is used to identify the three options for defining USSOCOM's leadership role within the GSN in Chapter III and for suggesting NORSOCOM and SWESOCOM's leadership role within the national SOF network in Chapter IV.

How the network identifies and accepts new members is another critical task for the network governance. There are three basic membership structures: *open*, *criteria-based*, and *invitation-only*.[67]

- *Open* networks are completely open for anyone to join. These networks trust that only people who have a serious intent on sharing the network's purpose will become participating members.
- *Criteria-based* networks require specific certifications, degrees, associations, resident with a particular area, or require members to sign agreements to become members.
- *Invitation-only* networks might suggest the close exclusionary bias of a country club. The members have to be invited to become members.

[66] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 23.

[67] Anklam, *Net Work*, 69.

In the 21st century, successful businesses and government organizations are attuned to the need to partner throughout their valued network. But the most important step after the network has figured out its purpose is to identify the right partners that can provide the resources that the network needs.[68]

f. Network Leadership

The work of network leaders is primarily to create and maintain the conditions that enable relationships. This statement relates back to Anklam's sixth principle: *Principle #6: A leader's work is to create and maintain the conditions that enable productive and innovative relationships* (Table 1).

Leaders convene diverse people and groups to identify common interests, build social capital with emphasis on trust and reciprocity, engage network members in a shared vision, manage conflict, generate cooperation, and build consensus through dialogue. Tim DeMello, founder and CEO of Ziggs, Inc., says the role of a leader is to make employees start to think in terms of their networks, to begin each day and each new task by thinking about their entire co-working network.[69]

The leadership element has to focus on integrating all the elements of interaction, orientation, locus, and culture to ensure that the members of the network can work in harmony. One aspect of the uniqueness of network is that everyone in a network can influence the relationships in the network, and thereby the outcomes of the network, as stated in Anklam's fifth principle (Table 1).

g. Network Style/Culture

Network style points back to Anklam's third principle. *Principle #3: Once we learn to distinguish and identify the unique and individual characteristics of networks we can create, examine, and shape their properties, boundaries, and environment*. To characterize a network by its style means looking at five key factors that contributes to the network's uniqueness. These are locus, culture, interactions, orientation, and

[68] Anklam, *Net Work*, 70.

[69] Ibid, 226.

leadership (described previously), which all have a key role to play in the design of a network.[70]

(1) Locus

Locus is where the network "lives"; its dimensions are *place, space,* and *pace*. For networks that meet and interact face-to-face the locus is a real physical place. For virtual networks the "place" can be cyberspace. All networks need an information space. It would be rare to find a network that does not have a virtual presence of some kind in an information system somewhere. A website can reflect the purpose, structure, and style of the network. The pace of a network comprises both rhythm and momentum, balancing connections in both place and space. The rhythm is what enables members to synchronize. When a network is not actively engaged in a project, it needs to have some regular pace of communication so that its membership continues to identify with it.

(2) Culture

Culture is the overall tone of the network. Cultural factors that set the tone for how the network is experienced include *identity, core values*, and *norms*. These all lead to and enhance the social capital of the network. All networks have an identity that it shares with all its members and often it is the basis for membership in the network. The network's core values are (or should be) part of the network's purpose statement, which reflects the common beliefs of the members. Key values that are common to successful networks are openness, diversity,[71] and transparency. The cultural norms consist of expectations about how people will behave in various situations. The specific norms that are foundational to a network are commitment to the collective, reciprocity, and trust. However, violation of trust—or any of the network's norms—can be managed well only in an environment rich in social capital. Social capital is the sum of the bonds among

[70] Anklam, *Net Work*, 81–116.

[71] However, other research suggests significantly lower trust in culturally heterogeneous teams, indicating that diversity can make it more difficult to build trust in a network with great cultural differences. Bjørnstad points to a need to allocate time to build trust in culturally diverse teams. Anne Lise Bjørnstad, "Network Organization Pitfalls and Success Factors for Team and Organizational Processes: Analyses of Key Organizational Variables and Cultural Differences in International Contexts." University of Oslo, PhD diss. submitted to the Faculty of Social Sciences and Department of Psychology. February 2012.

people in a network and the behaviors that are expected, allowed, and enabled by how people meet, greet, interact with, and otherwise express their shared identity with others.

(3) Interactions

Interactions are the way the network exchanges information both internally and externally. The three primary modes of interactions are transactional, knowledge-based, and personal or relational. The style of a network—and its ability to accomplish its purpose—is shown not just in the extent to which interactions of one kind or another predominate, but also in the ability of its members to know which style of interaction to use at what time.

(4) Orientation

Orientation of the network has to be aligned with the network's work. A network focused on outcomes designs its infrastructure, place, space, and pace toward production. But a network focused on discovery and learning might design its infrastructure and culture differently. It's not a matter of a "right" orientation, but rather a matter of making that orientation visible so the network can decide if it's balanced appropriately for its purpose.

C. ASSESSING NETWORK PERFORMANCE

Kenis and Provan established three exogenous performance factors: The form of network´s governance, whether the network is mandatory or voluntary, and the developmental stage of the network.

The governance form has consequences for what the network can actually achieve (see Table 3 and Figure 5). None of these governance structures is universally superior. Rather each differs in what it can do well. *Shared governance* has the strength of inclusion and involvement of its members and its flexibility towards its members' needs. A weakness is its relative inefficiency. *Lead organization governance* has the strength of efficiency and the inherent legitimacy provided by the lead agency. A potential weakness is the lead organization's own agenda and dominance of other members, which causes resistance. *Network administrative governance* has the strength of sustainability,

legitimacy, and to a lesser degree, its efficiency. Potential weaknesses are that network members may rely too heavily on the governance organization, making decision-making processes overly bureaucratic.[72]

Mandated versus voluntary inception of the network also will affect which type of performance criteria is most appropriate for use. Van Raaij's research shows a clear variation in the type of outcomes that can realistically be attained by the different types of inception. In contrast, regardless of inception type, Kenis and Provan argue that a network needs a common foundation of norms in order to achieve network-level outcomes such as a positive network climate, network legitimacy, and activating capacity.[73]

The developmental stage of the network is expected to affect the choice of performance criteria at various times during a network's life cycle. For example, it is clear that newly emergent networks have problems with goal attainment, while mature networks should be expected to attain network-level goals and be relatively efficient. During an early growth phase, networks should be expected to develop legitimacy, but not necessarily to *be* legitimate.[74]

This next section describes two tools to analyze a network, identify its tensions, and recommend solutions to enhance the network's performance to fulfill its main purpose. The two methods are the Systems Framework tool, and the Network Design Continuum tool, which are used in the analysis of the GSN in Chapter III.[75]

---

[72] Patrick Kenis and Keith G. Provan, "Towards an Exogenous Theory of Public Network Performance," *Public Administration* 87, no. 3 (2009), 444–449.

[73] Ibid., 449–450.

[74] Ibid., 451.

[75] Both tools described are from Professor Nancy Roberts, Naval Postgraduate School, Monterey, California, 2014.

1. Systems Framework Tool

The Systems Framework is a diagnostic tool to describe a network or an organization to identify areas for improvement. Figure 6 shows the systems framework tool with all its elements.

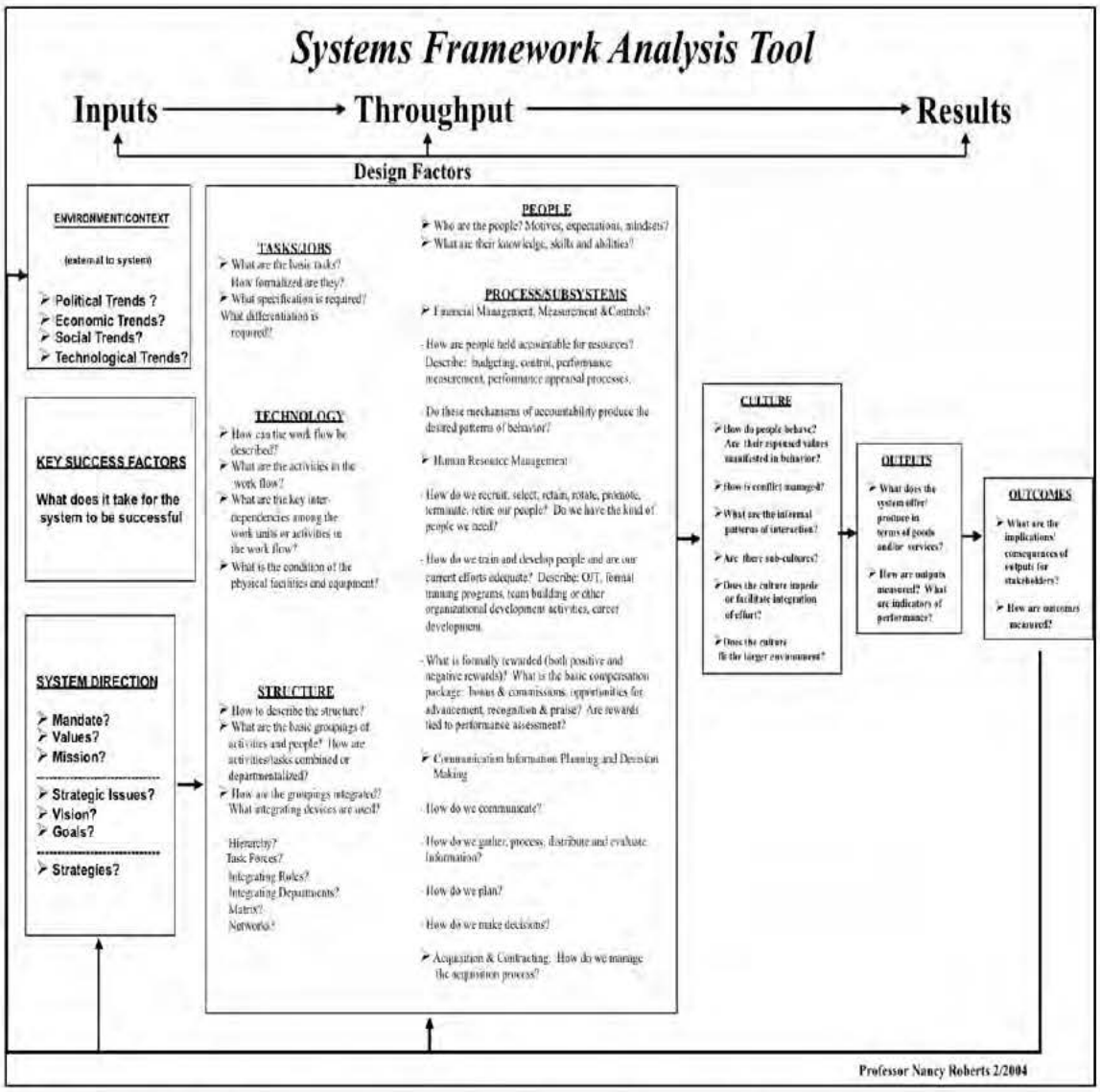

Figure 6. Systems framework diagnostics tool.[76]

[76] Nancy Roberts, "Systems Framework Diagnostics Tool" (PowerPoint presentation, Network Design course, Naval Postgraduate School, Monterey, California, 2014).

The systems framework tool is a comprehensive and systematic way of analyzing a network to identify where the network has difficulties that may interfere with its performance. The tool is split up into three parts: *Inputs*, *Throughput*, and *Result*. The inputs represent influence factors from the external environment and the guidance and directions given to the network from its leadership. Throughput identifies the design factors, or the internal elements of the network, which includes *structure*, *style*, and *value*. It describes how the members interact and cooperate within the network. Culture, for example, is manifested in people's behavior, conflict management, and informal patterns of interaction. Culture identifies the underlying health of the network, the informal structures, and what is the network's informal power. This element is made a separate element because it affects all three elements and is relative difficult to understand and change. Results are what the network achieves. This can be both positive and negative, and it can be both intended or unintended *outputs* and *outcomes*. Outputs are the direct results of an action, while outcomes are the more long-term results of the outputs.

One way to use this tool is to start by looking at what outputs and outcomes the network is producing and then go back and see if that matches the network's purpose. If there is a mismatch between the network's stated purpose and the actual performance then the next step is to ascertain where the problems lie—in the assessment of the environment, the system direction, the design elements, or the measurement of its results, or in the fit among all the elements that form the whole network.

2. Network Design Continuum Tool

The Network Design Continuum is a tool to describe a network in terms of its four different dimensions: *Unbounded to Bounded Membership*, *Informal to Formal Interactions, Heterarchical to Hierarchical Coordination,* and *Shared to Centralized Governance/Decision making*. When placing the network on these four dimensions, a judgment can be made of where the network lies on the continuum that ranges from *Anarchic Networks to Organized Networks*. Figure 7 gives an example of the network design continuum tool.

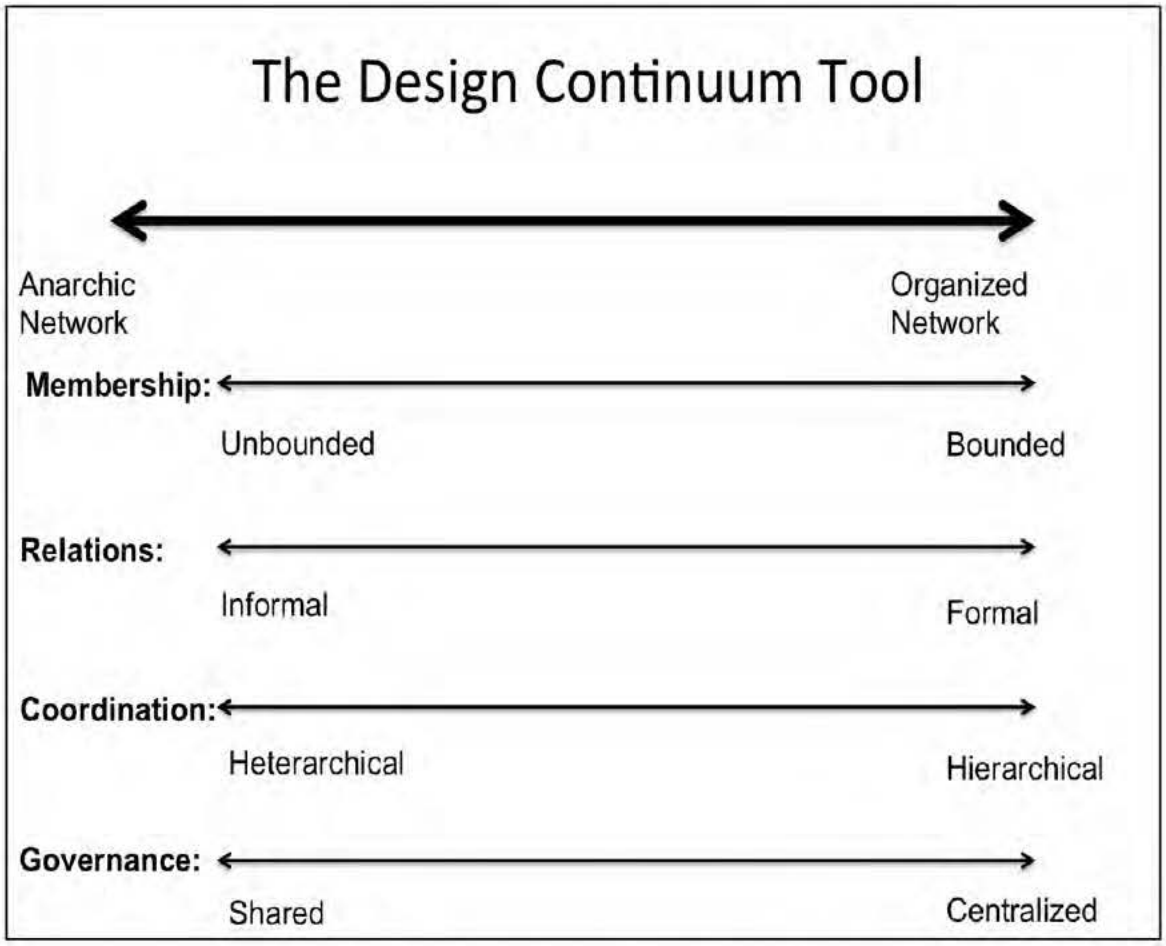

Figure 7. The design continuum analysis tool.[77]

Roberts' definition of the four dimensions:[78]

Unbounded to Bounded Membership Dimension

- Unbounded networks have no limitations on membership.
- Bounded networks limit participation and membership based on location or shared purpose or identity.

Informal to Formal Relations Dimension

- Informal networks are spontaneous, ad hoc, with voluntary interactions that emerge organically. They lack role definitions, codified purposes, and rules to govern network interaction, are built on personal relationships and self-organization.

[77] Nancy Roberts, "Design Continuum Analysis Tool" (PowerPoint presentation, Network Design course, Naval Postgraduate School, Monterey, California, 2014).

[78] Ibid.

- Formal networks have a purpose or goal that guides collective action. They are production networks, and have specified roles, tasks, processes, and procedures that constrain interactions.

Heterarchical to Hierarchical Coordination Dimension

- Heterarchical networks form structural patterns where each node connects with other nodes to coordinate and integrate activity.
- Hierarchical networks form structural patterns where one node coordinates and integrates all nodes in the network

Shared to Centralized Governance Dimension

- Shared governance networks have co-equal nodes that assume collective responsibility for decision-making. It is "pluralistic governance." Outcomes are generated without reference to centralized authority.
- Centralized governance networks have one node that assumes responsibility and authority for network decision making. It is "unicentrix governance."

Two main configurations anchor the network design continuum: *Anarchic Network* and *Organized Network*.

- Anarchic networks are voluntary with unbounded membership. This configuration will focus on informal interactions that rely on self-organization and shared decision-making.
- Organized networks have bounded membership. They have rule-constrained interactions that rely on hierarchical coordination and centralized decision-making.

A network design analysis should describe the whole network and its constituent elements. A configuration is composed of mutually supportive and interdependent features that "fit" together such that the presence of certain elements will vary consistently with the presence of others.[79]

By locating a network on the network design continuum, the analyst may be able to ascertain how well the network elements fit together. For example, a hierarchical coordination structure may fit better with a network based on mainly formal relations. An example of poor fit may be the combination of shared governance in a network with hierarchical coordination. A poor fit would suggest a need to intervene to improve

[79] Miller and Friesen (1984), *Estimation of "Fit,"* cited in Nancy Roberts, Network Design course, Naval Postgraduate School, Monterey, CA, 2014.

network performance.[80] For example, a well-organized network operating in a rapidly changing and dynamic environment might need to reorganize towards an agile, self-organizing network. Alternatively, as networks increase in size and complexity, leaders typically move towards the organized end of the design continuum, as a way of being better able "to manage" the network. The movement towards the organized end of the design continuum might enhance the network effectiveness, but only if the network, its constituent parts, and its environment are a good fit with one another.

3. Design Tensions

All networks will have tensions as they respond to changes in the environment, changes in the demographics of their members, and changes in purpose, structure, or style of the network.[81] For example, NATO, as a network of member nations has encountered internal tensions due to Russian actions related to Ukraine (change in the environment).[82] When a network principle or its underlying rules are broken, the network may go off course. It will need intervention of some kind to restore it either to the state from which it veered or to take it in another direction altogether, but with purpose.[83]

During the phases of a network's evolution, there are always tensions at play. It is important to understand that the network's evolution has to be constantly monitored throughout its lifespan. Networks can experience many different types of tensions, for example, between what's good for the network, that is, what supports both its purpose and its existence, and what's good for the individual in the network.[84] Both leaders and members need to be aware of how these tensions impact the network as a whole.

Different design tensions are further discussed in the analysis of the GSN in Chapter III and in Chapter V.

---

[80] Nancy Roberts, "A Conceptual Framework" (lecture, Network Design course, Naval Postgraduate School, Monterey, California, 2014).

[81] Anklam, *Net Work*, 142.

[82] NSNBC International, "Will France and Germany Challenge NATO?" September 22, 2014, http://nsnbc.me/2014/09/22/will-france-germany-challenge-nato/.

[83] Anklam, *Net Work*, 161.

[84] Anklam, *Net Work*, 99.

D. SUMMARY

Understanding social networks is a continuing process and demands some analysis throughout the life cycle of a network. Understanding the complex relationships between nodes within a network, and between the network and the external environment, are essential parts of making a network function and perform well. Roberts has put forward some guidance for practitioners when it comes to creating and designing networks. These are:

- Understand that network design is a matter of choice.
- Decide how you want to design your network and its elements, so that they are compatible with one another and the environment.
- Decide where you want to position your network on the design continuum, and manage the network accordingly.
- Understand that leadership and management vary depending on the network designs.
- Be prepared to identify and manage design tensions during the network's life cycle to secure network effectiveness and performance.[85]

The theoretical framework given in this chapter is the basis for the next two chapters, which provide an analysis of the overall GSN and a descriptive analysis of challenges for NORSOCOM and SWESOCOM as managers in networks and managers of networks. The analysis will utilize the elements discussed in this chapter, using both the systems framework tool, and the design continuum tool to illuminate potential tension areas within the overall GSN, and between the GSN and the environment.

[85] Roberts, "A Conceptual Framework."

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYZING THE GLOBAL SOF NETWORK

This chapter describes and analyzes the Global SOF Network with the overall purpose of deepening the understanding of the GSN from a network perspective among Norwegian and Swedish stakeholders. As an added bonus from this analysis, the paper also derives recommendations for USSOCOM on how to improve the overall GSN performance. The GSN's performance, evolution, internal and external "fit," design tensions, and strengths and weaknesses are analyzed through the lenses described in the previous chapter.[86] The second part of this chapter will focus on the network's initial performance, which includes an evaluation of the network's current weaknesses and strengths.

The United States and its allies have realized that no single nation can address the threats of the 21st century alone, and that there is rarely such a thing as a local problem. The globalized world is so interconnected that an incident in one place will have both second-and-third order effects in another place on the globe.

The international SOF community has been engaging one another for decades, but during the last two years, USSOCOM has strengthened the SOF enterprise into a Global SOF Network.[87] Currently, the GSN is in its early stages and still under development. Since 2012, USSOCOM has reinforced this network with communications infrastructure, stronger partnerships via liaisons officers (LOs) and a consistent battle rhythm.[88] The potential long-term benefits include promoting shared interests, enhanced information sharing, and improved integration, interoperability, and interdependence with partner nations and the U.S. inter-agency partners.[89] Ultimately the goal of this effort is to produce globally networked SOF—a cost-efficient, low footprint force capable of providing a persistent presence and rapid response to potential threats.

---

[86] The analysis is conducted on the organizational level.

[87] USSOCOM, ISOF Conference 2014, *Senior Leader Guide.*

[88] Ibid.

[89] Ibid.

A. DESCRIBING THE GLOBAL SOF NETWORK

1. The Network Participants

The GSN is an unbounded and open network where any nation can initiate contact with USSOCOM to become a member. The individual partner nation's (PN) degree of participation depends on its needs, ambitions, and resources. Some of the PNs are members because they need and want support through the GSN membership, while others are members because they have the SOF capacity and a desire to share the burden within the network. The GSN started with USSOCOM internally connecting the U.S. SOF and with the U.S. interagency communities. The growth continued through connection of PN SOF. Today the GSN consists of multiple sub-networks that together create the overall network. The main sub-networks are:

- The U.S. SOF network
- The U.S. inter-agency network
- The PN SOF network
- The Geographic Combatant Commands (GCC) and Functional Combatant Commands (FCC) network
- The Theater Special Operations Command (TSOC) network
- NATO SOF network

The list does not represent all the sub-networks of the GSN. However, these sub-networks are the most prominent at the inter-organizational level.

USSOCOM´s depiction of the GSN and its nodes is shown in Figure 8. The figure provides a generic picture of the overall network and the ties within the GSN, but a more detailed analysis of the network's structure and design is needed.

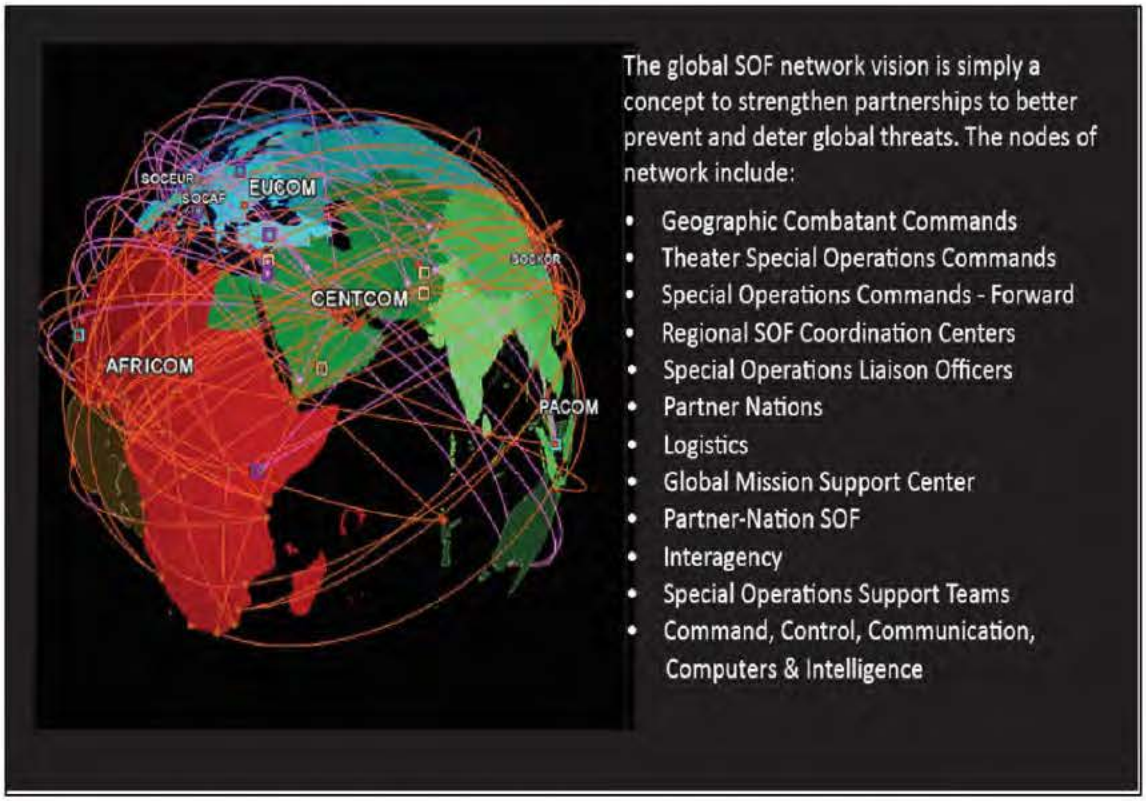

Figure 8. The Global SOF Network's nodes and ties.[90]

Figure 9 presents the authors' interpretation of the GSN nodes and relationships. This network will be the basis for the analysis in this chapter.

[90] USSOCOM, *SOF 2020, Global SOF Network.*

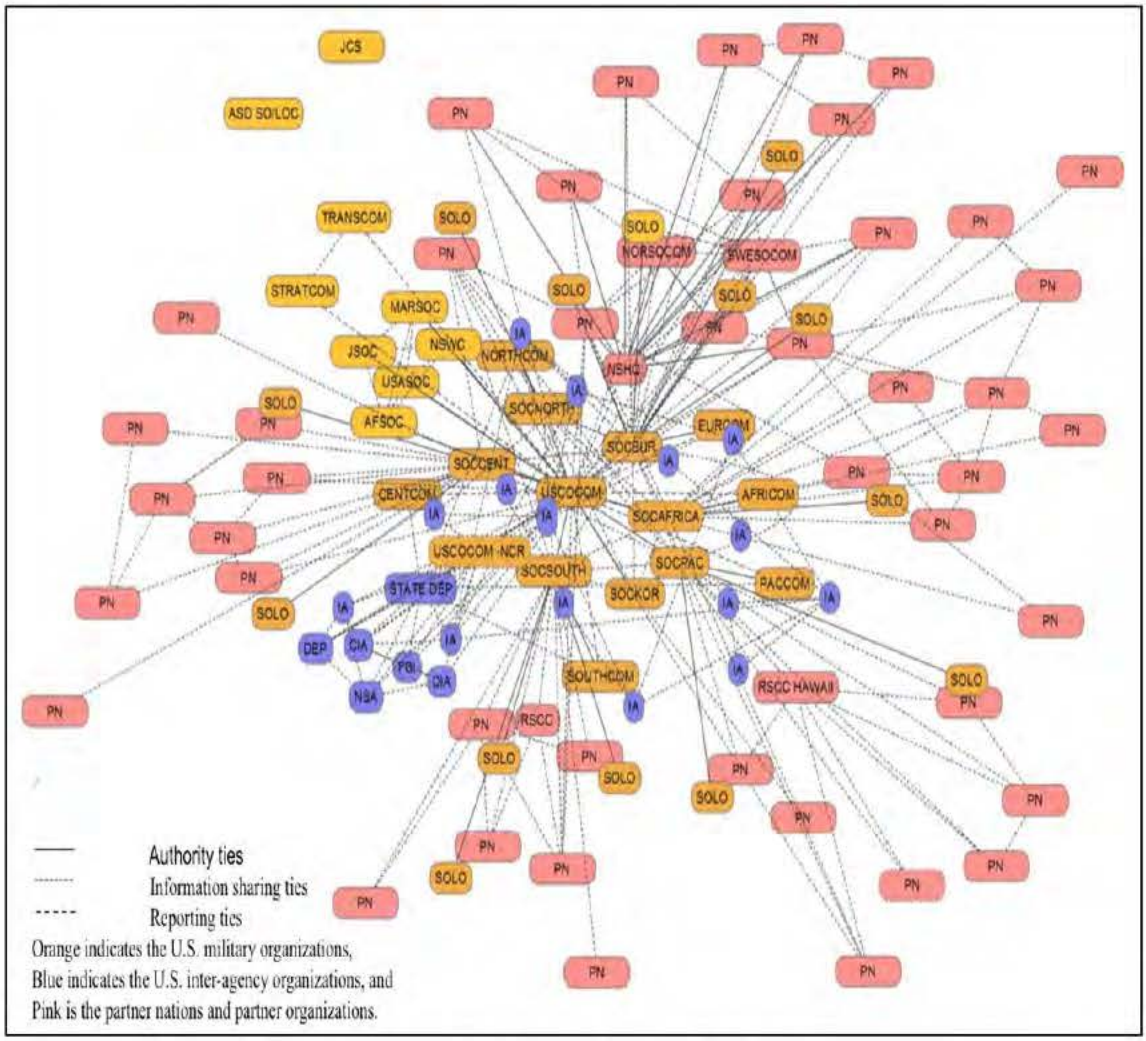

Figure 9. Sociogram of the Global SOF Network structure.

2. Purpose of the GSN

USSOCOM introduced the Global SOF Network concept to enhance its already worldwide force by networking with U.S. interagency counterparts, foreign allies, and partners around the globe.[91] One of the main drivers behind this approach was to link the SOF approach to the whole-of-government strategy, which would give the political leadership a holistic, small-footprint, and cost-effective tool to meet the threats of the 21st century.

[91] McRaven, Posture statement before the 113th Congress.

In the official USSOCOM documents the primary purpose of GSN is defined as:

> A globally networked force of SOF, Interagency, Allies, and Partners able to rapidly and persistently address regional contingencies and threats to stability.[92]

The more specific purposes for the GSN as part of the U.S. global strategy are:[93]

- To better support the GCC and TSOC with special operations forces and capabilities.
- To gain expanded situational awareness of emerging threats and opportunities by enabling small, persistent presence in critical locations and facilitating engagement where necessary or appropriate.
- To create a common picture of the global situation between the member nations to identify common interests and through that share the burden of action among the capable members.
- To enhance the information sharing between the network members.[94]
- To creating a forum where the various SOF communities can learn from each other and share lessons learned and tactics, technics, and procedures (TTPs).
- To build mutual trust, foster enduring relationships, and provide new opportunities to effect shared challenges among the GSN members.

Further, the development of J3-International at USSOCOM (discussed later in this chapter) facilitates opportunities for partner nations to identify common interests and build "coalitions of the willing" on specific issues. This function acknowledges the required processes among partner nations, for example, required UN mandate and parliamentary decisions before deployment of combat troops (see also Figure 12).

In sum, it appears that the GSN is a combination of a mission, an idea, and a learning type network. The *mission focus* is on improvement of the local, national, regional, and global level. The *idea focus* is on generative thinking for innovation and

---

[92] *The Role of the Global SOF Network in a Resource Constrained Environment*, JSOU Report. Ed. by Chuck Ricks, 2.

[93] McRaven, Posture statement before the 113th Congress.

[94] Information sharing and collaboration are the keys to building strong relationships with international partners and allies that assist in combating mutual threats and challenges. See USSOCOM, ISOF Conference 2014, *Senior Leader Guide*.

problem solving. The *learning focus* is on continuous improvement and enhancement of collective knowledge.[95]

3. The Network Evolution

The GSN was created intentionally by USSOCOM to address two major concerns:

- With Afghanistan ending, there was a need to conserve all the partnerships that have been created during the last decade of warfighting.
- Due to fiscal austerity and constraints the SOF community saw a need for a holistic, whole-of-government approach that focused on international collaboration and burden sharing.

In terms of the network's evolution, USSOCOM has focused on connecting the U.S. SOF community internally and connecting it with the inter-agencies to build a whole-of-government approach within the United States. At this initial stage, the U.S. stakeholders were identified and USSOCOM started working on the overall purpose for the network. The internal U.S. network became the basis for the continued evolution of the GSN. Figure 2 in Chapter II shows Anklam's depiction of the different phases the network goes through during its network evolution. The figure also illustrates that a network must go back to adjust as the environment changes or it will not perform the way it was intended.

During the growth phase, USSOCOM initially focused on the nations that already had LOs at either CENTCOM or USSOCOM and created what was known as the International Special Operations Coordination Center (ISCC) under USSOCOM to enhance the tensile strength among members while solidifying the network's purpose.

As the growth phase continued the ISCC transformed into the J3-I Division to better promote shared interests, enhance information sharing, and promote integration, interoperability and interdependence among PNs.[96]

---

[95] Anklam, *Net Work*, 31.

[96] USSOCOM, ISOF Conference 2014, *Senior Leader Guide*.

Currently the GSN is still in its growth phase and has met some setbacks and disruptions during its rapid growth, mainly from the political level, but also from the conventional side of the U.S. military. These setbacks are exemplified by the Commander USSOUTHCOM's rejection of USSOCOM's plan for a Regional SOF Coordination Center (RSCC) in Colombia, and the House Armed Services Committee's disapproval of USSOCOM's request to establish a Washington office.[97] In 2013, USSOCOM submitted the "Global Campaign Plan-Special Operations," which currently is with the political leadership for approval. Figure 10 shows the main objectives for the campaign plan.

Figure 10. Global Campaign Plan-Special Operations main objectives.[98]

Once this campaign plan is approved the GSN will be able to move from the growth phase and into the perform phase of its evolution.

a. Ties and Types of Relationships

The GSN consists of multiple sub-networks, which have different types of ties. The relationships range from simple information exchange to problem-solving

[97] Paul McLeary, "Lawmakers Skeptical of Global Spec Ops Plan," defencenews.com, August 10, 2013. http://www.defensenews.com/article/20130810/DEFREG02/308100007/Lawmakers-Skeptical-Global-Spec-Ops-Plan

[98] USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief).

collaboration to rich dialogue that raises ideas and insights. The main ties and relationships within the GSN are:

- Authority ties within the U.S. SOF community (JCS-USSOCOM-TSOC-SOCFWD-RSCC-SOLOs)
- Reporting ties with the greater U.S. military community (USSOCOM-GCC-FCC[99])
- Information sharing ties with the U.S. inter-agency (USSOCOM-IA-Dep)
- Reporting ties with the NATO SOF Alliance (USSOCOM-NSHQ)
- Information sharing ties with the partner nations (USSOCOM-PN SOCOM)

Figure 9 illustrates type of ties and relationships with various types of lines. However, the figure does not show the strength of each tie that is to say which ties are strong or weak. Strong ties are between nodes that have an active connection and communicate often with each other. Within the GSN strong ties are found in the authority relationships within the U.S. SOF community. Weak ties are between the nodes that do not have an active connection and do not communicate often. Within the GSN, one example is with PN and the interagency where there are information-sharing relationships.

The strength of the network depends on the mixture of strong and weak ties, and how well the network is able to utilize both types of ties and relationships to work together towards a common purpose. This research assesses that the GSN currently has an appropriate mixture of weak and strong ties. However, it is too early to judge how well the GSN is utilizing these ties to create the common picture so that the members can contribute towards a common purpose.

b. The Structure of the Network

The structural pattern of a network is the most tangible of a network´s property: It is the aspect of the network that can be drawn and visualized.[100] See Figure 9. The

[99] FCC-Functional Component Command. In addition to USSOCOM, the U.S. military has two additional FCCs: U.S. Strategic Command and U.S. Transportation Command.

[100] Anklam, *Net Work*, 51.

overall GSN consists of multiple structures within the sub-networks:[101]

- *Hierarchy* structure in the U.S. SOF network
- *Hub and Spoke* structure from USSOCOM to the PNs and the inter-agency
- *Mesh* between the PNs within the J3-I
- *Federated* network toward the GCC/FCC.

Looking at Figure 9, the overall GSN has to some extent a core/periphery structure. USSOCOM and the different organizations and nations with a Liaison Officer (LO) in USSOCOM are the core and the members that do not have an LO in USSOCOM are located on the periphery. The reason for this claim is that all the members that have a LO in USSOCOM have only one degree of separation and have more active ties among one other, while the members that do not have an LO in USSOCOM are separated by two or more degrees of separation and will automatically have a less active relationship.

However, another relevant criterion for active membership can be a PN's level of engagement in the J3-I's processes to address common interests. A PN's LO at USSOCOM J3-I, with only one degree of separation, who is not used for national interests and contributing to common purposes with other PNs in the GSN may, according to network structure, be positioned in the core of the network, but in practice have a less active partnership.

c. The Topography of the Network

Topography is described by Anklam as "Texture," which is the sum of all ties within the network. The texture/topography gives insight into the resilience of the network. Will the network withstand disturbance or will it just fall apart? A network's texture can be measured or analyzed through examining the network's *density*, *distance*, *centrality*, and if it is *open or closed*.

The *density* of the GSN is assessed as relatively sparse based on the developed sociogram (Figure 9). There are elements of the network that have higher density, but

[101] These structures can be inferred from Figure 3. The U.S. SOF hierarchy is illustrated by the authority ties (solid lines); the USSOCOM- PNs' Hub and Spoke is visualized through the information sharing ties (dotted lines) from USSOCOM to the pink colored PN nodes; the federated network, including the GCC/FCC, can be interpreted with the "geographical" dispersion of these nodes in the figure. The scale of the figure does not allow for the mesh-like structure of J3-I to be visualized.

overall it is sparse. This will probably change in the future as the network continues to grow. Density of 100 percent means that everyone in the network is connected to everyone else.[102]

Distance is a measure of how many people a piece of information needs to go through to get to everyone in the network. It indicates how quickly information can spread out across a network to reach all members.[103] In the GSN the longest degree of separation is five degrees, which means that there are no more than five steps between one member with a problem and a member with the potential solution. In most cases it will be less than five degrees. As the GSN continues to grow the degrees of separation can both increase and decrease depending on the number of established brokers.[104]

Centrality is the measure of how dependent a network is on one or two organizations. Currently the GSN is highly centralized around USSOCOM. The reason for this is that USSOCOM is the organization that has taken the initiative to facilitate the creation of the GSN and is the main champion of the network. The centralization around USSOCOM might be less obvious in the future. Perhaps the future will show a slight shift from USSOCOM to the TSOC's when the GSN starts to perform, and/or a slight shift to the PN's being more self-organizing outside of USSOCOM facilitation.

The *open or closed* metric describes how the network interacts with the outside. This is how the network balances the external ties with the internal ties. Is the network open for outsiders to join the network or is it closed? GSN is an open network that actively tries to connect with outside elements to grow and expand. However, some sub-networks are more closed to external ties because of the nature of compartmentalization for operational security and foreign disclosure. This is most prominent within the intelligence community and the inter-agency (IA). This will be discussed further in the section on the style of the network.

---

[102] The analysis has not used analysis software to develop the various metrics.

[103] Anklam, *Net Work*, 74.

[104] A broker is defined as a node, in this case, an organization that makes connections across groups. Anklam, *Net Work*, 77.

d. The Coordination Infrastructure of the Network

Aware of the difficulties associated with sharing of information between nations and organizations, the GSN is utilizing what is called the All Partners Access Network (APAN) as an unclassified information-sharing service. The U.S. Department of Defense (DOD) has used this system with great success for over a decade, primarily to coordinate disaster relief and organize multinational exercises and conferences.[105] The APAN system is a good example of the network's informal relations. Because this system is unclassified and accessible to everyone in the network it promotes a heterarchical structure of coordination. (See "Network Design Continuum" in Chapter II, for more information.)

As a network of military organizations, the GSN has a need for a classified information-sharing system as well. BICES-X, based on the already existing NATO Battlefield Information Collection and Exploitation System (BICES), offers a potential solution to this challenge; however, it is currently not widely fielded. The BICES system is distributed through the chain of command (top-down distribution), and because the system has more restrictions when it comes to access, it promotes a more hierarchical coordination structure within the network (see "Network Design Continuum" in Chapter II). Figure 11 shows USSOCOM's plan for Information and Communication Technology (ICT) infrastructure within the GSN.

[105] USSOCOM, ISOF Conference 2014, *Senior Leader Guide*.

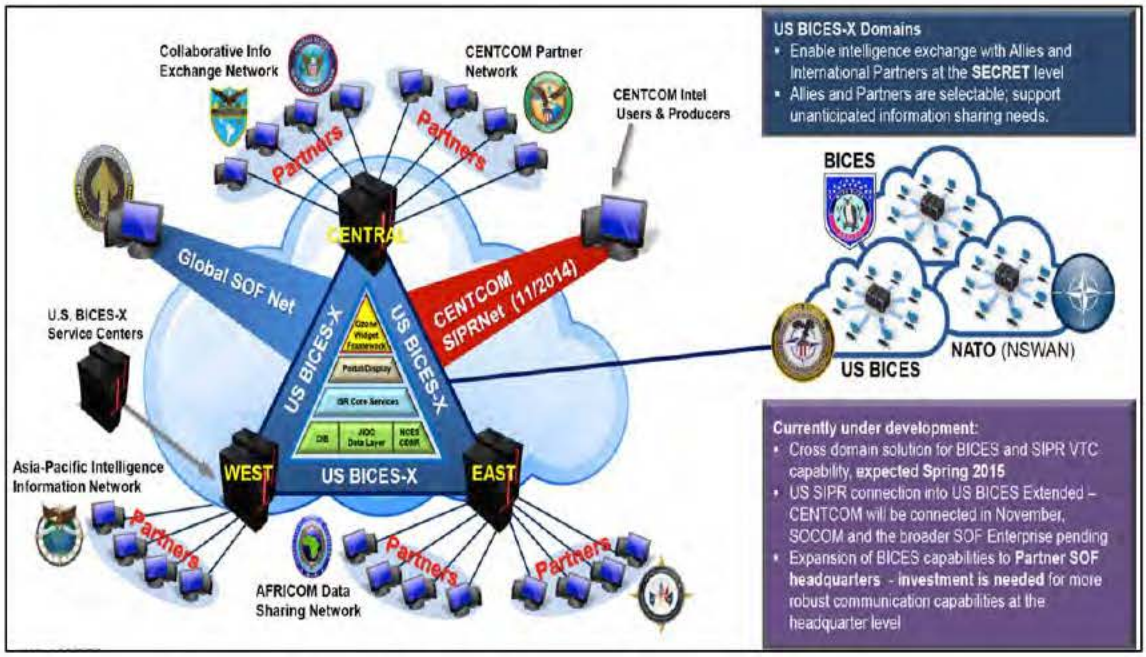

Figure 11. GSN planned communication infrastructure.[106]

All of these systems can be utilized as a tool for collaboration, a forum for information sharing, and a virtual workspace to enhance collaboration with a goal of creating a common picture within the network.

The last enhancing element to connectedness and information sharing is the LO's ability to connect to their national systems, allowing rapid reach back to their own countries. In addition, USSOCOM hosts the International SOF Conference (ISOF Conference) biannually in Tampa, creating a venue for face-to-face meetings and discussions.

e. The Governance and Leadership of the Network

Governance is the fine art and delicate practice of guiding and steering a network in a steady operational state. Governance is not static but flexible, attuned to the environment, and capable of change.[107]

---

[106] USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief).

[107] Anklam, *Net Work*, 59.

USSOCOM, as the champion of the GSN, has taken on the governance role of facilitating, and synchronizing the Global SOF effort. Thus, within the U.S. SOF network decision-making tends to be centralized. However, decision-making in other parts of the GSN is decentralized and differs within the various sub-networks. For example, for the PN sub-network and the IA sub-network, the decision-making is done within each organization/nation based on individual interest and needs. In short, the GSN has overall shared governance, which makes the *Leadership and Management* of the GSN a challenge; there is no one single leader of the network. This makes the synchronization and information sharing even more important to enable members of the network to make decisions based on a common picture. Another example of how USSOCOM is building commitment to the networks' purpose is the biannual ISOF Conference, which is a venue for the PNs to raise their concerns and be part of the discussion.

One important aspect that Milward and Provan highlight in their inter-organizational network research is that the leaders or managers of a network must first understand what type of network they are managing and its purpose.[108] Their research has identified four distinct types of networks: *Service Implementation Networks, Information Diffusion Networks, Problem Solving Networks,* and *Community Capacity Building Networks*.[109] Through this lens, the GSN is a combination of the information diffusion, problem solving, and capacity building networks. All of these objectives and purposes are built into the overall purpose of the GSN: sharing information to build the collective capacity with the ultimate goal of solving new challenges.

The next step for a network manager is to perform essential tasks that ensure the network is successful. Milward and Provan's five broad and essential tasks that managers must perform, described in Chapter II Table 2, were: *Management of Accountability*, *Management of Legitimacy*, *Management of Conflict*, *Management of Governance*, and *Management of Commitment.*[110] We return to these issues in Chapter IV when we review

---

[108] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*.

[109] Ibid.

[110] Ibid.

the tasks essential both to the role of the *Managers of Networks*, and *Managers in Networks* (see Table 2 in Chapter II and Figure 11 in Chapter IV).[111] As the GSN has not started its performance phase, the most important task at this point is the management of the governance structure to secure the GSN's accountability, legitimacy, and its ability to handle future conflicts and commitments.[112] These management tasks are further discussed and developed from the PN perspective in Chapter IV.

Provan and Kenis' three basic forms of network governance, as described in Chapter II, include: *Self-governance*, *Lead Organization governance*, and *Network Administrative Organization (NAO) governance*.[113] They have different strengths and weaknesses and have to match up with the network's structure and purpose (see Table 3 and Figure 5 in Chapter II). This aspect of network management is also further discussed in Chapter IV.

Based on the creation of the J3-I and the GMSC within USSOCOM, it appears that USSOCOM has adopted the form of a Network Administrative Organization for the overall network. USSOCOM is facilitating and synchronizing the day-to-day management through a focus on strategic/global involvement. The synchronization and facilitation is done through the Global Mission Support Center (GMSC) and the J3-I staff procedures. One way that USSOCOM manages this process is through the *Campaign Synch Process* (see Figure 12).

---

[111] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*.

[112] Accountability and legitimacy will be further discussed later in this project.

[113] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*.

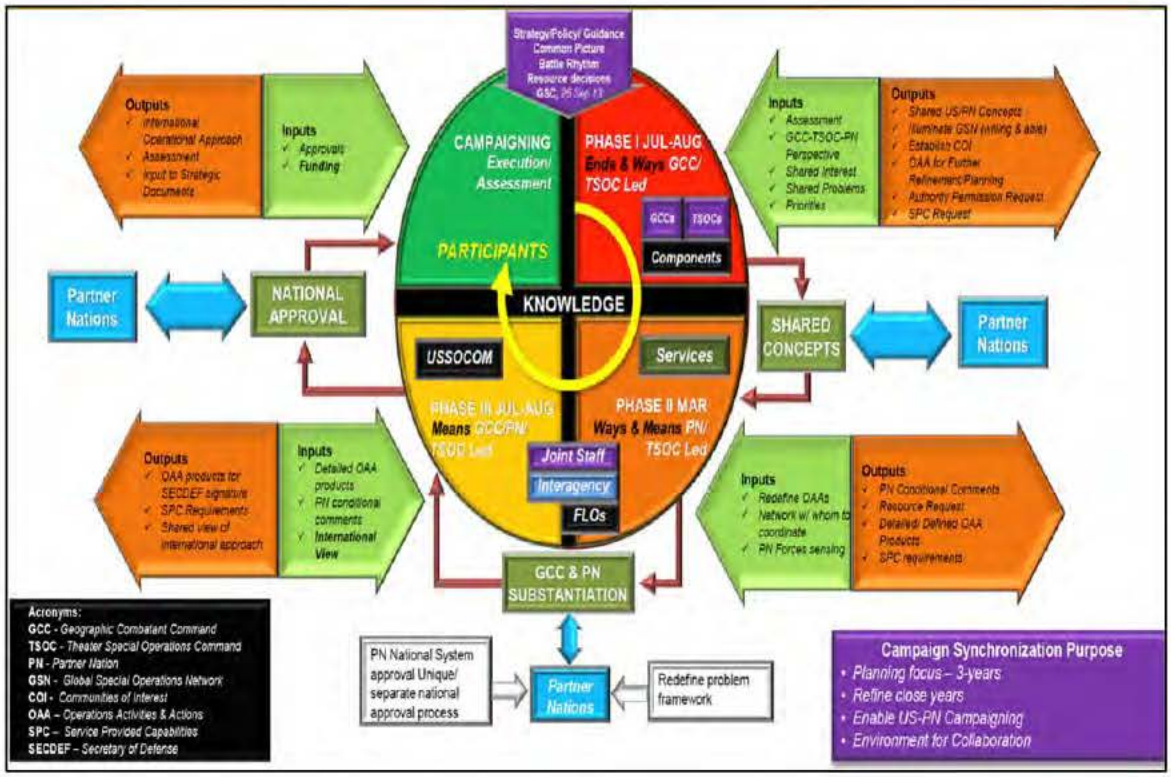

Figure 12. Campaign synchronization process.[114]

The campaign synch process (Figure 12) is a one-year planning cycle with a three-year planning focus. Based on the strategic guidance the GMSC and the J3-I manages this process for multiple problem sets around the world. The model illustrates PN involvement in each phase through the inputs and outputs.

A complicating factor to this synchronization is that the different sub-networks have different forms of network governance. The PN network has a self-governing network, where all members manage participation and the individual organizations/nations make their own decisions. Within the U.S. SOF network, USSOCOM has the lead organization form, which is more centralized and formal. The different forms of governance can present both advantages and disadvantages for network performance. It can provide sub-networks more autonomy, but again it can be difficult to create a strong commitment toward the overall purpose of the network.

[114] USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief).

f. Roles, Tasks, Activities, Operations, and Processes within the Network

(1) Roles

Anklam describes the roles in a network through the categories of stakeholders, choreographers, and orchestrators, and structural roles of governance and infrastructure.[115] The main stakeholder in the GSN is the founder and driver, USSOCOM. The lack of outspoken and salient supporters at the policy level as well as at the highest levels of defense raises the stakes for USSOCOM. The GSN needs buy-in from the U.S. military, interagency, and policy level and from PNs on the initiative. The other U.S. stakeholders within the network such as the interagency, departments, and military services will to some degree be affected, but mostly in the areas of cooperation and sharing. A PN with national internal security challenges will benefit from better coordinated and sustained support from the network. An expeditionary capable PN can possibly foresee access to supporting resources and information from the vast U.S. SOF capacities when conducting SOF operations abroad.

USSOCOM confirms Anklam's notion that successful networks need the choreographer and orchestrator to "stay with the show."[116] The original architects that established the NATO SOF Coordination Center (NSCC) with Admiral McRaven in 2006 have been intimately involved in the overall GSN concept development as well as the ISCC and J3-I progress.[117]

The GSN has been developed on the U.S. SOF "frame," which naturally results in USSOCOM holding most of the *structural roles.* USSOCOM fits Anklam's *governance roles* of network leader and "steering group." However, discussions point to USSOCOM desires for more PN LOs/staff officers in the lead of planning and coordination events

---

[115] Anklam, *Net Work,* 136–140.

[116] Ibid., 137.

[117] Two of the GSN architects are Colonel (USA, Ret.) Stuart Bradin, who after his recent retirement continues to head the Global SOF Foundation, and Colonel (USA, Ret.) Mark Rosengard, who has been employed as a contractor to work in the USSOCOM ISCC/J3-I.

within the J3-I.[118] Hence, USSOCOM is trying to reduce the perception of U.S. leadership in the network. Further, USSOCOM frames its role as "synchronizer" of the global SOF effort.[119] PNs with LOs in J3-I can be defined as *core members*, while *peripheral members* can be seen as PNs without permanent U.S. SOF presence in their country or without LOs at USSOCOM. PN with permanent U.S. SOF in their country and/or with well-developed regional U.S. SOF cooperation might fall closer to the core member definition.

The USSOCOM's infrastructural roles fall within Anklam's classifications of meeting coordinator, facilitator, and communicator. As with the structural governance roles, USSOCOM rotates other nation's representatives as meeting coordinator and working-group leaders to decrease its dominance. However, USSOCOM will continue as the main facilitator and communicator for the GSN. The notion of rotating staff leaders indicates informality within J3-I.[120]

Another way to define the roles within the GSN might be: USSOCOM as facilitator and synchronizer; TSOCs as user (of U.S. SOF assets); intelligence agencies as intelligence/information sharers and receivers; departments as co-coordinators of the whole-of-government approaches; expeditionary capable PNs as burden sharers; and internally focused PNs as receivers of SOF support.

(2) Tasks

Tasks are defined as the basic jobs, their level of formalization, and their specifications required.[121] The basic tasks for the GSN can be found in the GMSC, which has the following responsibility: maintain global awareness; provide responsive support

---

[118] Colonel (USA, Ret.) Mark Rosengard is one of original architects of the GSN concept. Discussions during International SOF Conference, May 21, 2014.

[119] USSOCOM, "ISCC Processes and Battle Rhythm," (Information Brief, April 30, 2014, PowerPoint).

[120] Anklam, *Net Work*, 140.

[121] Roberts, "Organizational Systems Framework."

to TSOCs and components; and manage the strategic battle rhythm.[122] J3-I, which is integrated within the GMSC, holds the following tasks: maintain common picture of (PN's) shared interests; facilitate and institutionalize mission PN relationships; and catalyze PN collaboration, integration, interoperability, and interdependence. Further, J3-I holds the task to identify and suggest multinational solutions to problems. This is done for Commander USSOCOM purposes, as well as for the PN SOCOMs that have invested in the GSN effort.[123]

The J3-I's mission statement is as follows:

> Maximize mission partner nation integration in HQ USSOCOM staff processes to inform strategic planning and resourcing, and accelerate development of multilateral courses of action and cooperation among our global SOF partners in support of the partner nations, TSOCs, and Geographic Combatant Commands.[124]

These tasks require a certain level of structure and formalization, which USSOCOM has created and manages through the campaign synchronization process (see Figure 12).

For example, one task is the effort to standardize reporting formats and routines. As USSOCOM describes it in the Senior Leader's Guide for the ISOF conference: "in order to network an enterprise, we need … a disciplined battle rhythm."[125] Staff officers and PN LOs conducting these tasks have a certain degree of specification visible in the job qualifications.[126]

---

[122] USSOCOM, *Job Description*: Part 1, Job Identification (Special Operations Liaison Officer to HQ USSOCOM, Foreign Liaison Officer), DRAFT 1. Tampa, Florida, 2014.

[123] USSOCOM, "ISCC Processes and Battle Rhythm," (Information Brief). Other tasks within the GSN are mostly "military staff actions," such as information, planning and coordination meetings, Inter-agency/ LO coordination and/or input, etc., and are seen as common knowledge to the reader, hence not described in this paper.

[124] USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief).

[125] USSOCOM, ISOF Conference 2014, *Senior Leader Guide*, 7.

[126] USSOCOM, *Job Description*. For example, suggested PN LO standards include Command and Staff College, English proficiency level 3/3, SOF qualified on command level, and experience at the national military strategic level.

(3) Operations and Processes

The description of Operations and Processes will be limited to what Roberts defines as Communication Information Planning and Decision Making. This is how the GSN *communicates*, *manages information*, *plans*, and is involved in *decision-making*.[127]

Communication is conducted through a combination of standard military reporting according to a set battle rhythm as well as informal information sharing. Notably, video teleconferences (VTCs) are regularly used to conduct meetings, such as the COM USSOCOM regularly scheduled meeting/VTC with all the TSOC commanders. The overall purpose of the communication is to develop and maintain the "common picture." The communication is a mix of regularly scheduled reports and meetings; ad hoc communication related to crisis response, and "deep dive" meetings to improve the understanding in a specific area. Included in the GSN communication, as described earlier in the chapter, is the use of APAN as a forum for unclassified communication and the utilization of BICES for classified SOF forums. Articles, regional situation summaries, and other SOF-related topics are posted on the APAN web page. In summary, the communication is a mix of written correspondence, phone calls, VTCs, and face-to-face meetings. They are either conducted within the framework of GMSC/J3-I, or via the APAN webpage.

This study has limited information on the actual information management procedures. However, discussions have identified some challenges for the PN LOs in communicating via secure national means to their national HQ.[128] For example, the J3-I is separated from the "U.S.-only" GMSC. The planned distribution of BICES-X will improve the capability in this area by establishing a common communication network for sharing of classified information. This system also will enable selected groups, or enclaves, to share classified information. For example, during combined/coalition operations, an enclave for collaboration can be established so that only the involved

[127] Roberts, "Organizational Systems Framework."

[128] The J3-I premises are prepared for PNs national secure communications. The frictions in this regard are related to the respective PNs' efforts to establish the national communication system.

countries (the burden sharers) share information without disclosure to other PNs (shown in Figure 11).

The principle outline of the GSN strategic level facilitation and planning procedures between USSOCOM and the PNs has recently been updated (see Figure 13).

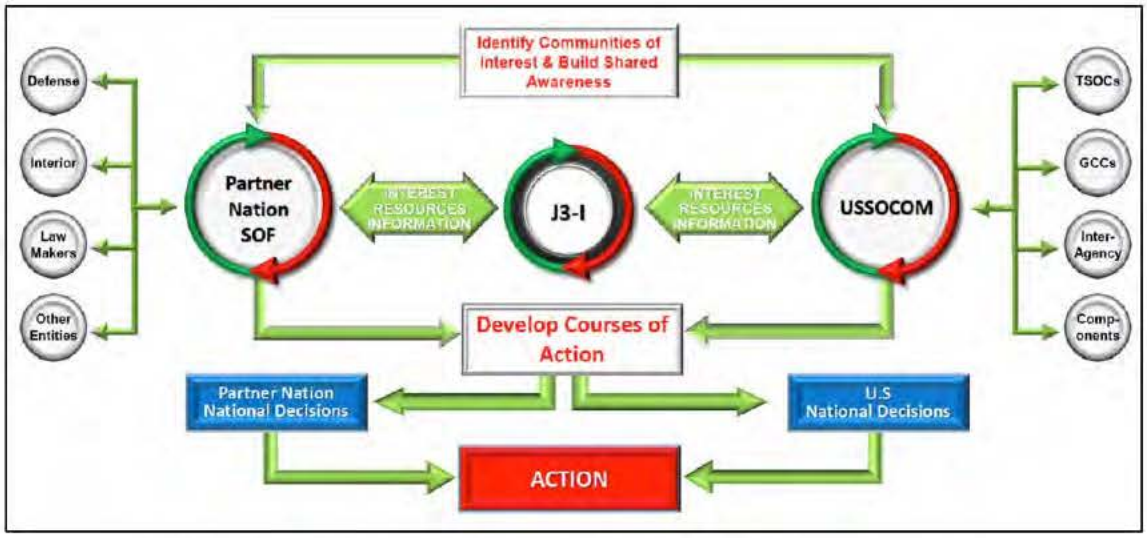

Figure 13. U.S. and PN´s facilitation and planning process.[129]

This is the framework for how PNs will integrate into the overall long-term SOF campaign plan (see Figure 12 and 13), as well as collaborate on emergent issues. The campaign design process includes PNs' input of national strategic guidance, and national interests and issues to identify potential partners and requirements. For example, when a problem is identified and framed solutions are developed into concepts including multi-national approaches, required resources, and required level of accesses. When national approval from the contributing PNs is attained, the J3-I continues detailed planning for possible execution.[130]

Emergent crisis collaboration includes PNs' input with national information and possible requests for support (RFS). Pending time available for strategic planning, there

[129] USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief).

[130] USSOCOM, "ISCC Processes and Battle Rhythm," (Information Brief), 7. This is J3-I's intention. Detailed planning is also done at the TSOC level. This might be a challenge for small contributing PNs.

will be staff procedures including analysis, regional and functional issue forums, and coordination among PNs. These processes then will develop into a common picture, concept collaboration, COAs, CONOPs and resource solutions.[131]

Decision-making in relations to the GSN is described previously (see "Governance and Leadership of the Network"). In short, decision making outside of the U.S. SOF realm is decentralized to the PN's national decision-making process, which in turn is often related to UN, NATO, EU, and AU decision-making processes.[132] These decisions often result from a collaborative process among PNs.

g. The Style of the Network

The style of a network can be found in the unique-shaping key factors of locus, culture, interaction and orientation, which in turn influence the design of the network.[133]

(1) Locus

Locus is where the network "lives" and can be divided into the dimensions of a *real place*, *information space*, and *interaction pace*.[134] While the GSN is globally dispersed physically, USSOCOM facilitates the J3-I with real place localities that are adjacent to the GMSC. The new localities are designed specifically to meet anticipated needs and procedures within J3-I described earlier.[135]

---

[131] USSOCOM, "ISCC Processes and Battle Rhythm," (Information brief), 10.

[132] The PN can also conduct unilateral or bilateral operations outside the framework of these alliances based on political approval.

[133] Anklam, *Net Work*, 81. Anklam also includes Leadership within the Style factors. This paper analyzes leadership separately.

[134] Ibid., 81–82.

[135] The authors' visit at J3-I on May 19, 2014. The office design is composed of open spaces promoting informal communications and spontaneous meetings, as well as space for secure group meetings or individual secure communication back to the PN.

The virtual workspace, or information space, is created through the APAN platform, allowing for unclassified information sharing and collaboration in the GSN.[136] Classified information will require the use of BICES or national communications means between PN LO at J3-I and the PN. Admiral McRaven describes the idea (maybe with a focus on the U.S.-specific capacities): "The C4I structure flattens the network and enables all levels to reach out to get what they need."[137]

The interaction pace within the GSN is met through USSOCOM's, and more specifically, J3-I's Battle Rhythm. COM USSOCOM holds regular VTCs with GCC and TSOCs. The J3-I is integrated in the schedule with VTCs and other correspondence with the PNs.[138] Anklam would classify the ISOF conference as an event, which all networks might require to refresh and revitalize themselves.[139]

(2) Culture

How the network is experienced is dependent on the tone-setting cultural factors, which include identity, core values, and cultural norms. These factors affect the social capital of the network.[140]

The name of the network—the Global SOF Network—appeals to the identity of the members, regardless of nationality: Special Operation Forces emphasizes the people in the organization as the main strength. The personnel are what make SOF "special": attracting and preserving the right people with a high standard of training and education, empowered with advanced technology. USSOCOM advocates for the need to cultivate

---

[136] USSOCOM, ISOF Conference 2014, *Senior Leader Guide*, 7–8. Videoconferencing (VTCs) can easily be arranged. Various GSN communities have established sites/forums; Training, Aviation, Regional Groups, and Joint Intelligence Center. It is too early to evaluate the architecture and design of this effort. Will it be useful and purposeful? Anklam, *Net Work*,85.

[137] William McRaven, Briefing during GEOINT 2013 Symposium, Tampa, Florida. 14–17 April, 2013. http://geointv.com/archive/geoint-2013-keynote-adm-william-h-mcraven/

[138] USSOCOM, "ISCC Processes and Battle Rhythm," (Information Brief).

[139] Anklam, *Net Work*, 88, 90.

[140] Ibid., 92. In this project, the term "social capital" is used interchangeably with "trust."

this unique SOF culture and to continue to invest in people to be able to operate in any future environment.[141]

Successful networks often include the core values of openness, diversity, and transparency. These properties complement each other.[142] The GSN, as has been described previously, is an open network due to its bridges to other networks and its active use of those bridges: USSOCOM has LOs at more than 20 agencies in the United States, as well as Special Operations Liaison Officers (SOLOs) connected to U.S. country teams in many high interest countries. Moreover, the GSN bridges through each PN's existing national networks. The diversity within GSN is manifested through the variety of PN capacities and their ethnical, religious, security, and political contexts together with the inclusion of various agencies, departments, academia, and think tanks. The transparency, which Anklam asserts as required for problem solving and innovation, is clearly indicated as in the example of the creation of the J3-I inside USSOCOM, and the enhanced cooperation with U.S. IA. However, the compartmentalization does limit transparency in areas of operational security and certain capacities.[143]

The cultural norms covered in this analysis are the specific norms of commitment to the collective and trust.[144] The fact that a PN can have purposes for participating in a specific action other than the overall network can affect the commitment to the collective. Anklam points specifically to the commitment to build and sustain relationships as a core obligation of the work within the network:[145] How much effort the PNs are willing to spend on building and sustaining relationships depends on USSOCOM's ability to address this need (see also Chapter IV about PN's management of commitment).

One of the main objectives of the GSN is to build trust among and between partners. The extent network members are able to freely seek and share information, and

---

[141] USSOCOM, ISOF Conference 2014: *Senior Leader Guide*, 12.

[142] Anklam, *Net Work*, 93, 97–98.

[143] The authors, imbued with NORSOF and SWESOF policies, assess the USSOCOM/GSN approach in regard to transparency as almost surprisingly inclusive and open.

[144] Anklam, *Net Work*, 98.

[145] Ibid., 99.

ideas and insight is one way to build trust.[146] The USSOCOM effort for improved information sharing to partners must be credited as an honest effort. Admiral McRaven, when he was Commander USSOCOM, constantly pushed his own organization as well as the intelligence community to improve information sharing within the network. However, USSOCOM seldom "owns" the information, making the information sharing challenging. Discussions with USSOCOM personnel confirm the situation: information sharing will be the most challenging piece to operationalize in the GSN concept.[147] However, beyond the scholarly view of network trust, there are other means for trust building in the military context that can somewhat mitigate the information issue: the conduct of combined operations as well as support with resources and/or combined training events. As, USSOCOM officials point out, the trust has been built within the SOF community throughout the last 13 years of combat and the GSN initiative should be seen as an action to specifically upholding this trust.[148]

Holohan also associates trust with the network culture and argues for a constant effort: "Trust … has to be continually produced on the ground."[149] This notion of a "local approach" to establish and maintain trust is acknowledged by USSOCOM:

> Networks are rooted in relationships. Building global relationships requires trust and, at its foundation, can only be achieved by persistently engaging and operating with the population of fragile, inherently unstable places, and those populations that appear stable.[150]

---

[146] Anklam, *Net Work*, 100.

[147] Louis Rachal (Deputy Current Ops (J-33), USSOCOM) in discussions with the authors during International SOF Conference, Tampa, Florida. May 19, 2014; Major General J.Timothy Leahy (Director of Operations (J 3), USSOCOM), in discussion with the authors during International SOF Conference, Tampa, Florida. May 19, 2014; Rear Admiral Robert D. Sharp (Director for Intelligence (J 2), USSOCOM) in discussions with the authors during International SOF Conference, Tampa, Florida. May 19, 2014; Major General Marshall B. Webb (Commander of Special Operations Command Europe (SOCEUR)) in discussions with the authors during International SOF Conference, Tampa, Florida. May 22, 2014.

[148] William J.A. Miller (Director, Strategy, Plans and Policy (J 5), USSOCOM) in discussions with the authors during International SOF Conference, Tampa, Florida. May 19, 2014.

[149] Holohan, *Networks of Democracy: Lessons from Kosovo for Afghanistan, Iraq, and Beyond*, 72. Holohan also relates trust directly to identification of mission, information transfer, and collaborative problem-solving capabilities. Leadership is vital in establishing these connections.

[150] USSOCOM, *Commanders Appreciation: The Strategic Environment*, 2.

(3) Interaction

The style of the network, and its capacity to achieve its purpose, is illustrated both through the type of interaction that dominates, and also through the member's ability to know which type of interaction to use at a given time. Anklam divides it into three types: transactional (task-typed), knowledge-based, and personal (relational) interactions.[151] The GSN seems to have a managed, distinguished, and relevant mix of transactional, relational, and knowledge-based interactions. Transactional interactions can be illustrated through the sharing of information for action during a crisis response. Relational interaction can be illustrated through interactions between PNs based on personal friendships. Knowledge-based interaction is illustrated through USSOCOM/J3-I regular "deep dives" into certain problem sets inviting various expertise and leaders from PN, interagency, and U.S. SOF to video teleconference (VTC) discussions.[152]

(4) Orientation

Outcome-focused network designs for production might have a somewhat hierarchical structure with more formal relations, while a discovery-and-learning network might have more of a mesh-like structure with more informal relations.[153] Our assessment is that the GSN balances the two approaches well, with an emphasis on the outcome orientation so that it becomes a viable option for the political leadership. However, in this early phase of development the main effort is to establish routines for dialogue and cooperation with partners, and in that regard few tensions or issues have been identified. As one of the USSOCOM leaders stated: "J3-I creates the opportunities to discuss."[154]

---

[151] Anklam, *Net Work*, 102–107.

[152] Brigadier Mark Smethurst, Australian Armed Forces (Deputy Director of Special Operations (J3-I), USSOCOM) in discussions with the authors during International SOF Conference, Tampa, Florida. May 20, 2014. See also USSOCOM, "ISCC Processes and Battle Rhythm," (Information Brief).

[153] Anklam, *Net Work*, 107.

[154] Smethurst, in discussions with the authors during International SOF Conference.

4. Placement on the Design Continuum

As a summary of the description of the GSN, we have used the network design continuum to visualize how the network functions.[155] As described in Chapter II, the overall design continuum spans the two extremes of Anarchy Network to Organized Network. The analysis has evaluated the GSN on the four dimensions: *unbounded-bounded membership, informal-formal interaction, heterarchical-hierarchical coordination, and shared-centralized governance*.

Unbounded-Bounded Membership is a dimension that describes how open or closed a network is towards external actors within its environment. The GSN is an open network, which encourages diverse nodes to join. Even though anyone can apply for membership, USSOCOM controls the decision to admit new members based on U.S. national interests and policies. The fact that there is no formal cost of joining the network supports the basis of it being an open network. Overall the GSN is placed on the left side of the scale on this metric.

Informal-Formal Interaction is a dimension that shows the level of formality within the network when its members interact. One of the important objectives of the GSN is to increase the informal interaction between the different nodes. Referring to the previous discussion regarding ties, governance, and leadership, one can argue that the GSN on the organizational level is relatively informal. Admiral McRaven seems to, from the authors' perspective, be aware of and put effort into continuous dialogue with network leaders. The social events planned and conducted during the ISOF conference suggest dedicated effort in this regard. On the other hand, because the network is based on military and government cultures we found formalities within the work processes, such as a structured and disciplined battle rhythm and bilateral agreement directing the sharing of information. Overall, we placed the GSN on the left-center on this dimension.

Heterarchical-Hierarchical Coordination is a dimension that shows how coordination among the nodes occurs. The GSN uses both heterarchical and hierarchical coordination based on the task performed. An example is APAN discussions versus

[155] Roberts, "Network Design Continuum."

classified information sharing over BICES. The military organizations within the network are by nature hierarchical; the same is also true for most of the other government organizations, so tasks are coordinated in a hierarchical fashion. On the other hand, one of the reasons for creating the network was to flatten the way members are coordinated. The informal relations among the partner nations suggest more heterarchical coordination. Overall we placed the GSN in the center of this dimension.

Shared-centralized governance is the dimension that describes who governs. The GSN has both shared and centralized governance, depending on the sub-network examined and the type of task performed. Within the U.S. SOF network, the governance is highly centralized around USSOCOM as the functional COCOM for U.S. SOF.[156] But, then again, an examination of the PN sub-network reveals governance that is highly shared, as well as decentralized decision making to the different nations. Overall the GSN is placed on the center-left on this metric.

Based on the positions of the four elements and making an overall judgment for the GSN on where it stands on the continuum between an Anarchic Network and an Organized Network, we have placed it slightly left of center. See Figure 14 for the visualization of the design continuum.

[156] Decision-making regarding U.S. SOF operations are centralized around the GCC and respective TSOC, while strategic level decisions, procurement, and development issues are centralized to USSOCOM.

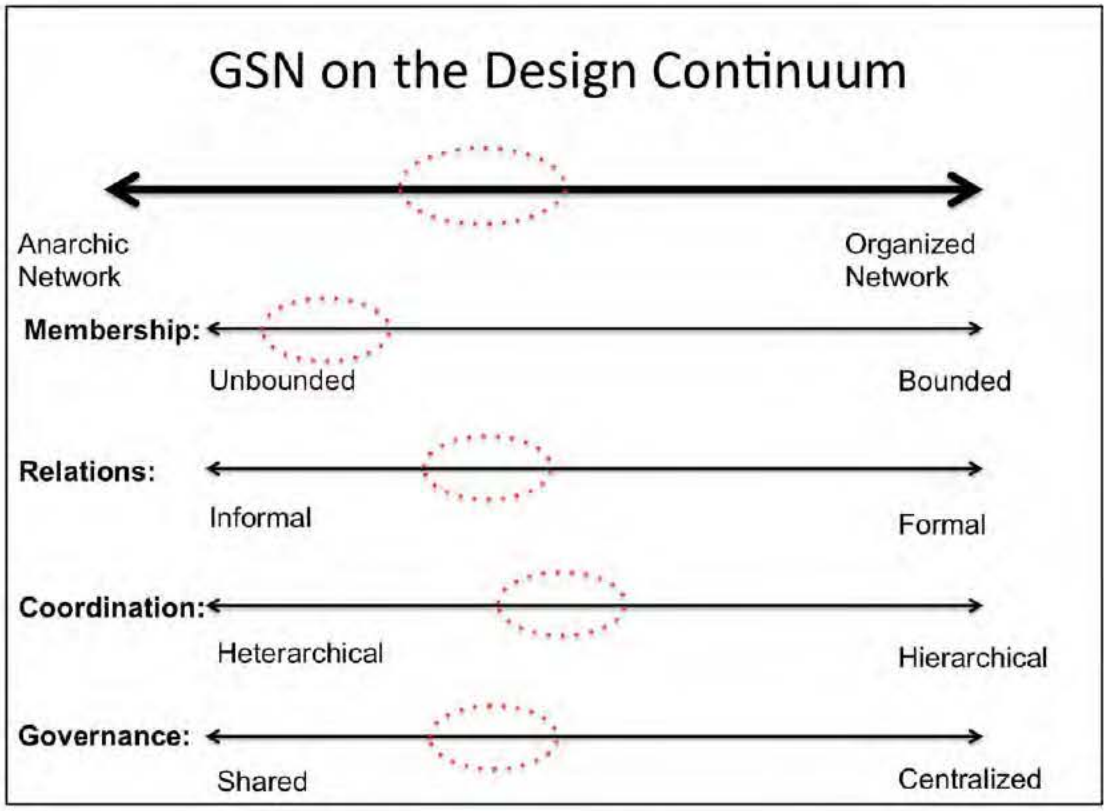

Figure 14. GSN placement on the design continuum.

B. ANALYSIS OF THE NETWORK

1. The Evolution of the Network

Members of the international SOF community have been engaging each other globally for decades, both in training and in active exchange of lessons learned. During the last decade in Afghanistan and Iraq, the cooperation and collaboration among different SOF units, and between the SOF community and the IA, have been at an extremely high level. This common experience was so important that the leadership within the U.S. SOF community saw a need to establish a method to continue this cooperation after Afghanistan and Iraq.

The idea of a GSN was born out of a need for continued cooperation and collaboration to address asymmetrical threats realizing that no single nation can meet the 21st environment alone in the coming fiscal reality. Starting in 2011, USSOCOM

introduced the GSN concept in the SOF vision for 2020. However, the evolution of the GSN has occurred mainly in the last two years.

Sustaining a network at its full capacity to accomplish its purpose and to produce value for its stakeholders is the result of intentional activities during its development and growth.[157] The GSN is still in its growth phase, and is in need of strong and persistent management to maintain the traction needed on the political level both within the United States and within the PNs.

The relationship between accountability and trust has been revealed through stakeholders' criticism of USSOCOM's GSN effort. Lawmakers have expressed concern about oversight and accountability in USSOCOM's ambitious and controversial network strategy. USSOCOM faces challenges with informing and convincing policymakers of support to this effort.[158] Although the official documentation shows that the GSN aims are clearly nested in the national defense strategies, this is not enough to avoid criticism for overreach.[159]

Some of the principal milestones within the GSN evolution are the IA cooperation, the PN cooperation, and the creation of the ICT portal and web 2.0. IA cooperation has evolved from none/sparse cooperation in the beginning of the Afghan and Iraq conflicts to robust cooperation with USSOCOM LOs in 20 different agencies and departments, and reciprocal IA LOs at USSOCOM. It is reasonable to assume that USSOCOM will have future expectations on PNs to improve their internal interagency efforts. PN cooperation has moved from a "Coalition village" outside of CENTCOM and USSOCOM supporting both headquarters with a mix of conventional and SOF LOs to an established ISCC within USSOCOM as a pure SOF LO entity, and further, to what is

---

[157] Anklam, *Net Work*, 63.

[158] Paul McLeary, "Lawmakers Skeptical of Global Spec Ops Plan." The U.S. House Armed Services Committee refused the USSOCOM 2014 request for $ 25 million for establishing a Washington office and Regional SOF Coordination Centers in Colombia and Hawaii. See also, Paul McLeary, "Special Ops Nominee Wants Review of SOCOM Initiatives," defensenews.com, October 11, 2013. http://www.defensenews.com/article/20131011/DEFREG02/310110015/Special-Ops-Nominee-Wants-Review-SOCOM-Initiatives.

[159] USSOCOM, *SOF 2020 Global SOF Network*, 5.

today: the J3-I Division as part of USSOCOM's J3 shop. Figure 15 shows the current PN cooperation within USSOCOM and where USSOCOM is planning to take this cooperation in the near- and long-term future.

Figure 15. J3-I/TSOC current and future PN representatives.[160]

Recently, USSOCOM is reaffirming that the TSOCs are the primary owners of PN SOF relationships within their respective Areas of Responsibilities (AOR), but that many PNs have cross-AOR capabilities and responsibilities. The decision whether a PN should have its LO at USSOCOM rather than at the TSOC is based on the PN SOF maturity, expeditionary capabilities, and responsibilities.[161]

The ICT portal and web 2.0 have moved from a simple face-to-face coordination interface to the common platform of APAN and BICES[162] that the network uses today. In addition to this, USSOCOM has created PN rooms for LOs to access their national systems for quick and secure reach-back to their national SOF headquarters.

[160] USSOCOM, "Operationalizing the Global SOF Network," (J3I-Brief).

[161] The topic of LO placement was discussed by several USSOCOM leaders in discussions with the authors during International SOF Conference.

[162] BICES-X is still under development and has currently not been distributed to the PNs.

Knowing that the GSN is still in its growth phase and looking at the progress over the last two years, it seems like USSOCOM has managed the network well as the network administrative organization, and has been able to acquire investment from the partners and the stakeholders. This administrative role will likely have to continue for some time into the future until more PNs are able to increase burden sharing and the network is able to self-organize among the members.

2. The Network "Fit"

a. The Network "Fit" with the Environment

To look at the "fit" between the GSN and the environment we will focus on two main environmental elements that will impact the GSN. First, the 21st century threat environment is fast moving, asymmetrical, complex, and networked with a high degree of instability. Second, the next decade will continue to face economic constraints, which will demand reductions within military forces and will shrink each nation's capacity for handling new challenges alone.

From the perspective of the design continuum, the GSN as a whole has a relatively good "fit" to the environment. On the continuum area of informal cooperation and shared governance, where the GSN is placed to the center-left, the network also shows a good "fit" with regard to the threat environment. By utilizing informal cooperation and shared governance, the network will have more flexibility and the ability to move information quicker within the network. Being aware that a military organization will never become a totally informal or decentralized entity, the GSN has found a good middle ground and focused on those tasks and processes that can be informal and decentralized.

The openness and unbounded membership make the network "fit" well in the fiscally restrained environment currently challenging all military forces. Growing the GSN into this global entity and focusing on utilizing each other's capacities while sharing the burden between the members fits perfectly to the projected economic environment.[163]

[163] To confirm this analysis would require "success stories" of measurable cost savings.

At the same time, the main purpose of the GSN is playing directly to the political ambition of holistic approaches that are cost effective with a low footprint while maintaining the option of persistent presence to support national interests in the future. Most of the national strategies espouse whole-of-government approaches, which the GSN is trying to develop.

The governing style of USSOCOM as the network administrative organization fits well with the development phase of the GSN. The main focus is to legitimize the GSN on the political level and at the same time start the development of a common picture to identify common interests. To accomplish this effort, the network has to have an entity like USSOCOM that facilitates and synchronizes these processes and keeps the different PNs accountable for their contribution.

In summary, the GSN appears to be a good "fit" with the current environment but will have to continuously monitor the environment to be able to evolve to address gaps that may emerge.

b. The "Fit" among Design Elements.

The analysis of "fit" among Design Elements uses Roberts' grouping of design factors: *tasks, technology, structure, people, and processes.*[164] See Figure 6 in Chapter II. The factor of leadership will be added to the analysis.

The processes include communication, information management, planning, and decision making as well as the aforementioned interactions. The processes together with GMSC and the J3-I's basic tasks, as described earlier, have been developed according to the network structure. The structure includes the USSOCOM's hierarchical structure, the mesh-like structure of the J3-I internal apparatus, and the hub-and-spoke structure of the USSOCOM's relations out to the PNs and interagency. Further, the supporting technology, APAN websites and BICES, is adapted to the tasks and processes requirements for both an open communications means for collaborative learning, and the

[164] Roberts, "Organizational Systems Framework."

need for classified information sharing.[165] The leadership function is adapted to the structure of the various sub-networks. SOF, with its unique culture (people), makes the flattening of the network possible: one SOF leader describes this as using "SOF maturity and honesty."[166] Overall, the synch among the design factors gives the impression to have been thought through by the GSN designers. The network appears to have a relatively good internal fit between its elements.

3. Network Design Tensions

There are five major design tensions identified. They are: *information sharing*, *cultural differences*, *burden sharing*, the *identification of common interests*, and *accountability*.

Information sharing. There is a great awareness within USSOCOM about the inherent challenges of sharing classified information, and great deal of effort has been focused on improvements in this area. The ongoing effort to distribute BICES-X is one example. Another example is to change the narrative: It is easier to share information than intelligence.[167] However, in most cases, USSOCOM and PN SOF must fall back on intelligence sharing agreements between countries[168] and the goodwill of intelligence agencies. If these agencies do not have incentives to share, why should they? One way to counter the argument of over-sharing is establishing specific PN groups in pre-operation planning phases where information can be more easily shared.[169] But the assertion remains: the most important trust-building tool is restricted. Regardless of significant improvements, tensions in this field will be evident in the foreseeable future.

---

[165] The various sub-networks have different ties, which implies relationships that vary from a need for "simple" information sharing to problem-solving collaboration.

[166] The U.S. SOF sub-network with USSOCOM is the lead organization and the PN network is a self-governing network. The SOF personnel described in Style/ Culture category earlier, holds a unique culture. This is also visible in SOF truth # 1: Humans are more important than hardware. The quote is from Smethurst, in discussions with the authors during International SOF Conference.

[167] Rosengard, in discussions with the authors during International SOF Conference.

[168] These are often bilateral agreements between specific intelligence agencies, which complicate the GSN vision of enhanced information sharing.

[169] The BICES-X supports this kind of selected distribution of information.

Cultural differences. Tensions attributed to cultural differences between nodes in the network will certainly be an everyday issue. Perhaps the most obvious is the general differences between military and civilian organizations. Cultural differences between the SOF and the intelligence community are not exclusively a U.S. issue. SOFs also need access and high-resolution intelligence. The intelligence services prioritize among requirements and customers, and resist revealing information without exchange. Other issues are the different security cultures of the PNs. Some nations are relative open, and others are more closed when it comes to information about their SOF and activities. For example, looking at the United States, which has one relatively open side, called white SOF and one closed side, called black SOF, we find a different culture than that of a PN which has only one of these types.[170]

Burden Sharing. Internal accountability is a potential design tension. USSOCOM desires future burden sharing, noting, "As we build the network we will require partners to share the burden."[171] This PN involvement can take many forms and there is a notable awareness among the GSN architects that PNs have different capabilities and capacities to contribute which may shift over time pending national interests. The logic that "give and share" or "participate and provide" might pay benefits is obvious. However, how should partners who do not seem to contribute be managed? Free-riders can negatively impact the openness and trust within the network (see also Chapter IV under "Management of Accountability").

Common Interests. The process of identifying common interest among PNs seems to be a wise idea to generate output and share burden in a complex multinational context challenged with information-sharing issues. However, there may be difficulties for PNs in defining useable strategic inputs in the process in the first place. For example, a small nation does not have the same global interest as the United States. Further, what tensions

[170] Harvey Sapolsky, Benjamin Friedman, and Brendan Green, eds. *U.S. Military Innovation Since the Cold War: Creation Without Destruction* (New York: Routledge, 2009). White SOF are units whose existence are openly acknowledged by the U.S. government even if their operations are almost always classified and clandestine, for example, the U.S. Army Special Forces community. Black SOF are units (often referred to as Special Mission Units or SMUs) whose existence is not acknowledged and whose operations are not only always classified/clandestine, but often covert.

[171] USSOCOM, *Commanders Appreciation: The Strategic Environment*, 3.

and trust-reducing effects can follow if some of the PNs, including the United States, have contrary interests on a matter revealed during the process? Also, how are "national interests" defined? Are these actual national interests, or should these be defined as interests that PNs' SOF want and can influence?

Accountability. The GSN concept touches, sometimes to a high degree, the field of foreign policy. How is the trust and "top cover" for the GSN established at the policy level? Don Tapscott and Anthony Williams point to the challenges when "multistakeholder" networks claim larger roles treading on responsibility at the political/policy level.[172] The policy level might perceive this enterprising, fast moving, cost driving, multinational network as somewhat out of its political control. Also, stakeholders may question the benefits. USSOCOM and some of the PN SOF leaders need to establish their legitimacy and accountability to the political masters: normal chain of command and national deployment procedures will not be changed (see also Chapter IV for more discussions about management of accountability and legitimacy). At the same time, the idea of sharing the costs and burdens to meet future threats is fiscally attractive to policy makers. In summary, Even though USSOCOM seems to be open and transparent in its messaging about the GSN, USSOCOM still has challenges reaching the target audiences.

4. Networks´ Overall Strength and Weaknesses

The GSN sub-networks create a multi-layer structure, which enables more global connections and therefore increases the density. The way the network communicates (pace of communication and interaction) supports a fast and robust network. However, the increased numbers of connections indicate something that might be seen as a weakness, or at least a risk: in spite of battle rhythms and information management procedures, there is an apparent risk of bypassing (by mistake) a node in the intense communication. This is particularly challenging for the military hierarchical structure within the network.

---

[172] Don Tapscott and Anthony D Williams, *Makrowikonomics: New Solutions for a Connected Planet* (New York: Portfolio/Penguin, 2012), 316–319.

The texture reveals that the distances—the short "degrees of separation"—in the network support rapid response to external conditions as well as rapid distribution of information. The centralized position of USSOCOM in the network paired with the mesh-like structure within the J3-I, supports a common picture in the overall network: detailed situational awareness in the central hub can easily be distributed to peripheral nodes. In other words, it allows PN governments a new and "direct" source for situational awareness.

For the PNs with LO presence in USSOCOM, the mesh-like structure of J3-I allows for day-to-day discussions and cooperation on concerns other than operational: identification of opportunities for training, procurement of hardware, and R&D projects can result in fruitful and cost-effective cooperation and collaboration.

One possible weakness might be the establishment of PN LOs at HQ USSOCOM in Tampa, on the behalf of LOs at the regional hubs, the TSOCs.[173] PNs with internal security concerns and with no ambition to deploy SOF abroad might have better use of an LO at the regional hub (TSOC) and not USSOCOM.

Another possible weakness in the GSN effort is the fact that USSOCOM focuses on the TSOCs as "central of gravities," while the PNs focus on USSOCOM. This is a potential friction mostly illuminated in operational contexts that has to be considered both by USSOCOM and the PNs.

5. Performance of the Network

An important element highlighted by Kenis and Provan is how to choose criteria for network performance. They believe that one should consider criteria only when a network has the ability to actually influence the criteria.[174] As described in Chapter II, Kenis and Provan establish three exogenous performance factors that impact the choice

[173] A few of the resource-rich PNs also have LOs at the TSOCs. However, many PNs might have to prioritize their resources on one location. A weakness that USSOCOM is aware of, and are looking at different solutions. The topic of LO placement was discussed by several USSOCOM leaders in discussions with the authors during International SOF Conference.

[174] Kenis and Provan, "Towards an Exogenous Theory of Public Network Performance." 444–449

of criteria: The form of the network; whether the network is mandatory or voluntary; and the developmental stage of the network.

The Network Form. Currently, USSOCOM is assessed as having the governance role as the network administrative organization. The command is currently focusing on synchronization of information to be able to develop the common picture within the network, and at the same time facilitating the growth of the network by creating the space, place, and pace for the members to interact and cooperate. Being a network of both U.S. organizations and PN organizations, this structure is probably the most appropriate for the GSN. At least for now in the growth phase, the network needs an administrative organization that can tie the different members together and take the initial burden of being the network administrator. USSOCOM is the only organization with the resources and ability to take on this responsibility today. This may change in the future when the network is more mature and has started its performance phase.

Mandatory versus Voluntary. GSN is assessed to be a voluntary network and based on the following three criteria, appears to be operating well as a voluntary network: *network legitimacy, activating capacity*, and *network climate*.[175] The aspect of network legitimacy is one of the most demanding tasks for USSOCOM, and is a focal point when dealing with the political leadership within the United States. The focus on partnerships and networking in the Quadrennial Defense Review 2014[176](QDR) and the approval of the Global Campaign Plan-Special Operations confirms the GSN legitimacy. Additionally, each PN will have to create this legitimacy within their political leadership. The manner in which USSOCOM has included the IA and PNs has resulted in a strong and positive network climate, which is absolutely crucial at this stage of the network evolution. The establishment of the J3-I with the PN LOs and the IA LOs within

[175] Kenis and Provan, "Towards an Exogenous Theory of Public Network Performance," 449–450. These are the three outcome-criteria that Van Raaij deemed to be appropriate for a voluntary network such as the GSN.

[176] Department of Defense, *Qudrennial Defense Review 2014*, Washington, DC: Department of Defense, 2014.

USSOCOM has created the processes and the ability to have the activating capacity within the network.[177]

The Development Stage. The GSN, still in its growth phase, should not yet be measured according to goal attainment. In this phase, most of the time and energy of USSOCOM's J3-I and its members is expended developing the network structure and processes, rather than on achieving the network purpose outcomes.

Based on USSOCOM´s network governance, its type, and its development stage, the following metrics can be used to measure GSN output and outcomes in its current growth phase:[178]

- Output metrics:
  - # of member nations/organizations in the network (see Figure 15)
  - # of times GSN is mentioned in political/strategic documents (to measure the level of legitimacy)
  - # of participating member organizations and nations in the various network activities
  - ICT development (# of BICES distributed; # of APAN accounts created)
- Outcome metrics:
  - Level of IA cooperation and integration
  - Level of PN cooperation and integration
  - Extend to which a common picture of PNs interests and intentions (and possibly objectives) are developed and distributed within the network
  - Extend to which the GSN becomes an instrument of choice for problem solving (legitimization)

Based on the analysis of the GSN and the fact that it is still in its growth phase the network seems to perform well. The main metric during a growth phase of a network is to attract new members, which the current and future appointments of LOs at USSOCOM J3-I indicate is happening (See Figure 15). The GSN have faced some challenges with regards to stakeholder buy-in from the political and military leadership during its early phases of development. However, both the 2014 QDR and the signing of the Global

[177] The value of USSOCOM's IA LOs for PNs may rise should the PNs establish national IA nodes within their national network.

[178] In the future, other metrics could include: information developed and provided that influences decision making; generated alternatives solutions presented to commanders; and burden sharing examples.

Campaign Plan-Special Operations indicate that stakeholders are now supporting the initiative and that the GSN is becoming legitimate.

C. SUMMARY OF THE ANALYSIS

The GSN is a network of organizations with multiple sub-networks that are physically dispersed, creating a global and multilayered structure. The network is built upon the framework of the U.S. SOF organization and technology, which support bonding and the ability to communicate. The unique personal relationships and experience of SOF personnel from years of warfighting is a vehicle to realize this effort. Trust is to a certain degree already established within the SOF community—the challenge is to maintain and spread this trust further within the IA and the political community.

The initiative to establish a GSN fits well with the U.S. strategic directives as well as to address foreseeable threats. The purposes of the GSN are logical and should appeal to all the stakeholders. As noted during this research, there is a constant challenge with the GSN in reaching out with strategic messaging. Those not directly involved in the GSN effort suffer greatly from knowledge gaps on its status and intent.

The internal design elements also have a good fit. GSN architects/designers have done their homework. From a network perspective, most considerations seem to have been addressed throughout the development of the GSN concept. Nonetheless, it is an ambitious effort with considerable challenges. In many cases, future outputs and outcomes require policy-level decisions, especially for the participating PNs. In the short term this means that the information campaign is far from over. The main effort should be to inform the political and military policy level of the GSN effort.

Based on the theoretical framework from Chapter II and the understanding of the overall Global SOF Network from this chapter, the next chapter will focus on the challenges for NORSOCOM and SWESOCOM as both Managers in Networks (a node in the overall GSN), and as Managers of Networks (within the national SOF network), as shown in Figure 16.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CHALLENGES FOR NORSOCOM AND SWESOCOM AS MANAGERS IN THE GSN, AND MANAGERS OF NATIONAL SOF NETWORKS

Chapter III analyzed the overall GSN, identifying the primary challenges for USSOCOM as the manager, initiator, and facilitator of the global network (see #1, in Figure 16). This chapter examines the PNs' SOCOM (or the equivalent) perspective as member organizations in the GSN. More specifically, the focus is on the Norwegian and Swedish SOCOMs.

For NORSOCOM and SWESOCOM to benefit and contribute as member organizations in the GSN, they need to understand Milward and Provan's concept of the *Management in Networks.* There are certain management requirements for organizations that are members of a network to make sure the organization contributes and works toward the overall network purpose (see Table 2 in Chapter II, and Figure 16). NORSOCOM and SWESOCOM have taken active measures to join the GSN, but what else might be needed if the ambition is to be long-lasting active members?

Second, if NORSOCOM and SWESOCOM want to strengthen, or establish, their own in-country network, they need to understand Milward and Provan's concept of the *Management of Networks.* There are certain management requirements for organizations that have the responsibility to lead a network as a whole, to make sure the member organizations contribute and work toward the overall network purpose (see Table 2 in Chapter II, and Figure 16).

To address the Management in Networks and the Management of Networks concepts, the chapter is divided into two parts. The first part focuses on how NORSOCOM and SWESOCOM, as organizations in a network (see #2, in Figure 16), can manage their GSN membership to enhance its contribution to the network as a whole. The second part focuses on how NORSOCOM and SWESOCOM can bridge out from the GSN and formalize their national partnerships into a "National SOF Network" (see

#3, in Figure 16).[179] These two perspectives are separate and at the same time interrelated, and should be conducted in parallel to encourage the continuous co-evolution of both types of networks.

The diagram in Figure 16 illustrates the difference between Management of Networks, which is management of the whole, and Management in Networks, which is managing one's organizational involvement in the network.

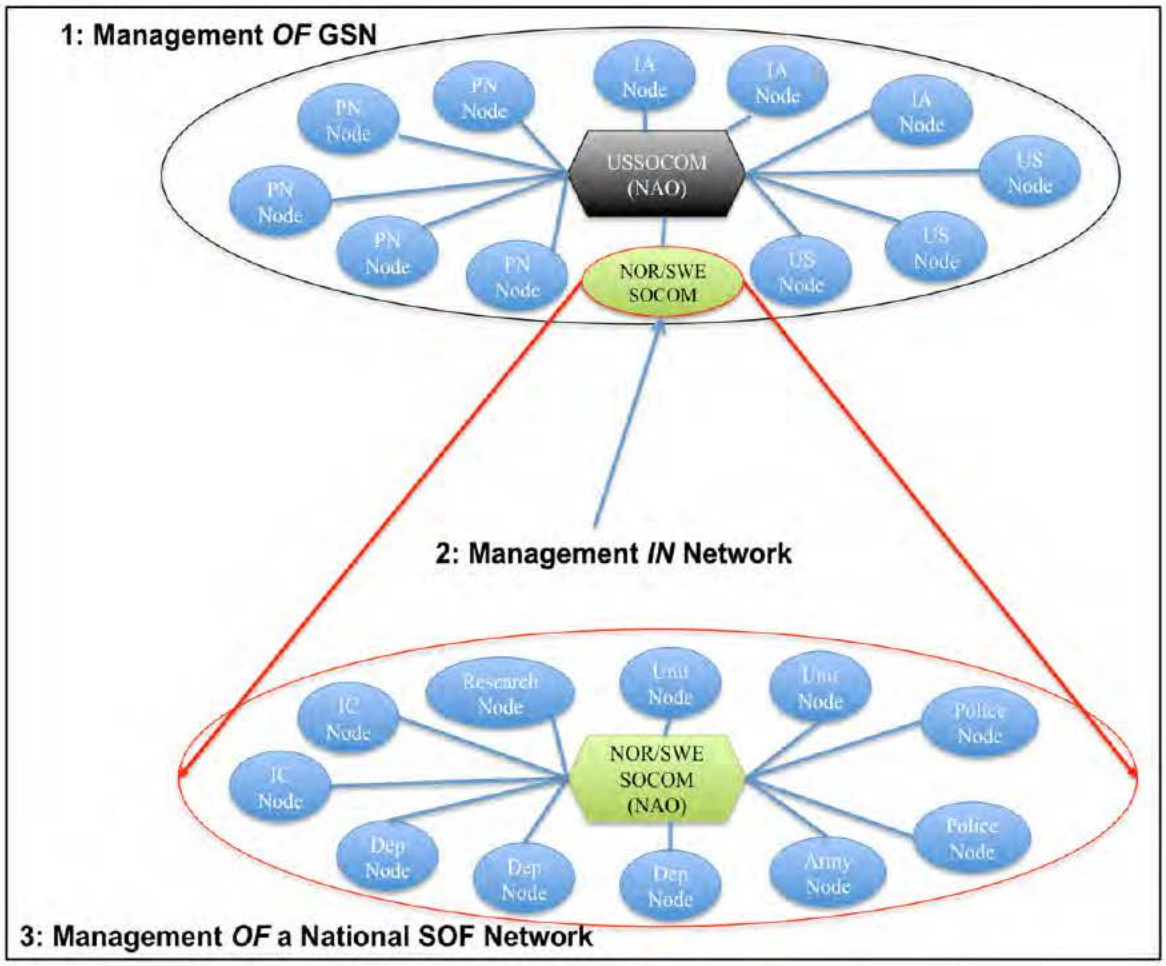

Figure 16. Management in networks vs. management of Networks.

[179] The actual naming of the network may be tied to the main purpose of a developing network. This research uses the term national SOF network. One reason for this term is the natural legitimacy of NORSOCOM and SWESOCOM if initiating and taking the leadership role in this kind of national network effort.

There are myriad challenges that can be identified related to membership in an evolving global network as well establishing and leading one's national network. We have identified what we consider the main challenges for initial action for NORSOCOM and SWESOCOM following GSN membership.[180]

For NORSOCOM and SWESOCOM as *managers in the GSN*, we have identified eight challenges that should be addressed. These are: preventing perception of being a free-rider; maintaining recognition and visibility in a growing network; understanding the value of participation; establishing internal information sharing routines; building legitimacy towards other network members; working effectively with the network level manager; building commitment to the GSN overall objectives; and committing only one individual to network activities. These challenges and suggested counter actions are described in the first part.

For NORSOCOM and SWESOCOM as *managers of their national networks*, we have identified ten challenges that should be addressed. These are: handling free-riders; bringing members onboard; getting members to behave as network members; seeing the network effort as worthwhile; handling internal frictions due to added workload; addressing stove-piping and "turf" issues; managing perception of formal leadership; uniting members toward a common purpose; understanding the value of contribution; and upholding member commitment over time. These challenges and suggested counter actions are described in the second part.

The challenges identified are addressed through Milward and Provan's five dimensions of management tasks (accountability, legitimacy, conflict, governance, and commitment). Table 4 summarizes suggested actions to address the different challenges, which are divided into the five dimensions of Milward and Provan.

[180] The suggested actions are based on the authors' understanding about the national SOF contexts in Sweden and Norway as well as on discussions with USSOCOM leaders, Norwegian and Swedish SOCOM commanders, and their respective national Liaison Officers at USSOCOM.

Table 4. Suggested management actions to counter initial challenges.

	Challenges to Management in Network Tasks (Management of GSN membership)					Challenges to Management of Network Tasks (Managing a National Network)				
Actions to counter challenges	Accountability	Legitimacy	Conflict	Governance	Commitment	Accountability	Legitimacy	Conflict	Governance	Commitment
Establish Management Function	(X)			X	X	(X)	(X)		X	X
Conduct Information Campaign	(X)	X			X	(X)	X	(X)		X
Strengthen Communication Infrastructure	(X)			X			X			X
Participate in information sharing		X					X			X
Disciplined Information management	X			X			(X)		(X)	(X)
Active dialog with LO	X						(X)	(X)		(X)
Formalize Network commitment					X	(X)		(X)		X
Contribute to Burden Sharing	X	X			(X)					
Build support from the I.C.		X			(X)				(X)	
Active dialog with policy level					X					
Address contribution expectations						X				(X)
Build support from the policy level					X		X			X
Leverage existing collaboration fora		X					X		X	
Participate in regular network activities		(X)			X		X	X		
Share of resources										X
Define Network Purpose							X		(X)	
Informal Leadership: Facilitator/Host		(X)							X	
Maintain personal relationships			(X)					X		X

X = Direct relationship between actions and management challenges described in Chapter IV.
(X) = The action has an indirect effect or is not directly described in relation to the specific management tasks in Chapter IV.

A. CHALLENGES FOR NORSOCOM AND SWESOCOM AS MANAGERS IN THE GLOBAL SOF NETWORK

How can NORSOCOM and SWESOCOM manage their GSN membership? The framework for recommendations is Milward and Provan's concept of Management in Networks, described in Chapter II (see Table 2 in Chapter II), where the Essential Network Management Tasks are divided into five categories: *Management of Accountability; Management of Legitimacy; Management of Conflict; Management of Governance; and Management of Commitment.*[181]

1. How Can NORSOCOM and SWESOCOM Manage their *Accountability* within the GSN?

Accountability is two-sided and entails both willingness to take responsibility for one's action and an expectation that actions will be recognized. Accordingly, managers *in* networks have to make sure that their organization contributes to the overall network by setting aside specific resources to support network specific activities.[182]

A potential accountability challenge for NORSOCOM and SWESOCOM is to avoid being perceived as a "free-rider." Another challenge is to be recognized and visible in a growing network with many members (PNs).[183] We suggest three initial actions to mitigate these accountability challenges.

a. Participate in the GSN "Dialogue" through Disciplined Information Management

At a minimum, a main effort should be to pass and receive information and participate in the GSN "dialogue."[184] Even if it is of interest for various staff sections to

[181] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 18–24. USSOCOM has, according to this theory, the responsibility of Management of Networks, while organizations as member nodes have the challenge of Management in Networks.

[182] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 18–19.

[183] The growing number of LOs at USSOCOM J3-I may make it more difficult for individual partner nations to get recognition for their contributions. See Figure 15. Further, discussions with LOs at USSOCOM have hinted at difficulties to contribute with defined "national interests" into the J3-I process to identify common interests among partner nations.

[184] Advice given to the authors by Admiral McRaven, Commander USSOCOM, in discussions with the authors via APAN VTC, July 8, 2014.

communicate and participate in forums/working groups freely, a structured responsibility and rhythm for communication is suggested.[185] The main reason is, for example, to keep track of requests, questions to be answered, and information that has been shared. This should be done to ensure dissemination of information, to avoid the unintentional by-passing of the chains of command,[186] to keep track of the responsiveness of own national SOF staff, and to keep track of how much staff effort goes into fulfilling the GSN objectives versus how much time the staff spends in fulfilling own organization's needs and requirements.

b. Make "Burden Sharing" More Visible

NORSOCOM and SWESOCOM's current dedicated resource for GSN activities is primarily their respective LOs at USSOCOM J3-I. These LOs are the means by which NORSOCOM and SWESOCOM ensure that their GSN involvement and various contributions to the GSN effort are visible and recognized within the USSOCOM "enterprise," at other PNs SOCOMs, as well as at J3-I.

NORSOCOM and SWESOCOM should consider making national efforts like their operations, regional SOF cooperation, assistance and training of partners, R&D, or combined procurement projects that can be seen as "burden sharing" visible and known within the GSN.

NORSOCOM and SWESOCOM may need guidance in their efforts to aim for network objectives and burden sharing for the whole network. A comparative analysis between NORSOCOM and SWESOCOM's interests in relation to GSN's interests may identify burden-sharing possibilities for NORSOCOM and SWESOCOM that match their own interests. The purpose should be to identify both common interests and divergent interests.

---

[185] USSOCOM shares this philosophy: The Command emphasizes dialogue and information sharing while having disciplined battle rhythm, for example, scheduled timings for recurrent VTCs, etc. Admiral McRaven, Commander USSOCOM, in discussions with the authors via APAN VTC, July 8, 2014.

[186] Network communication, for example: Commander USSOCOM's direct dialogue with PNs' LO at J3-I may keep the relevant TSOC "out of the loop" or "bypassed." Major General Marshall B. Webb, Commander of Special Operations Command Europe [SOCEUR], gave this example in discussions with the authors during International SOF Conference, Tampa, Florida. May 22, 2014.

c. Dialogue with LO at USSOCOM about Contribution Perception

Most importantly, routine checks via dialogue with the LO about the perception of the nation's contribution to the network is important to avoid the label of "free rider." Awareness among SWESOCOM and NORSOCOM leaders and staff about this important issue should underscore the need for regular participation with inputs to the GSN effort.

2. How Can NORSOCOM and SWESOCOM Manage their *Legitimacy* within the GSN?

Legitimacy is based on external reputation and social acceptance. It is often used as an alternative indicator of effectiveness and success. Managers of organizations *in* networks must establish the legitimacy of their own organization as a viable network player, while balancing legitimacy needs as an autonomous entity. It is relatively easy to lose autonomy and recognition as a member of a network with more than 20 members.[187]

Legitimizing NORSOCOM and SWESOCOM GSN participation among other network members is to a degree achieved through current SOF cooperation in the European context: bilateral training arrangements between SOF partners, among NATO SOF, EU framework, and other regional cooperation, etc. However, GSN participation may require additional efforts on the global and strategic level to uphold reputation and acceptance.

The main legitimacy challenges for NORSOCOM and SWESOCOM may be to get national stakeholders to understand the value of NORSOCOM and SWESOCOM participation in the GSN. In this regard, NORSOCOM and SWESOCOM may face challenges to establish national information/intelligence sharing through "SOF-channels" to the GSN. NORSOCOM and SWESOCOM may also have challenges to prove their legitimacy towards other more active and resourceful GSN members.[188]

This research suggests four actions to meet these three legitimacy challenges:

---

[187] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 20–21.

[188] Legitimacy issues among other PNs may rise should NORSOCOM and SWESOCOM be perceived as not contributing to the GSN processes.

a. Establish a National Information Campaign

NORSOCOM and SWESOCOM initially need to establish a basic understanding about the GSN effort among national stakeholders.[189] This point cannot be overstated. The research has identified areas of misunderstanding, misinterpretation, and lack of knowledge about the GSN effort, even within the international and U.S. SOF community. One theme has been the over-emphasizing of a single aspect of the GSN idea coupled with a lack of insight into the overall GSN concept and development.[190] It would appear an initial national information campaign is needed for national stakeholders to focus on a thorough understanding of the GSN effort.

Beyond the initial buy-in from stakeholders, NORSOCOM and SWESOCOM probably need to put emphasis on showing stakeholders the value of participating, both from a national SOCOM perspective and their stakeholder perspective.

b. Ensure Visibility of Operational Burden Sharing

The deployment of national SOF for international operations including cooperation and sharing of information and lessons learned among GSN members might be the most effective means to establish recognition within the GSN. Norwegian and Swedish SOCOMs could consider making their own SOF operations more visible within the GSN forums. More specifically, they could put effort into specific reporting and information sharing to the GSN audience during and after operations.

GSN can provide a new forum for preventive security cooperation. For example, the J3-I ambition to develop and suggest multinational solutions on problems, including preventive efforts, should interest Norwegian and Swedish policy makers. In cases of EU or NATO non-consensus situations, the GSN can be seen as an alternative forum to generate an ad hoc coalition for crisis response or long-term preventive missions.

[189] NORSOCOM and SWESOCOM's stakeholders related to the GSN are here defined as national actors that might be affected by the GSN membership. The main stakeholders include the military leadership at the operational and strategic level, SOF tactical units, intelligence community, law enforcement, the Ministry of Defense, and Ministry of Foreign Affairs.

[190] Class discussions about the GSN during the Network Design course at Naval Postgraduate School, 2014.

Pending national will, this can be seen as both opportunities for "burden sharing" and as opportunities for the relatively small nations of Norway and Sweden to perform role model missions for obtaining credibility beyond their contribution. One example would be committing NORSOF or SWESOF to a long-term and focused capacity building effort toward a host nation in need of support. Such a mission could include a national comprehensive effort combining and coordinating military means (SOF trainers and advisors),[191] diplomacy, law enforcement (trainers and advisors), and national aid into a focused whole-of-government approach.[192]

c. Promote Information Sharing within the GSN

NORSOCOM and SWESOCOM could enhance their legitimacy by identifying national information that could be seen as value-added if shared in a wider group of partners/nations. NORSOCOM and SWESOCOM could identify issues of interest to the GSN as well as of interest to their own organizations. An example could be R&D and procurement projects that are shared with other PNs. This may provide an opportunity to take on a leadership role on specific projects, hence enhancing NORSOCOM and SWESOCOM's legitimacy among PNs.

Sharing of sensitive information and intelligence is a challenging issue within the GSN.[193] It should not hinder NORSOCOM and SWESOCOM's ambitions. On the contrary, the outspoken USSOCOM awareness of the challenges hints at legitimacy benefits should NORSOCOM and SWESOCOM successfully establish sharing routines

---

[191] In military terms these kinds of SOF Training and Assistance missions are often described at the operational level as "shaping the environment" or "Phase Zero Operations." NATO SOF nomenclature defines these missions as Military Assistance (MA).

[192] This option resonates with the national security strategies of Norway and Sweden, which seek to develop comprehensive, flexible, and proactive approaches to crisis management. The strategies acknowledge the veto-challenges in the UN and the consensus requirements in NATO and EU. However, the strategies do not elaborate on possible new approaches for security cooperation outside the framework of the alliances. Regjeringskansliet, Forsvarsdepartementet. [Ministry of Defense] "Veivalg i en globalisert verden." [Choices in a globalized world] Stockholm, 2013; Regeringskansliet [Swedish Government], En strategi för Sveriges säkerhet [A Strategy for Swedish Security], Ds 2006:1.

[193] Admiral McRaven acknowledges information sharing to be the most challenging issue among PNs. He strives to make USSOCOM a model for information sharing: rather share too much information than to little, or as he summarized the reasoning, advocating "aggressive information sharing." See also Chapter III for how USSOCOM leaders have specified information/intelligence sharing as the main challenge for the GSN.

toward the GSN with their national intelligence community. In other words, even seemingly small amounts of information shared can enhance NORSOCOM and SWESOCOM legitimacy within the GSN.

d. Build Intelligence Community Support

NORSOCOM and SWESOCOM need to establish support from their national intelligence agencies to enable occasional sharing with the GSN forum. Norwegian and Swedish intelligence agencies could be tasked to support their respective SOF HQs GSN membership efforts.[194] This would require Norwegian and Swedish SOF commanders informing and encouraging decision makers in this direction. The intelligence community support would enable information sharing to the GSN, which in turn enhances NORSOCOM and SWESOCOM legitimacy in the eyes of other PNs.

At a minimum, NORSOCOM and SWESOCOM will need to be well linked into their national intelligence agencies in order to follow up on information and intelligence that typically is not released through SOF channels.[195] Thus, NORSOCOM and SWESOCOM will need to update PNs' LOs at USSOCOM when their respective intelligence services have received SOF-related Norwegian or Swedish intelligence through bilateral intelligence-sharing agreements/channels.[196]

3. How Can NORSOCOM and SWESOCOM Manage *Conflicts* within the GSN?

Conflict among network participants is inevitable. On an overall network level, examples of potential conflict areas can be: free-riding, intelligence sharing, partner

[194] Such a supporting effort can naturally be restricted to occasional sharing within the framework of a specific "Community of Interest." One example to facilitate sharing is USSOCOM J3-I's procedures that enable selected information sharing among interested nations on specific issues. Depending on issue, ad hoc-groups of nations can establish "working groups" where information is shared with involved and "trusted" partners. A working group of nations is also called a "Community of Interest." This kind of intelligence agency support could also be seen as a driver to improve connectivity within the GSN through the use of BICES.

[195] Advice given to the authors by Rear Admiral Robert D. Sharp, Director for Intelligence [J2], USSOCOM, during International SOF Conference, Tampa, Florida. May 19, 2014.

[196] The intention is to make partners aware of valuable information sharing through intelligence channels, while acknowledging the already existing intelligence cooperation agreements.

nations not contributing with inputs regarding national interests and lack of contribution to build the common picture, "turf" issues between members, and issues related to political oversight.

Networks are comprised of multiple members with different organizational objectives, stakeholder preferences, procedures, and cultures. Network-level managers need to minimize incidents of conflict. Although it can contribute to creative solutions, frequent conflict can undermine trust building. Managers in networks have an important role in supporting the overall network manager and work as a "linch pin" in trying to address these issues among the member nations and organizations. They have a responsibility to cooperate to ensure that problems and conflicts are resolved before intervention by the overall network manager.[197]

The research has not identified any specific challenge for Commander NORSOCOM or Commander SWESOCOM to negotiate conflicts with other PNs. Consequently, there are no specific actions recommended.

However, are the various commanders´ conferences and the biennial ISOF conference enough to enable the national SOF commanders to establish personal knowledge of one another and a sufficient degree of trust and informality? If Norwegian and Swedish SOF Commanders feel improvements are needed, reaching out to establish informal communication among SOF leaders is entirely in line with the GSN philosophy.

4. How Can NORSOCOM and SWESOCOM Manage their *Governance* within the GSN?

Chapter III assessed the GSN to be appropriately governed by USSOCOM as a network administrative organization (NAO).[198] In this kind of structure, managers of the organizations in the network have a responsibility to work closely with the network-level manager. This means accepting that the network-level leader makes decisions for the whole network that may not necessarily be in the best interest of individual network

[197] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 21.

[198] See Chapter III, Analyzing the Global SOF Network, B. Analysis of the Network, 5. Performance of the Network.

members. The perceived loss of control can be difficult, but it is necessary for the sustainment and effectiveness of the network as a whole in accomplishing its goals.[199]

Milward and Provan's notion of loss of control to the lead administrator (USSOCOM) is assessed to be of less concern for Norway and Sweden as GSN members. Instead USSOCOM, as the leader/manager (NAO, coordinator, facilitator) of the voluntary non-obligation network for information sharing and identifying common interests among members, should be seen as providing opportunities for the members to exploit if militarily feasible and politically appropriate.[200]

The main governance challenge identified for NORSOCOM and SWESOCOM is for them to be able to work effectively towards the network level management (USSOCOM J3-I).[201] The project suggests three initial actions to meet this governance challenge:

a. Designate a GSN Network Manager Function: A Reach-Back Capacity for the LO

The Norwegian and Swedish LOs at USSOCOM J3-I facilitate NORSOCOM and SWESOCOM's ambition to work closely with the network managers at USSOCOM. However, to improve the interaction with the central hub in the GSN, the national SOCOMs might consider a designated reach-back capacity—a Network Manager—for the GSN membership at their HQ.

The management responsibility within the HQs of NORSOCOM and SWESOCOM for GSN engagements could be appointed to a section or individuals in line with the concept of Management in Networks. For example, a "Network Officer" may be appointed capable of advising the Commander NORSOCOM and Commander

---

[199] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 21.

[200] In other words, the GSN cannot make decisions: USSOCOM J3-International is facilitating PNs' identifying common interests, suggesting multinational preventive solutions, and establishing "coalitions of the willing," based on national decision making on different issues. Further, J3-I supports various Commanders (USSOCOM, TSOC, Partner Nation SOF) with multinational perspectives and options.

[201] Potential issues related to respond to/communicate with the LO/J3-I at USSOCOM could include: J3-I expectations of inputs from PNs' policy level regarding national interests, great variety of topics, and infrequent communication.

SWESOCOM of GSN matters, supporting and directing and the LO at USSOCOM, and have the seniority to liaise with national agencies and departments.[202]

An additional objective in establishing a network manager for the GSN membership is to make the national LO at USSOCOM, and Norway and Sweden as PNs, more influential and contributing to the GSN through active communication, hence also supporting the challenges of accountability described earlier.[203]

b. Facilitate Information Management: Separate Network Communication from Formal Communication

The communication topics between the LOs and their parent staff can vary between training events for a few SOF operators, procurement and R&D projects, and reporting from ongoing operations, to sensitive national strategic issues. Therefore, the communication should logically pass through the Chief of Staff (COS) of the national SOCOM for distribution. Alternatively, networked non-hierarchical communication could reduce the risk of information overload on the COS, improve the speed of communication and transfer of information, decrease the response time to questions (including to a potential national network of agencies and departments). This means that NORSOCOM and SWESOCOM's information management have both formal/hierarchical and informal/heterarchical aspects.

Some discussion about information management in both formal and informal communication is probably needed. How do the SOCOMs communicate effectively, keep track of messages, and avoid unintentionally bypassing nodes that might need to be informed?[204] A natural guideline for communication should be for everybody involved to

---

[202] The organization of a "reach-back" capacity could be considered with how connections and communication are conducted with national partners: perhaps the "reach back" staff function (the national GSN manager) should be the main node for communication or networking with national partners. This idea of a dual use of the network manager to also manage a national network is elaborated in Section B.

[203] According to Admiral McRaven, active communication should include an overall attitude that information should move more quickly. It is about passing and receiving information. This might require leadership efforts to "drive people to talk" within the network. McRaven (Commander of USSOCOM) in discussions with the authors via APAN VTC, July 8, 2014.

[204] An example is communication about U.S. SOF issues. To whom do we communicate? And who should be informed? The U.S. Military Attaché, SOCEUR, or other TSOCs, NSHQ, HQ USSOCOM, the Norwegian/Swedish embassy in Washington, or the planned U.S. SOLO positioned in Norway?

distinguish between “informal” network communication and the sometimes necessary use of formal or “official” communication using the hierarchical or reporting structure (chain of command and official channels).[205] Examples of the latter would naturally include planning, reporting, and requests related to operations.

GSN topics will likely affect most of staff sections at NORSOCOM and SWESOCOM. For example, relations with the intelligence community should naturally be done through the J2 section while other issues require the commanders’ attention. A national network manager would probably have to coordinate closely with the COS and the information manager within HQ.

c. Strengthen the Communication Infrastructure

Special attention is required for connectivity. Logically, a well distributed, functional, and effectively used BICES system forces members and nodes into the network.[206] BICES may as well be sufficient for most national communications between NORSOCOM and SWESOCOM and their LO at USSOCOM. However, the reality is that most of the national communication within NORSOF and SWESOF communities is conducted on national secure communication systems, leaving the national LO at USSOCOM somewhat “out of the loop” and unable to communicate on those systems. A wider distribution of BICES and an effort to increase the use of it as a mean of communication between national entities may support the GSN effort. But, once again, the reality of current distribution and frequency of use of BICES points to a complementary need for connecting the national LO at USSOCOM into a national secure communication network.

Establishing secure national communication inside the national offices in USSOCOM J3-I could address information issues and would increase the LO’s ability to

[205] This distinction is in general natural and is normally an unspoken guideline for any communication in organizations. The point is to keep communication disciplined, specifically in regards of ensuring formal communication passing through the hierarchical chain of command. Noteworthy, though, informal communication can also be conducted according to a disciplined battle rhythm.

[206] NORSOCOM and SWESOCOM are currently using the NSHQ distributed BICES. How these systems work in relations to the U.S. BICES-X has to be clarified. NORSOCOM and SWESOCOM should ask USSOCOM for a timeline regarding the distribution of the U.S. BICES-X framework.

contribute in scenarios of national crisis, address the need for discussions of sensitive national issues, and avoid lost opportunities of reporting and communication. Selected information sharing in "groups of interested" within USSOCOM J3-I might require communication on national channels. Also, a national secure communication system might support the frequency and quality of communication with the national GSN network manager function. Further, it may support NORSOF and SWESOF visibility as burden sharers and contributors to the GSN. For example, their LO's at J3-I direct access to current national SOF reporting, through a national secure communication system, might provide opportunity to share selected information within the GSN. In other words, the effort to distribute and increase the use of BICES does not exclude connecting the national LO at USSOCOM to the national communication system.

5. How Can NORSOCOM and SWESOCOM Manage their *Commitment* within the GSN?

Milward and Provan argue that it is critical for network sustainability that managers at both the network level and the individual organization level work to institutionalize key network relations. Commitment guarantees that relations are not based purely on personal ties of a single individual in each network organization. Participating organizations need to commit resources and personnel to the network relationship that goes beyond a single individual. Managers in Networks need to build commitment in their organization to the goals of the network as a whole. One way is to ensure that multiple people are involved. When support to the network is built through the organization (instead of individuals) the commitment to the network becomes institutionalized.[207]

Foreseen commitment challenges for NORSOCOM and SWESOCOM might include difficulties in building commitment to the objectives of the overall GSN within their own staffs/organizations because of lack of understanding and priority. In addition, related to such a challenge might be the issue of NORSOCOM and SWESOCOM participating in GSN activities with only single individuals.

[207] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 24.

There are five initial actions that could be considered to institutionalize the GSN commitment and membership in Norway and Sweden:

a. Build Policy Level Support: GSN as a Strategic Option

The GSN concept may be addressed at the policy level as a "strategic option" enabling new avenues for security cooperation. The objective could be to get the GSN membership and mechanisms grounded at the national strategic level as facilitating non-alliance alternatives for both crisis prevention and crisis management. To achieve this goal requires NORSOCOM and SWESOCOM to thoroughly inform the national military leadership and the Department of Defense of the GSN (J3-I) concept of identifying common interests among PNs, suggesting multinational preventive solutions, and establishing "coalitions of the willing" based on national decision making.

A strategic level commitment to the GSN effort may in turn support other national entities' commitment to NORSOCOM and SWESOCOM's network membership (see also the following section about a potential national SOF network).

b. Build Policy Level Support: Active Dialogue with the Policy Level

Communication with the policy level should get special attention at NORSOCOM and SWESOCOM if they are striving to optimally contribute and benefit from the GSN membership. Beyond a necessary understanding among relevant civil servants in concerned departments (e.g., Department of State, Department of Defense) through an information effort by NORSOCOM and SWESOCOM, the dialogue must be kept active. NORSOCOM and SWESOCOM would benefit from insights of relevant policy goals when their LO at USSOCOM J3-I interacts in the efforts to identify common interests and collaborative opportunities among the PNs. Otherwise, NORSOCOM and SWESOCOM have a challenging task to provide their LOs with policy documents and guidelines regarding inputs to the J3-I strategic coordination process.[208]

[208] Discussions with NORSOCOM and SWESOCOM leadership have touched on the issue of what kind of inputs to the J3-I process (in identifying common national interests among PNs) should NORSOCOM and SWESOCOM provide to their LOs.

USSOCOM J3-I's ambition to establish "a common picture of PNs interests" through PN inputs is a foundation for J3-I to be able to look ahead and suggest collaborative and multinational solutions on issues. Thus, beyond forwarding the national policy documents to the LO as national inputs to the GSN common picture, identifying relevant Norwegian and Swedish national interests may require an initial outreach from NORSOCOM and SWESOCOM to the national policy level.[209]

c. Launch an Internal Information Campaign

Internal knowledge about the GSN effort and development should be enhanced through briefings within NORSOCOM and SWESOCOM staffs and at tactical SOF units. This could get more individuals and staff sections involved in GSN forums (supporting more active GSN communication), and improve overall understanding of the GSN within the Norwegian and Swedish SOF communities. In turn, this would probably support national interaction with the LOs at USSOCOM. The knowledge about purposes and possibilities of the LO position and GSN membership can increase both PN inputs to the GSN as well as easier identification of potential benefits, such as training opportunities and R&D projects.[210] Briefings could be conducted by the national LOs at USSOCOM when in Norway and Sweden.

d. Establish a Network Manager

Formalizing a national network manager ("reach-back capacity") assisting and directing the national LOs at USSOCOM J3-I, described earlier under governance, will support organizational commitment. As noted previously, this responsibility should not depend on individuals.

---

[209] The authors acknowledge challenges related to such an outreach to the political level. This underscores the requirements for a conscious national information campaign. The GSN ambitions and ideas must be explained in order to not "scare the politicians" with notions of SOF foreign policy ambitions.

[210] Communication directly between the national LO and the tactical SOF units might be another argument for including the LO in the national communication system. As touched on previously, the BICES system at the tactical SOF units should not exclude this action.

e. Formalize Objectives of the GSN Membership

The GSN is an informal network striving to minimize bureaucracy and formality.[211] However, to support commitment from the organization, within NORSOCOM and SWESOCOM it may be decided to internally institutionalize the membership by announcing the ambitions. Thus, the GSN membership, including the NORSOCOM and SWESOCOM objectives and levels of commitment related to the network, could be formalized in their internal policy documents.

The next section will address challenges and provide proposals on how NORSOCOM and SWESOCOM can create and enhance their own in-country networks; which is Management of Networks. The GSN membership can potentially support such an effort by providing national partners with access to GSN information. At the same time, an improved national SOF network can possibly make NORSOCOM and SWESOCOM better contributors to the GSN effort if provided timely national information from the various entities.

B. CHALLENGES FOR NORSOCOM AND SWESOCOM AS MANAGERS OF A NATIONAL SOF NETWORK

The participation and membership in the GSN can be a driver to create or improve a national SOF network for NORSOCOM and SWESOCOM. Overall, the national agencies and departments can potentially benefit from the GSN connections, access, and resources. In turn, a more efficient national SOF network can enhance Norway and Sweden's contribution to the GSN through enhanced information sharing and the ability to generate holistic approaches to new challenges. Therefore, one could argue that the GSN and a national SOF network will mutually nurture each other. Following that argument, not exploiting the GSN development and membership into strengthening a national network can be seen as a missed opportunity.

An underlying assumption in this section is that tangible improvements of interconnectedness between national SOF partners are unlikely unless the initiative is

[211] The only formality required for J3-I representation, and in a sense for a GSN membership, is to negotiate agreements and status of the individual LO positioned at USSOCOM.

launched from NORSOCOM and SWESOCOM. This could be a supporting argument for creating a national network unless the current status of national interconnections is satisfying for NORSOCOM and SWESOCOM. Regardless, the notion of contributing to the GSN by enhancing the information sharing might require efforts to better "connect the nodes" from a national perspective.[212] In this regard, with conscious efforts to be an active member of the GSN, the national connections will likely also improve.[213] The efforts as Manager in Networks, described earlier in Section A, to inform national stakeholders about the GSN and to institutionalize the network membership can create widespread national understanding about the GSN. Hence, those actions can directly support NORSOCOM and SWESOCOM as potential Managers of a National Network. Ultimately, to actively disseminate information about the GSN contributes to identifying opportunities and possible benefits of the GSN membership for the nodes in a national network.

Development of a national network will require NORSOCOM and SWESOCOM to take on the responsibility as Manager of Networks, leading a whole network (see #3 in Figure 16), as USSOCOM has done within the GSN. The framework for the recommendations will be Milward and Provan's five dimensions of Management of Networks, described in Chapter II, (see Table 2 in Chapter II).

As mentioned earlier, we have identified ten challenges that could be addressed by NORSOCOM and SWESOCOM as managers of their national networks. These are: handling free-riders; bringing members onboard; getting members to behave as network members; seeing the network effort as worthwhile; addressing internal frictions due to added workload; handling stove-piping and "turf" issues; addressing the perception of formal leadership; uniting members toward a common purpose; understanding the value of contribution; and upholding member commitment over time (see also Table 4).

---

[212] Connecting the nodes in a national network might support the creation of a better holistic "picture" of national interests.

[213] Active membership in the GSN will likely require NORSOCOM and SWESOCOM to increase outreach for information among national entities (stakeholders), and hence communicate more frequently among national partners. Chapter II describes how active communication strengthens ties between nodes. Chapter II also describes that the density of network ties often is directly related to effectiveness.

1. How Can NORSOCOM and SWESOCOM Manage *Accountability* in their National SOF Networks?

Milward and Provan argue that networks are essentially cooperative endeavors. However, even in the case of principal agreements of sharing the work in a network, it is relatively easy to evade responsibility and assume that someone else will be responsible for a network activity. Managers of Networks have a major responsibility monitoring participation among member nodes and to protect against the "free rider" problem. Network managers should reward members (organizations) who take on a broader network-level perspective and responsibility by aiming also to achieve network objectives. In a network, incentives take the place of a chain of command.[214]

The main accountability challenge identified for a national network may be "free-riding" among partners. The one suggested action to address this challenge has to consider the voluntary aspect of the network, as well as the challenge to get partners on board:

a. Address Expectations of Contributions Early in the Evolution

The guidelines from Milward and Provan (see also Table 2 in Chapter II) are applicable for NORSOCOM and SWESOCOM if a national SOF network is established. However, this point needs to be made during the "organizing phase" of the network. NORSOCOM and SWESOCOM should not only address potential benefits (incentives) for the members when bringing them to the network. Their staffs should also consider addressing the expectations for network members from the beginning.

The disparity of potential network members spanning tactical SOF units to intelligence agencies and policy-level institutions (see sociogram, Figure 17) calls for a wide variety of expectations on contributions to a national network. Also, it will probably

[214] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 18. It is the role of the network manager to try and work around free-riders or even to encourage other network members to exclude these free-riders from beneficial network activities. Network members acknowledging the network-level objectives and perspectives could be rewarded by the network manager through providing available resources.

require some patience before members can be expected to "deliver."[215] General expectations of contribution could be related to the overall purpose and be widely addressed, while specific expectations can be discussed with members, respectively.[216] Also, accountability issues could initially be expressed in general terms, for example, as outspoken awareness from NORSOCOM and SWESOCOM to avoid free-riding among members.

2. How Can NORSOCOM and SWESOCOM Manage *Legitimacy* in their National SOF Networks?

As was described earlier, legitimacy is based on external reputation and social recognition and is often an indicator of effectiveness and success. Network managers must consider both the internal and external legitimacy of the network, something that can be a considerable task for Managers of Networks. Externally, managers need to be able to attract new members, generate good publicity, and generally, prove to outside groups that the network is a worthwhile entity effectively addressing complex public problems. Internally, managers need to maintain the legitimacy of the network to member organizations by encouraging and enabling interaction, providing resources, and ensuring that member organizations behave like they are part of a network. Building network legitimacy (support and recognition) can in practice be done through simple activities such as hosting regular meetings, regularly talking to network members, and distributing newsletters to members and other interested parties.[217] Examples of this within the GSN are USSOCOM J3-I's Think Tank series, monthly newsletter, and bimonthly "deep dives."[218]

---

[215] As a comparison and described in Chapter III, GSN architects are well aware that PNs' (member nodes) opportunities to contribute may shift over time.

[216] For more about the network's purpose, see actions to counter legitimacy challenges in the following sub-section.

[217] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 19–21.

[218] The J3-I Think Tank series is an unclassified, informational briefings delivered by a prominent subject matter expert on an issue of current interest to the SOF community, follow by a moderated discussion with the virtual attendees through the APAN system. Bimonthly, USSOCOM hosts what it calls "deep dives" in the different regions of the world, focusing on the current and emerging challenges, and discussing potential solutions. The deep dives are done on classified VTC, and all the members of the GSN are invited to participate.

Potential legitimacy challenges related to a national network include challenges to get partners on board, get members to cooperate as network members, and to get members and internal SOF personnel to see the network effort as worthwhile. This paper puts forward six actions to counter these challenges:

a. Launch an Information Campaign

From an external management perspective, NORSOCOM and SWESOCOM initially need to get national members on board. Earlier suggested efforts to manage NORSOCOM and SWESOCOM's membership in the GSN by establishing a basic understanding of SOF and the GSN among national stakeholders through a comprehensive information campaign would also benefit ambitions to institute a national network. Thus, stakeholders could already be informed about NORSOCOM and SWESOCOM's ambitions with the GSN membership. This may include possible benefits for partners and support requests from NORSOCOM and SWESOCOM in their effort to be active members.

Some members may be easier than others to connect into a network. Stove-piped and bureaucratic agencies and departments may need more incentives than others before committing to network contribution. NORSOCOM and SWESOCOM need to identify participation advantages for potential members. As Admiral McRaven advised, "You´ve got to be able to give something to your interagency. Find out what is the touch point to bring the interagency to you."[219] For example, the Norwegian and Swedish intelligence community and law enforcement can, through NORSOCOM and SWESOCOM, get access to GSN information and working groups as well as establishing an alternate access to their U.S.-equivalent agencies through the GSN/USSOCOM interagency network.[220] A more specific advice can be for NORSOCOM J2 and SWESOCOM J2 to bring national intelligence agency and law enforcement representatives to GSN/USSOCOM-

[219] McRaven. In discussions with the authors via APAN VTC, July 8, 2014.

[220] Ibid.

hosted tabletop exercises regarding SOF intelligence.[221] In other words, the GSN membership can be leveraged when improving or establishing a national SOF network.

b. Leverage Existing Information-Sharing/Collaboration Forums

NORSOCOM and SWESOCOM could consider how existing national information-sharing forums could be leveraged to support their objectives. For example, participating in the Swedish Council against Terrorism might support SWESOCOM as an active contributor of information sharing within the GSN.[222] (See also sub-section 4 about Managing Governance later in this chapter).

c. Host Regular Network Meetings and Keep the Networked Members Informed

To enable internal legitimacy in a national network NORSOCOM and SWESOCOM could host regular meetings with various members,[223] as well as reach out and talk to individual members. Lessons can be drawn from Admiral McRaven's deliberate effort to drive communication in the GSN. The Admiral relates to his weekly VTCs: "I sometimes ask questions that I already know the answer to, in order to force people to communicate."[224]

d. Strengthen the Communication Infrastructure

To enable information sharing and interaction, including supporting the network manager to reach out with legitimacy-enhancing information and communication, NORSOCOM and SWESOCOM may consider additional distribution of national secure communication means among national network partners. Another possibility is to ensure wide distribution of BICES and enforce a more frequent use of that system.

---

[221] Rear Admiral Robert D. Sharp gave this advice during discussions with the authors during ISOF Conference, 2014.

[222] In Sweden, for example, the Interaction Council against Terrorism includes 14 agencies divided into various working groups. Säkerhetspolisen [Swedish Security Service] *Säkerhetspolisens årsbok 2013* [*Swedish Security Service Yearbook 2013*] Edita, April 2014, 14.

[223] The disparity of the members may call for dividing various members into working groups.

[224] McRaven, in discussions with the authors via APAN VTC, July 8, 2014.

e. Share Resources

NORSOCOM and SWESOCOM could also reflect on what resources, capabilities, and actions NORSOF and SWESOF can provide to encourage and recognize network membership. For example, NORSOF and SWESOF should provide specific training, equipment, and/or operational support for network partners. Partners should be invited to specific events to receive recognition for network contribution. National partners should get access to GSN information and forums.

f. Define Network Purpose

Finally, to enable legitimacy a network purpose should be defined. NORSOCOM and SWESOCOM may formulate this purpose in association with national partners. Anklam states that the first phase of creating a network is to establish the network purpose. To have a shared purpose is one of the most important factors when it comes to encourage network member collaboration within the network (see Figure 2). NORSOCOM and SWESOCOM should define one overarching purpose for a national network to support both internal and external legitimacy. Member organizations will in addition have their own purposes and agendas for participating.

A national SOF network may have an overarching purpose to connect entities not previously cooperating and improve national information sharing in order to support and improve national capacity to counter complex, globally networked, and border-crossing security threats.[225] The purpose also could be nested with the Norwegian and Swedish security strategies.[226] The purpose of a national SOF network could be a combination of Anklam's mission, idea, and learning (see Figure 3 in Chapter II).

For example, an overarching purpose for a national network could be:

> *To be a low-cost, innovative, problem-solving network connecting contributing entities in order to create holistic approaches to new security*

[225] The authors acknowledge that there are already-existing networks among law enforcement, security services, and intelligence agencies in Norway and Sweden who share information related to criminality, terrorism, etc.

[226] Official USSOCOM documents and information folders describe and illustrate how the GSN effort is nested with U.S. strategic directives and documents. See USSOCOM, *SOF 2020 Global SOF Network*.

> *challenges for the national leadership. Continually, be able to share information and grow its knowledge to enhance its performance, and keep up with the changing threat environment.*

NORSOCOM and SWESOCOM's main purpose for the GSN membership should be known among the national network members. They need to understand some of NORSOCOM and SWESOCOM's incentives and drivers for initiating a national network. NORSOCOM and SWESOCOM's purpose for the GSN membership could be in line with:

> *To be an active and contributing member in the GSN by clearly defining the national interests, sharing and receiving information to increase the GSN's ability to create a common picture and identify common interests between partner nations as well as to discover other valuable fields of cooperation. Based on national interests and political decisions, contribute to the burden sharing within the network.*

3. How Can NORSOCOM and SWESOCOM Manage *Conflict* within their National SOF Networks?

Network managers need to minimize incidents of conflict among multiple members with different organizational objectives, stakeholders, procedures, and cultures. As Milward and Provan warn, "turf issues" between agencies and issues about resource disposition within the network can undermine trust building.[227]

These warnings might call for an internal effort to conduct conflict prevention. A national SOF network consisting of various agencies and organizations with varied objectives and priorities might need some encouragement and support of delicate efforts to ensure understanding and contributions to a national network effort.

Potential conflict when managing a national network include the following: internal frictions within NORSOCOM and SWESOCOM staffs due to additional workload not directly related to their "normal" tasks and activities. Also, "stove piping" and "turf issues" among member organizations may hinder sharing of information, which in turn could affect trust building. There are two actions presented to counter these challenges:

---

[227] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 21.

a. Promote Personal Relationships among Key Leaders and Stakeholders

The relative small size of Norway and Sweden is in this case beneficial. The possibility to establish and maintain personal relationships among key leaders and stakeholders supports conflict prevention in a national network. An effort to establish a national network may require NORSOF and SWESOF leaders to put extra energy in to this effort.[228]

b. Manage Network Activities as Obligatory Tasks for the Staffs

Internal frictions within the NORSOCOM and SWESOCOM's staffs related to workload and efforts not obviously directly related to their objectives might surface. Thus, requirements for managing a national network must be understood by the staffs. For example, distributing information and contacts between a national network and GSN nodes may pass through NORSOCOM and SWESOCOM increasing the amount of work regarding information management. To overcome these tensions NORSOCOM and SWESOCOM must hold network activities as obligatory tasks for the staff.[229]

4. How Can NORSOCOM and SWESOCOM Manage *Governance* in their National SOF Networks?

When most people think about networks, they often think of a group of organizations that collaborate with each other and govern themselves. However, during a network's evolution some decisions will need to be made about how it should be structured and governed and how the governance form should be implemented. As described in Chapter II, this is what the authors call the Organize Phase (see Figure 2 in Chapter II).

NORSOCOM and SWESOCOM have to consider the design choices when creating their network. For example, deciding which of Provan and Kenis' three basic

[228] Admiral McRaven advised the authors of the importance of establishing personal relationships among leaders. He gave several examples of when personal relations between leaders untied stovepipe issues between agencies and U.S. SOF. McRaven, Discussions with the authors via APAN VTC, July 8, 2014.

[229] One notion to create a better understanding among staff personnel about a network effort could be to clearly divide the network actions from the hierarchical Chain of Command. The network itself takes no actions; instead, the network is the precondition for the Chain of Command's actions.

forms of network leadership structure they will use (see Table 3 and Figure 5 in Chapter II). The design continuum is a good tool to use in this process (see Figure 7). Roberts also states that managers have to understand that network design is a matter of choice.

Specific governance challenges for NORSOCOM and SWESOCOM could be: potential members who might view NORSOCOM and SWESOCOM as formal leaders of the network, which may negatively affect their willingness to volunteer for network membership or contribution. Also, the number and disparity of potential member organizations may prove a challenge in uniting toward a common purpose. Three initial main actions are suggested to meet these challenges:

a. Implement Governance Form as a Network Administrative Organization (NAO)

This research recommends NORSOCOM and SWESOCOM choose a Network Administrative Organization (NAO) form of governance. The number of potential network members paired with the disparity of these member organizations requires a centralized approach. The lead organization management approach is naturally rejected, at this point, due to the likely informality and voluntary style of an anticipated national network. The network administrative organization form of governance is about facilitating or hosting network activities and information sharing, in line with USSOCOM J3-I's role in the GSN. It may be essential to explain this leadership role when bringing potential partners to the network.

b. Make Dual Use of the National GSN Network Manager Function

As Provan and Kenis advise, the governance form of an NAO will require designated resources at NORSOCOM and SWESOCOM, a network administrative function. However, a cost-effective and efficient solution may be found if a "reach-back" capacity—a national GSN manager—is established at NORSOCOM or SWESOCOM (described previously in Section A). Such a function could potentially be dual-use capability as a central hub when bridging out to a national network. *That means that actions that have been implemented to manage the GSN membership at the national SOF HQs can be leveraged if establishing a national SOF network.* As described earlier, this

solution may also support increased speed of communication between the GSN and a national SOF network, hence enhancing NORSOCOM and SWESOCOM as active members within the GSN.

c. Link into Existing Information Sharing/Collaboration Forums

NORSOCOM and SWESOCOM may consider linking into already existing security-related national information-sharing and collaboration forums, for example, with the earlier recommended working groups within the Swedish Council against Terrorism.[230] In network terms, that would reduce the number of connections that need to be established and maintained individually. However, such an effort may be combined with establishing separate connections to some of these nodes in order to enable additional information sharing and cooperation (Figure 17).

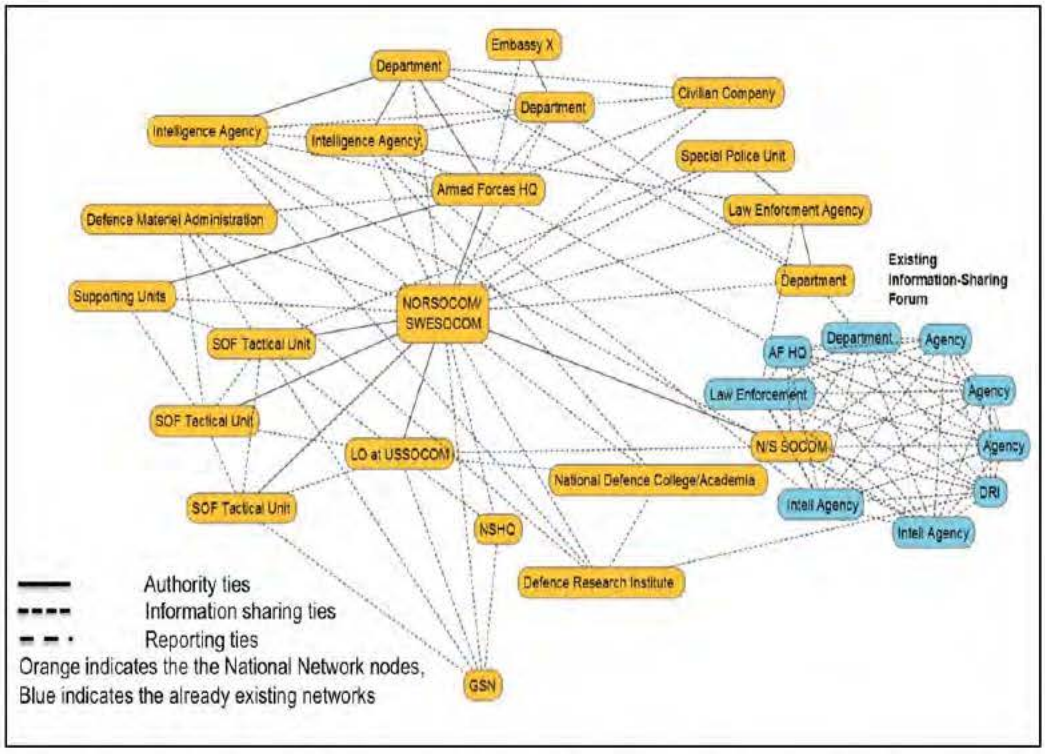

Figure 17. A national SOF network with SOCOM as the manager of networks.

[230] Interaction Council against Terrorism includes 14 agencies divided into various working groups. Säkerhetspolisen [Swedish Security Service] *Säkerhetspolisens årsbok 2013* [*Swedish Security Service Yearbook 2013*], 14

The sociogram (Figure 17) illustrates how NORSOCOM and SWESOCOM could utilize existing information-sharing mechanisms supplemented with additional connections to important network partners. The GSN node represents various entities in the Global SOF Network.[231] An example of a civilian company can be a shipping company affected by piracy. Armed Forces HQ includes operational and procurement Chain of Command, Service HQs, and supporting staff functions.

5. How Can NORSOCOM and SWESOCOM Manage *Commitment* in their National SOF Networks?

Network managers must recognize that all organizations and their representatives in the network are not equally committed to the network effort. Single organizations may be involved in several networks. Further, instead of saying that an organization is part of a network, it is often more correct to say that a particular program of an organization is part of the network. However, it is the task of the network manager to build and maintain commitment of all network members, even if not all members will participate to the same degree.

Allocation of resources and benefits should be based on level of commitment. But resources should also be used to build commitment of important, but marginally involved members. A part of the commitment-building process includes providing information to members about what the network is doing and how it is contributing to overarching goals. Further, to ensure network sustainability network managers must work to institutionalize key network relations and ensure member organizations commit resources and personnel to the network relationship beyond single individuals.[232]

For NORSOCOM and SWESOCOM, commitment challenges may include challenges to get members to understand the potential value of contribution to the network effort. Also, it could be a challenge to uphold members' commitment to the network over time. This paper presents five actions to address these challenges:

---

[231] USSOCOM J3-I; USSOCOM Interagency Network; and PN's SOCOMs and tactical SOF units.

[232] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 24.

a. Information Campaign: Define Possible Benefits for Member Organizations

Reaching out from NORSOCOM and SWESOCOM to potential national members will be needed to attract their interest. The staffs should emphasize that it is a voluntary non-obligation network and acknowledge the reality that not all participants can contribute and benefit equally over time. However, this message should be combined with notions about expected contributions (see earlier section about accountability).[233]

b. Trust-Building Efforts: Information Sharing and Personal Relationships

As USSOCOM has done with the GSN effort, NORSOCOM and SWESOCOM could focus on trust building. Ensuring commitment to a network effort and information sharing requires established trust between partners. Personal relations among leaders are one step in this direction, and so are information-sharing.[234] Sharing builds trust, which in turn leads to more sharing, which supports more trust as a mutually reinforcing mechanism. General McChrystal describes his efforts as commander of JSOC:

> We instructed our people to share more information than they were comfortable with and to do so with everyone who wanted to be a part of our network … [W]e widely distributed, without preconditions, intelligence we captured or analysis we'd conducted. The actual information shared was important, but more valuable was the trust built up through voluntary sharing with others.[235]

Acknowledging that these experiences are from a time of war with high stakes and that a "post-war" period can reduce incentives to share, they nevertheless suggest an important role for leaders. NORSOCOM and SWESOCOM leaders could identify what intelligence or information could be shared and then show good faith by "taking the first step" to share this information to build trust.

---

[233] Milward and Provan, *A Manager's Guide to Choosing and Using Collaborative Networks*, 7. Milward and Provan acknowledge that management of commitment can conflict with accountability.

[234] USSOCOM, ISOF Conference 2014, *Senior Leader Guide*.

[235] McChrystal, *My Share of the Task*, 154–155.

In line with the USSOCOM J3-I position, NORSOCOM and SWESOCOM also have to recognize the timeless challenges related to sharing intelligence by openly admitting that all information cannot be shared with everybody in the network at all times.

c. Get Members to Institutionalize their Memberships

When the initial identification of the participating nodes in the network is done, points of contact (POCs) should be established, including alternative channels and contact persons in the member organizations. That is, NORSOCOM and SWESOCOM should signal expectations towards participating organizations to institutionalize their network membership by involving more than single individuals.

d. Promote "Success-Stories" from the Network

NORSOCOM and SWESOCOM could promote network "success stories" to demonstrate network value,[236] for example, describing concrete successful cooperation among network entities or recounting innovative solutions to complex problems. Even if communication and meetings might take place in smaller forums or working groups, NORSOCOM and SWESOCOM might highlight successful network activities and regularly communicate their accomplishments throughout the network in order to build commitment.

e. Strengthen the Communication Infrastructure

A possible commitment-building effort would be to provide resources for secure communication between the different national members. The creation of a single platform for network collaboration would increase the probability of network participation.

[236] The idea of being able point to "success stories" from network collaboration has been suggested by LOs at USSOCOM when discussing the GSN.

C. SUMMARY

1. Management of NORSOCOM and SWESOCOM's GSN Membership: Management in Networks

NORSOCOM and SWESOCOM have been foresighted in the placement of LOs at USSOCOM and are well positioned for an evolving GSN. The LO is a relatively low-cost contribution to engage in a network with no formal requirements. The current complex security environment and constrained fiscal reality makes participating in a global network like the GSN potentially beneficial for a small nation. However, as the GSN evolves there are possible actions within the national SOCOMs that should be considered as member organizations in the network. Both network theory and discussions with GSN designers point to expectations and opportunities for NORSOCOM and SWESOCOM to contribute to and benefit from a conscious and active network membership.

Options for consideration are NORSOCOM and SWESOCOM´s information campaigns to various national audiences in order to obtain buy-in from internal and external stakeholders. The HQs also could establish internal staff and communication routines to actively participate in the GSN dialogue. The appointment of a national network manager may enhance the support and guidance of the LO at USSOCOM/J3-I. To enable network participation, a robust communication infrastructure is needed to encourage the flow of ideas and information. To benefit from a GSN membership NORSOCOM and SWESOCOM need to do their share of "putting energy into the network." In summary, resources (personnel and time) need to be assigned at NORSOCOM and SWESOCOM to manage the GSN membership in a trustworthy way.

2. Management of NORSOCOM and SWESOCOM's National SOF Networks: Management of Networks

If NORSOCOM and SWESOCOM have ambitions to develop current national partner cooperation into an enduring networked approach, it will require dedicated resources and deliberate actions. The management of the GSN membership can be leveraged. National partners can find incentives to "buy-in" to a network should they be provided a new information channel (GSN information). Further, dual-use of a national

GSN manager (the manager *in* network) as also the central hub of a national network (the manager *of* network) may be both cost effective and efficient for distributing information between international and national nodes. However, a unifying network purpose should be formulated to enable legitimacy and support collaboration.

Personal relations within the network and among organizational leaders can counter conflicts. The size and variety of organizations in a potential network based on voluntarism and informality call for a centralized facilitating approach—an administrative function managing the network. As a complement to establishing "their own" network connection to national entities, NORSOCOM and SWESOCOM also may consider linking into already existing security related information-sharing forums.

In order to establish and sustain commitment to a national network NORSOCOM and SWESOCOM could address trust-building activities, such as information-sharing efforts, as well as information campaigns to describe potential membership benefits. In addition, hosting regular network activities among members may support legitimacy, strengthen relationships, and enable shared understanding on issues. To do this, NORSOCOM and SWESOCOM should strive for a single ICT platform for network collaboration. They may also be prepared to provide resources in order to distribute these systems to partners. Further, NORSOCOM and SWESOCOM should honestly and early indicate awareness of intentions to avoid "free-riders in the network, while also acknowledging the reality that contributions can vary over time and between partners. Within NORSOCOM and SWESOCOM's staffs there has to be widespread understanding of the potential benefits, objectives, and challenges related to a network effort: working tasks for maintaining the network cannot be seen as secondary tasks for individuals directly involved.

As defense analyst, Christopher Lamb concludes about SOF and interagency cooperation:

> Making collaboration the priority and changing one's own organization to facilitate collaboration is painful. It is far easier, and often safer, to

> promote the importance of collaboration without doing anything to irritate one´s superiors or subordinates.[237]

Chapter V, which follows, summarizes the capstone project with conclusions and recommendations. The chapter puts forward a few recommendations to USSOCOM on how to continue and enhance the evolution of the GSN into the near future. Further, the chapter provides recommendations to NORSOCOM and SWESOCOM on how to manage their GSN membership as well as how to manage the initial phases of a potential national SOF network.

[237] Lamb, "Global SOF and Interagency Collaboration," 19.

V. SUMMARY AND RECOMMENDATIONS

The purpose of this capstone project has been to address the following question:

How can NORSOCOM and SWESOCOM contribute to and utilize the Global SOF Network to enhance SOF collaboration as a way to respond to 21st century threats?

To address this question, we first introduced some basic concepts of social network theory and provided an overview of the GSN and how it functions. We then summarized the challenges NORSOCOM and SWESOCOM faced as managers in the GSN and as potential managers of a national SOF network. Recommendations then follow what we believe can enhance NORSOCOM and SWESOCOM's ability to actively participate in the GSN.

A. THE NETWORK APPROACH

As early as 1996, John Arquilla and David Ronfledt proposed the concept that "It takes a network to fight networks." Their idea did not get much attention at the time. Scott Morrison recently stated that in the aftermath of September 11, 2001, Arquilla and Ronfledt brought the issue into sharper focus in a follow-on piece entitled "The Advent of Netwar (Revisited)," with the statement:

> It takes networks to fight networks. Governments that want to defend against Netwar may have to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially by building new mechanisms for interagency and multijurisdictional cooperation.[238]

In accordance with Arquilla and Ronfeldt, most Western nations now understand that a single nation´s tools alone are inadequate in confronting the challenges of the 21st

[238] Scott Morrison, "Redefining the Indirect Approach, Defining Special Operations Forces (SOF) Power, and the Global Networking of SOF," *Journal of Strategic Security* 7, no. 2 (2013): 48–54. John Arquilla and David Ronfeldt, eds. "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 15.

century. They are signaling the need for international cooperation and collaboration, intelligence sharing, interagency cooperation, and more flexible tools for implementing future solutions to destroy these interconnected, net-centric threats. The GSN is one example of this international effort.

Collaborative initiatives are the backbone of the Global SOF Network and the operational success in countering current threats and preventing future conflicts lies in a comprehensive whole-of-government approach.

The next two sections summarize what has been accomplished from a GSN perspective and from the perspective of NORSOCOM and SWESOCOM as GSN members. The main purpose is to provide NORSOCOM, SWESOCOM, and USSOCOM with recommendations on what needs to be done to support the continuing evolution of the network. The recommendations are derived from the analysis in Chapter III and Chapter IV, but are grouped in what we believe are the main themes that should be considered.

B. RECOMMENDATIONS TO THE OVERALL GSN INITIATIVE

1. What Has Been Accomplished?

As GSN representatives at USSOCOM define it,

> Global SOF Network represents the cornerstone of a new, prevention-oriented security posture. As special operations forces around the world collaborate in prosecuting complex problems, a new synergy emerges that is stronger than the sum of its parts. Navigating and adapting in unfamiliar environments; engaging, partnering, and building trust; and problem solving amidst uncertainty will be core competencies for a globally networked SOF postured to combat the threats of today, and the future.[239]

Operationally speaking, the GSN is a network of organizations with multiple sub-networks that are physically dispersed. They create a global and multilayered structure and are built upon the framework of the U.S. SOF organization and technology. Unique personal relationships, the experience of SOF personnel from years of warfighting, and

[239] Keenan D. Yoho, Tess deBlanc-Knowles, and Randy Borum, "The Global SOF Network: Posturing Special Operations Forces to Ensure Global Security in the 21st Century," *Journal of Strategic Security* 7, no. 2 (2013): 1–7.

the trust that has been established within the SOF community provide the foundation of this network. The challenge is to maintain and extend this trust within the IA and the political community.

The name of the network—the Global SOF Network—appeals to the identity of the members, regardless of nationality: Special Operation Forces emphasizes the people in the organization as the main strength. USSOCOM, through the GSN, advocates the need to cultivate this unique SOF culture and to continue to invest in people to be able to operate in any future environment..[240]

As analyzed in Chapter III, the internal design elements of the GSN are a good fit with each other. GSN designers have done their homework. From a network perspective, most considerations seem to have been addressed throughout the development of the GSN concept. Examples include, creating a common purpose, creating a disciplined battle rhythm, and establishing planning processes that facilitate PN contribution and decision-making processes (see Figures 12 and 13 in Chapter III). Nonetheless, the development of the GSN is an ambitious effort with considerable challenges. For example, in many cases, future outputs and outcomes require policy-level decisions, especially for the participating PNs. In the short term this means that the information campaign to get stakeholders' buy-in is far from over. Although the GSN ambition has attained momentum as one of the main strategic efforts for the future at USSOCOM, the current challenge for the network appears to be the understanding in the political and military leadership of the GSN concept.

The next subsections give USSOCOM, NORSOCOM, and SWESOCOM recommendations for how to support the future evolution of the GSN towards its performance phase. As Morrison concludes, the SOF community is ideally suited to lead these innovative efforts and serve as an enabler and catalyst to engender greater multinational and inter-agency collaboration through a comprehensive network approach.[241]

---

[240] USSOCOM, ISOF Conference 2014: *Senior Leader Guide*, 12.

[241] See also: Scott Morrison, "Redefining the Indirect Approach, Defining Special Operations Forces (SOF) Power, and the Global Networking of SOF," *Journal of Strategic Security* 7, no. 2 (2013): 48–54.

2. Recommendations for the Future: What Needs To Be Done?

Acknowledging the exceptional effort already undertaken by USSOCOM regarding the establishing of a GSN, one can see that continued evolution would require additional efforts. Our recommendations are grouped under the following themes: 1) framing the GSN narrative; 2) getting stakeholders' buy-in; and 3) strengthening network communication infrastructure.

a. Framing the GSN Narrative

The variation of declared purposes of the GSN effort and the overwhelming U.S. perspective in all the documents that have been produced regarding the GSN is probably a result of USSOCOM's need to convince internal stakeholders of the concept. Also, it can be seen as a natural result of the ongoing dialogue of the network's evolution and purposes, which can shift or be refined throughout time.

USSOCOM should now expand its focus to support the PN's national dialogue by framing the GSN purpose more clearly from a PN's perspective: *what's in it for the PN?* For example, USSOCOM could highlight the GSN as a forum for SOF collaboration (operations, training, and development), a framework for information sharing (improving the PN situational awareness), and a structure for discussion and identification of areas of common national interest. The network could potentially enable, increase effectiveness, and/or make the PN SOF operations more cost effective when addressing future threats. *In doing this, the target audience is no longer the PN SOF communities, but the military leaders and the political leadership who are the decision makers and policy makers within the PNs*. For example, Swedish and Norwegian participation is not intended primarily to support the TSOC and GCCs better with special operations forces and capabilities.[242] However, GSN as a forum for potential action and collaboration, according to the national interests, should be illuminated for PNs' policy makers.

To create this updated narrative, the USSOCOM leadership should task the GMSC with leading the review, and the narrative should address the most important

[242] This purpose is the most common in USSOCOM documentation and speeches.

participants- the PNs who contribute capabilities, access, and information to the overall GSN purpose. The J3-I Division should be responsible for updating the PN part of the narrative. It is crucial that during this process the PN LOs interact with their national headquarters to ensure that the national SOCOM leadership supports the narrative. The narrative also should play to the benefits of global SOF collaboration, since it is a framework for information sharing and enhancing the collective knowledge, and a forum for discussion and identification of areas of common national interests. The GMSC would then tie the J3-I product together with the IA and U.S. product into one document.

USSOCOM should get the U.S. administration to reach out with the GSN narrative within the U.S. communities to enhance the network legitimacy internally. The next step is to get the U.S. administration to reach out to international partners to enhance the network legitimacy externally. When doing this, it is important to emphasize that network performance is dependent on PNs' active contributions. A U.S. top-down blessing would possibly soften PNs' internal challenges with information sharing and burden sharing to the GSN effort.

The updated narrative would be an important statement to convince the PNs' policy makers of the purposes and benefits of GSN participation.

b. Getting "Buy-In" from Stakeholders'

All network members have to get commitment from their national stakeholders. For USSOCOM, as the main node in the network, this means that it needs to get buy-in from its internal U.S. stakeholders as well as the PNs.

The first step in the process, after the new narrative has been updated, is getting the internal stakeholders' buy-in. USSOCOM leadership has to sell the new narrative to the U.S. political leadership and the IA leadership to reinforce the importance of the GSN. Through this process, USSOCOM has to influence the U.S. administration to promote the GSN narrative when engaging with the PNs´ political leadership.

At the same time, USSOCOM has to encourage the PNs' SOCOM to sell the GSN narrative internally to their national stakeholders in order to build national support

for the GSN effort. It is also vital for PN SOCOMs to inform their political leadership so all can discuss the GSN effort and the potential benefits of participation.

The next step to get stakeholders to buy-in is for USSOCOM to create a releasable version of the *Global Campaign Plan-Special Operations* (see Figure 10, Chapter III), which today is a U.S.-only classified document. A wider distribution of this plan will enhance the GSN members' understanding of the U.S. global effort. Understanding the U.S. perspective, as the main node in the network, will increase the possibility of PNs' contribution to the plan from their national perspective. It likely will prompt the PNs to create a similar document within their own nation, something that can exponentially increase the network's ability to build a common picture and identify common interests. In summary, USSOCOM should initiate the process of making the *Global Campaign Plan-Special Operations* releasable to the different PN SOCOMs in order to increase the knowledge about U.S. goals.

c. Strengthening Network Communications Infrastructure

The ICT portal and web 2.0 are slowly moving from a simple face-to-face coordination interface to a common platform through APAN and BICES-X. In addition to these tools, USSOCOM has allocated PN office spaces for LOs to establish and access their national systems for quick and secure reach-back to their national SOF headquarters.

The ICT framework within the GSN needs continual attention, funding, support, and a robust distribution so all members can use a single information platform. The ability to communicate with other GSN members on a singular platform is critical to improving the GSN performance and achieving the network´s purpose. A wider distribution of BICES-X and a dedicated effort to increase the use of it as the primary means of communication within the GSN is also expected to enhance network cooperation and collaboration.

The network also will need to incorporate the three systems discussed earlier (see Figure 11, Chapter III): *APAN* for unclassified information sharing and collaboration; *BICES-X* for classified information sharing and collaboration; and finally *national secure*

systems within the national offices to make sure that the LOs are able to discuss with their national SOCOMs on national issues and at the same time be kept "in the loop" as long as the national system is the primary system used nationally.

The reality of BICES´ current distribution and frequency of use points to a need for PNs to support distribution of the systems and funding to secure a swift rollout and promotion of BICES within the GSN.

C. RECOMMENDATIONS FOR NORSOCOM AND SWESOCOM AS GSN MEMBERS

1. What Has Been Accomplished?

NORSOCOM and SWESOCOM have been foresighted in placing LOs at USSOCOM/J3-I and are well positioned for an evolving network. Hence, being among the earlier participants in a growing J3-I supports national understanding of the GSN and its processes, and enhances the LOs' influence within the J3-I Division. The appointment of an LO has been a low-cost contribution in this network; there are no formal alliance-like requirements. Further, NORSOCOM and SWESOCOM's leadership has actively participated in GSN activities and conferences and communicated with their LOs at USSOCOM. The leadership is well positioned to understand the GSN's benefits and implications, but what else might be needed to be long-lasting active members, especially in terms of additional resources (personnel, time, and hardware)?

2. Recommendations for the Future: What Needs To Be Done?

NORSOCOM and SWESOCOM need to enable efficient network communication, build national stakeholder support, contribute to the GSN, and strengthen national interconnectedness among partners. Our recommendations are grouped into three themes: 1) managing communication and information flow; 2) getting stakeholders buy-in; 3) burden sharing; and 4) strengthening or creating a national network.

a. Managing Communication and Information Flow

Organizationally, NORSOCOM and SWESOCOM should consider establishing a *network management function* to support and direct activities in the GSN. This management function could improve the commands' cooperation with the GSN management level (USSOCOM), enhance active network participation, and better organize network related activities within their respective organizations. The function also should involve a "reach-back capacity" directing and supporting the LOs at USSOCOM/J3-I, as well as having dual responsibility as a central hub bridging out to a national network from the overall GSN.

To make this network management function operational, NORSOCOM and SWESOCOM would need to expand and strengthen the communication infrastructure. A wider distribution of BICES-X and an effort to increase the use of it as a means of communication within the GSN is needed. In addition, connecting the national LOs at USSOCOM into a national secure communication network will strengthen their ability to support the LO with national information is warranted.[243] In other words, the effort to distribute and increase the use of BICES should not exclude connecting the national LO at USSOCOM to the national communication system.

The distribution of the BICES-X system should not be a U.S. responsibility alone. NORSOCOM and SWESOCOM have to support the effort of distributing the systems and, if necessary, supporting this effort with funds to secure a swift rollout.

To support communications and flows of information, NORSOCOM and SWESOCOM need to have disciplined information management. For example, integrating GSN communication in the internal staff's battle rhythm and consciously separating informal network communication from formal communication. A network manager must therefore work closely with the COS and the IM within the national SOCOM to ensure this integration.

[243] A national secure communication system inside the national offices at USSOCOM/J3-I might support the frequency and quality of communication with the "reach-back capacity" and support NORSOCOM and SWESOCOM's visibility as burden sharers and contributors to the GSN. For example, if their LOs at J3-I have direct access to ongoing national SOF reporting during operations through a national secure communication system, they then have the opportunity to share selected information at J3-I.

b. Getting Stakeholders' Buy-In

An information outreach to national stakeholders will require clarifying the GSN narrative. Network managers first need to be responsible to merge the updated GSN narrative from USSOCOM/J3-I with the national narrative in order to create an overall information campaign announcing the benefits of membership, and the potential benefits of creating a national SOF network.[244] The narrative should play to the *benefits* of global SOF collaboration in enhancing the collective information sharing, building intelligence, and acting as a forum for discussion of areas of common national interests (see also Section D, Main Benefits).

NORSOCOM and SWESOCOM also need to launch a focused information campaign to create a thorough understanding of the GSN among national stakeholders to enhance the probability for strategic-level utilization of the GSN membership. For example, enhanced understanding at national policy levels ideally would result in an active dialogue within the nation as well as the generation of relevant national inputs into the J3-I effort that identifies common interests within the GSN. Other prioritized targets for the information campaign would be those departments and agencies that can support NORSOCOM and SWESOCOM with the capabilities and information needed to participate in the GSN.

An information effort directed toward NORSOCOM and SWESOCOM staffs also could increase internal understanding of purpose, objectives, and potential benefits and challenges to counter potential challenges, such as increased workload and internal commitment within own staffs. Further, understanding of the GSN among national intelligence agencies could increase the likelihood for information sharing with the GSN. NORSOCOM and SWESOCOM have to champion and promote the GSN to their national administrations as they engage with other GSN members. It is vital for the national SOCOMs to keep policymakers updated so all can mutually discuss the GSN efforts and potential benefits.

[244]It is crucial during this process for the network management function to interact with the national stakeholders to ensure that they also gain ownership of the GSN narrative.

In summary, the ideal of an information campaign would be to improve the legitimacy of NORSOCOM and SWESOCOM's GSN membership, as well as enhance supportive commitment to the effort.

c. Burden Sharing

Burden sharing in a global SOF perspective can be done in many ways. However, deploying SOF to crisis regions is probably the most credible contribution. If UN, EU, or NATO opportunities drag on due to lack of consensus, GSN and J3-I can facilitate and support bilateral or multilateral opportunities for "preventive missions" that address, directly or indirectly, transnational and networked threats. Specifically, host nation-invited "indirect approach" missions to build capacity of local security forces are a foreseen need and these host-nation requests may coincide with Norwegian or Swedish national interest. These types of missions open new possibilities for small-scale, long-term comprehensive efforts as a national contribution. Diplomacy, financial aid, judicial support and advice, as well as SOF advisors/trainers can be combined in a unique effort from a "small nation" such as Norway and Sweden.

A less visible but still important aspect of burden sharing is for NORSOCOM and SWESOCOM to provide relevant inputs regarding "national interests" to their LOs that help the J3-I's efforts to identify PNs' common interests and solutions. Obtaining this kind of information can be difficult from countries like Norway and Sweden who may have less outspoken, or distinct, national interests that may be relevant in the GSN processes. Nevertheless, NORSOCOM and SWESOCOM need to put an effort into providing information that can be used in the J3-I process of generating common interests. Creating this information will prompt an active dialogue at the national policy levels and in their various departments.[245] If created, NORSOCOM and SWESOCOM could use their network management function to create a document explaining the national interest, which the LO at USSOCOM can use in the J3-I process of identifying common interests. Integrating the document in the J3-I process is a way to identify where

[245] The policy level would include the military strategic leadership and relevant personnel in the Ministry of Defense and Ministry of Foreign Affairs.

Norway and Sweden can utilize the GSN for national interests/benefits. Further, it is a method to signal commitment and build trust within the USSOCOM/J3-I.

Finally, another possibility to contribute to GSN is for NORSOCOM and SWESOCOM to establish national information-sharing channels to provide GSN with national information. National intelligence agencies could be tasked to support NORSOCOM and SWESOCOM in their GSN effort. Acknowledging challenges in this regard, a minimum effort should be to establish trusted (personal) relationships with national partners and establish mechanisms to make sure that they are informed when certain (SOF/GSN-related) information is shared through other intelligence channels.[246]

d. Strengthening or Creating a National Network

NORSOCOM and SWESOCOM are well positioned as contributing and active members of the GSN. Although it is possible to be an active and contributing member of the GSN without creating a national network, creating a national network could add value to the whole system. We suggest creating ties between the international network membership (GSN), and the national network. Designing these networks should be conducted in parallel to acknowledge the continuous evolution of the overall network. Only if resource constraints hinder such a practice should a sequential effort be considered.[247] The advantage is that the GSN and the national SOF network could mutually nurture each other and be a more cost effective and efficient way of building out the network. Hence, not exploiting the GSN membership and linking to a true national network can be seen as a missed opportunity.

National network ties do more or less already exist; but what is needed in the initial phase is to formally establish a management entity that establishes overall purpose for the network and organizes the network stakeholders. This effort will require a delicate

[246] The purpose is for the national LO at USSOCOM J3-I to be able to inform international partners (PN) that their nations have been provided Swedish or Norwegian information through, for example, intelligence agency channels.

[247] The advice of a sequential approach is made with an understanding of limited resources at the national SOF HQs. Therefore, a "one step at a time" approach might be the way ahead. Also, a solid GSN membership will probably support the establishment of a national network. However, some overlap between international and national networking efforts could be natural also in the earlier phases.

mix of informing stakeholders, attracting potential members, providing benefits and incentives, exploiting personal relationships, establishing communication routines, and formalizing the network's design. A plan for how to establish the network may be required, however, the details for such a plan are outside the scope of this project.

The size and variety of organizations in a potential national network requires some mechanism of integration as discussed earlier in this project. The NAO form of governance is one option, but it is important to explain its leadership role to potential partners to avoid the appearance of NAO having control over the network.

The NAO´s challenges would be to create shared national network purpose. NORSOCOM and SWESOCOM in association with national partners could develop one overarching purpose that supports both internal and external legitimacy to get buy-in from stakeholders. The purpose has to be nested with the national security strategies and in addition, it has to be understood that each participating entity will have its own purposes and agendas for participation.

The next step would be to establish buy-in from national stakeholders, like intelligence agencies, departments, and law enforcement agencies, to grow the network. NORSOCOM and SWESOCOM have to create incentives for these agencies and departments by identifying participation advantages. For example, the GSN membership can be leveraged to bring organizations into a national network by creating access to GSN information, working groups, and U.S.-equivalent inter-agencies that will be beneficial in a national context. To get organizations "on board," NORSOCOM and SWESOCOM should start by selling the narrative of a networked approach and GSN, in general, and the national network, in particular. The policy level should get special attention in this regard to build the necessary support from the political leadership. Additional actions to enhance the legitimacy of a national network and support the buy-in effort may include trust-building activities such as having NORSOCOM and SWESOCOM take the first step and share their resources and information with their national network.

Finally, to increase the probability of network participation, NORSOCOM and SWESOCOM should aim for a single ICT platform for network collaboration. It could develop through a wider distribution of BICES among national partners or through dissemination of a secure national system. A single ICT system would enable information sharing, interaction, and collaboration, as well as enhance for the network manager function to share information between the global and national levels. To underline the importance of a single ICT system, NORSOCOM and SWESOCOM should be prepared to provide resources (hardware) to secure a wide distribution of the system. This could be another way to convince partners to commit to the network effort.

Through the single ICT platform, the network management function could draw on GSN efforts to create and initiate network activities. For example, NORSOCOM and SWESOCOM could host regular group meetings with the members, as well as reach out and talk to individual members. Working groups could be formed to address specific topics through discussions and briefings aiming at increased knowledge and shared understanding, like USSOCOM/J3-I's Think Tank series and bimonthly "deep dives." A secure communication system, capable of hosting VTCs, would likely increase participation in network activities. Creating and distributing "newsletters" to inform about network activities can be another example of network activities that can reinforce the members' commitment.

e. Suggestions for the Way Ahead

If NORSOCOM and SWESOCOM want to pursue our recommendation to create a national SOF network, they would need to formulate a plan for establishing, and strengthening the national network. Examples of issues to be addressed for such a project include:

- Identify who are the obvious members and what other organizations are desirable participants.
- Investigate how differences in classification of information and security measures between agencies and departments (for example, differences between the armed forces, law enforcement, and departments) can be managed if distributing a uniform ICT system among national entities.

- Identify the kinds of network activities that could be relevant to all members and frequency of these activities.
- Explore whether LOs should be distributed within the network-permanently or on demand?
- Identify metrics to evaluate network performance, and identify desirable outputs and outcome.
- Formulate an initial communication plan to promote a national network.

To complete the project, the last section provides NORSOCOM and SWESOCOM a summary of the main benefits for a PN as a GSN member. These benefits have been identified when doing the research and the analysis of the GSN concept and future planned efforts.

D. MAIN GSN MEMBERSHIP BENEFITS IDENTIFIED FOR NORWAY AND SWEDEN

This project has suggested that NORSOCOM and SWESOCOM can define their future contributions regarding the GSN. If our recommendations are pursued, additional resources (personnel, time, and hardware) will be required. However, we believe these are "low-cost" investments with high benefits.

The main benefits identified for Norway and Sweden are: 1) developing connections that are already in place; 2) gaining new information channels; 3) realizing quick reaction time when reaching out for support; 4) gaining a new strategic option for security cooperation; 5) accessing enhanced opportunities for training and R&D projects; and 6) enhancing national interconnectedness.

- *Already in place global connections.* As a GSN member the nation can use all the different connections currently in place to deal with national crises response and in planning for deliberate operations.
- *A new channel for enhanced situational awareness.* As a GSN member, a nation has access to a broad information channel in case of a crisis involving national interest or to support the policy level following a potential threat.
- *Network connections that can enable quick reaction time.* As a GSN member, a nation can rely on the whole network for support in a crisis response situation like providing access to resources not organically available in Norway or Sweden. For example, Airlift and ISR-capabilities.[248]

[248] Smethurst, in discussions during International SOF Conference, 2014.

- *A new strategic option for security cooperation.* The GSN membership and the J3-I mechanisms facilitate non-alliance alternatives for both crisis prevention and crisis management. For example, the J3-I ambition to develop and suggest multinational solutions may match national will and military feasibility when facing NATO or EU non-consensus situations.
- *Cost-effective collaborations.* As a GSN member the opportunity for collaboration expands exponentially with every new member. For example, it enables identifying new opportunities for training, procurement of hardware, and R&D projects.
- *National interconnectedness.* Being a GSN member can be a driving force to connect national partners and stakeholders together. For example, the access to new information and communication channels, think tanks, and cooperation forums can create incentives for national partners to increase cooperation as well.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Books:

Anklam, Patti. *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World*. Amsterdam, Netherlands: Butterworth-Heinemann & Elsevier, 2007.

Cohen, Louis, Lawrence Manion, and Keith Morrison. *Research Methods in Education*. 7th ed. New York: Routledge, 2011.

Holohan, Anne. *Networks of Democracy: Lessons from Kosovo for Afghanistan, Iraq, and Beyond.* Stanford, California: Stanford University Press, 2005.

Sapolsky, Harvey, Benjamin Friedman, and Brendan Green, eds. *U.S. Military Innovation since the Cold War: Creation without Destruction*. New York: Routledge, 2009.

Tapscott, Don, and Anthony D. Williams. *Makrowikonomics: New Solutions for a Connected Planet*. New York: Portfolio/Penguin, 2012.

McChrystal, Stanley A. *My Share of the Task: A Memoir*. New York: Portfolio/Penguin. 2013.

Government Documents:

Department of Defense. *Qudrennial Defense Review 2014.* Washington, DC: Department of Defense, 2014.

European Union. *Internal Security Strategy for the European Union: "Towards a European Security Model."* Brussels, Belgium: February 23, 2010. http://eeas.europa.eu/csdp/about-csdp/european-security-strategy/index_en.htm.

Forsvarsdepartementet [Ministry of Defense]. *Et forsvar til vern om Norges sikkerhet, interesser og verdier* [*a defense for protection of Norway's security, interests, and resources*], Parliamentary Bill no. 48 (2007–2008). 2008.

_____. *Et forsvar for vår tid* [A defense for our time]. Parliamentary Bill no. 73S (2011–2012). 2012.

_____. *Evne til Innsats: Strategisk konsept for Forsvaret* [Capability for effort: strategic concept for the Norwegian defense]. http://www.regjeringen.no/upload/FD/Dokumenter/Evne-til-innsats_strategisk-konsept-for-Forsvaret.pdf.

Justis og Beredskapsdepartementet [Ministry of Justice]. *Terrorberedskap* [Terrorism preparedness]. White Paper no. 21 (2012–2013). 2013.

North Atlantic Treaty Organization. *NATO's Strategic Concept: For the Defense and Security of the Members of the North Atlantic Treaty Organization. (Active Engagement, Modern Defense)*. November 19, 2010. http://www.nato.int/strategic-concept/index.html.

_____. *Secretary General´s Annual Report.* 2013.

President of the United States. "2010 National Security Strategy." U.S. Government Executive Branch. May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

_____. *"2011 National Strategy for Counterterrorism."* U.S. Government Executive Branch, June 2011.

Regjeringskansliet. Forsvarsdepartementet. [Ministry of Defense] *"Veivalg i en globalisert verden*." [Choices in a globalized world] *Stockholm. Elanders Sverige AB. 2013.*

_____. "*En Strategi for Sveriges Sikkerhet."* [A strategy for Sweden's security] (summary). http://www.regeringen.se/sb/d/12083/a/59929.

United States Special Operations Command, *Concept of Operations for the Global Special Operations Forces Network 2020* (Global SOF Network 2020). Tampa, Florida. July 29, 2013.

_____. *Commanders Appreciation: The Strategic Environment*. Document provided as handout during briefing at Naval Special Warfare Command. Tampa, Florida. February 10, 2014.

_____. *The Global SOF Network: Campaign plan Fact Sheet*. Tampa, Florida. 2013.

_____. *Global SOF Network.* White Paper. Tampa, Florida. April 22, 2013.

_____. *Global SOF Network.* White Paper. Tampa, Florida. February 11, 2014.

_____. ISCC, "Processes and Battle Rhythm," Information Brief. Tampa, Florida. April 30, 2014.

_____. *International Special Operations Forces Conference 2014: Senior Leader Guide*. Tampa, Florida. May 19–22, 2014.

_____. Job Description: Part 1, Job Identification (Special Operations Liaison Officer to HQ USSOCOM. Foreign Liaison Officer), DRAFT 1. Tampa, Florida. April 30, 2014.

_____. "Operationalizing the Global SOF Network." J3-I Brief. Tampa, Florida. September 15, 2014.

_____. *SOF 2020 Global SOF Network*. Information folder. Tampa, Florida. 2013.

_____. *Special Operations Forces Operating Concept.* Tampa, Florida. May 2013. http://www.defenseinnovationmarketplace.mil/resources/SOCOM2020Strategy.pdf.

US Congress. McRaven, William H. Posture Statement Before the 113th Congress House Armed Services Committee. March 6, 2013.

Utenriksdepartementet [Ministry of Foreign Affairs]. *The EEA Agreement and Norway´s other agreement´s with the EU (2012-2013).* White Paper. 2012.

Periodicals/articles/reports:

Arquilla, John, and David Ronfeldt. "The Advent of Netwar (Revisited)." In *Networks and Netwars: The Future of Terror Crime, and Militancy*, edited by John Arquilla and David Ronfeldt. Santa Monica, California: RAND, 2001.

Feickert, Andrew. *U.S. Special Operations Forces (SOF): Background and Issues for Congress*. (CRS Report No. RS21048). Washington, DC: Congressional Research Service, September 18, 2013. http://fas.org/sgp/crs/natsec/RS21048.pdf.

Joint Special Operations University Report. Edited by Chuck Ricks. *The Role of the Global SOF Network in a Resource Constrained Environment*. MacDill AFB, Florida: The JSOU Press, 2013.

Kenis, Patrick, and Keith G. Provan. "Towards an Exogenous Theory of Public Network Performance." *Public Administration* 87, no. 3 (2009). 440–456.

Lamb, Christopher. "Global SOF and Interagency Collaboration." *Journal of Strategic Security* 7, no.2 (2013): 8–20.

Milward, H. Brinton and Provan, Keith G. "A manager´s Guide to Choosing and Using Collaborative Networks." *Networks and Partnerships Series*, IBM Center for The Business of Government, 2006.

Morrison, Scott. "Redefining the Indirect Approach, Defining Special Operations Forces (SOF) Power, and the Global Networking of SOF." *Journal of Strategic Security* 7, no. 2 (2013): 48–54.

Ricks, Chuck. "General Themes and Thoughts." *The Role of the Global SOF Network in a Resource Constrained Environment*, The JSOU Press, MacDill Air Force Base, Florida. 2013.

Roberts, Nancy. *Organizational Systems Framework*, 2/2004. Class handout. Network Design Course. Naval Postgraduate School. Monterey, California. 2014

_____. *Network Design Continuum*. Class handout. Network Design Course. Naval Postgraduate School. Monterey, California. 2014

Rubright, Richard, Dr. "A Strategic Perspective on the Global SOF Network: Little Money, Unclear Ends, and Big Ideas." *The Role of the Global SOF Network in a Resource Constrained Environment*. The JSOU Press. MacDill Air Force Base, Florida. 2013.

Szayna, S. Thomas and Welser, William IV. *Developing and Assessing Options for the Global SOF Network*. RAND. 2013.

Thomas, Jim and Dougherty, Chris. *Beyond the Ramparts: The Future of U.S. Special Operations Forces*. Center for Strategic and Budgetary Assessment (CSBA). 2013.

Yoho, Keenan D.; deBlanc-Knowles, Tess; and Borum, Randy. "The Global SOF Network: Posturing Special Operations Forces to Ensure Global Security in the 21st Century." *Journal of Strategic Security* 7, no. 2 (2013): 1–7.

Websites:

Stenberg, Ewa. "Sveriges hemliga krig." [Sweden's secret war]. Dagens Nyheter, [Today's news]. January 25, 2014. http://www.dn.se/nyheter/sverige/sveriges-hemliga-krig/.

McLeary, Paul. "Lawmakers Skeptical of Global Spec Ops Plan." Defensenews.com. August 10, 2013. http://www.defensenews.com/article/20130810/DEFREG02/308100007/Lawmakers-Skeptical-Global-Spec-Ops-Plan.

_____. "Special Ops Nominee Wants Review of SOCOM Initiatives." Defensenews.com. October 11, 2013. http://www.defensenews.com/article/20131011/DEFREG02/310110015/Special-Ops-Nominee-Wants-Review-SOCOM-Initiatives.

_____. "Admiral: Global Special Operations 'Network' To Be Unveiled This Fall," Defensenews.com. June 12, 2013. http://www.defensenews.com/article/20130612/DEFREG/306100023/Admiral-Global-Special-Operations-Network-Unveiled-Fall.

McRaven, William. Briefing (Tampa Conference Center, Tampa, Florida, 14–17 April, 2013) during GEOINT 2013, Symposium. http://geointv.com/archive/geoint-2013-keynote-adm-william-h-mcraven/.

NSNBC International. "Will France and Germany Challenge NATO?" September 22, 2014. http://nsnbc.me/2014/09/22/will-france-germany-challenge-nato/.

Thesis/Dissertation:

Bjørnstad, Anne Lise. "Network Organization Pitfalls and Success Factors for Team and Organizational Processes: Analyses of Key Organizational Variables and Cultural Differences in International Contexts." PhD diss. University of Oslo, Faculty of Social Sciences and Department of Psychology. February 2012.

Gates, Michael E. "Creating SOF Networks: The Role of NATO Special Operations as a Testing Ground for SOF Integration." Master's thesis, Naval Postgraduate School, 2011.

Discussions:

Bradin, Stuart. Colonel (USA, Ret.). International SOF Conference, May 20, 2014.

Holte, Nils Johan. Rear Admiral. Commander NORSOCOM. International SOF Conference, May 21, 2014.

Leahy, Timothy J. Major General, Director of Operations [J-3], USSOCOM. International SOF Conference, May 19, 2014.

McRaven, William H. Admiral, Commander USSOCOM. APAN VTC, July 8, 2014

Miller, William J.A. Director of Strategy, Plans and Policy [J-5], USSOCOM. International SOF Conference, May 19, 2014.

Molin, Urban. Brigadier, Commander SWESOCOM. International SOF Conference, May 21, 2014.

Rachal, Louis. Deputy Current Ops [J-33], USSOCOM. International SOF Conference, May 19, 2014.

Rosengard, Mark. Colonel (USA, Ret.). [J3-I], USSOCOM, International SOF Conference, May 21, 2014.

Sharp, Robert D. Rear Admiral, Director for Intelligence [J-2], USSOCOM. International SOF Conference, May 19, 2014.

Smethurst, Mark. Brigadier, Australian Armed Forces. Deputy Director of Special Operations [Dep. J-3], USSOCOM. International SOF Conference, May 20, 2014.

Webb, Marshall B. Major General, Commander Special Operations Command Europe [SOCEUR]. International SOF Conference, May 22, 2014.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California