NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DEFENSE ANALYSIS CAPSTONE PROJECT REPORT

COOPERATION AMONG NATIONS: UNDERSTANDING THE COUNTER NUCLEAR SMUGGLING NETWORK IN EUROPE

by
Counterproliferation Capstone Team
Ricardo Estrada
Andrew Kochli
Paul Minnie

June 2016

Project Advisors: Leo Blanken
Zachary Davis

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
	June 2016	Capstone project report

4. TITLE AND SUBTITLE
COOPERATION AMONG NATIONS: UNDERSTANDING THE COUNTER NUCLEAR SMUGGLING NETWORK IN EUROPE

5. FUNDING NUMBERS

6. AUTHOR(S)
Counterproliferation Capstone Team Ricardo Estrada, Andrew Kochli, Paul Minnie

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)
Assistant Secretary of Defense, Nuclear, Chemical, and Biological Defense Programs

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)

This research identifies and characterizes a U.S.-centric counter nuclear smuggling network in Europe, and recommends ways to improve its cooperation and effectiveness. The purpose is to provide USSOCOM, NSHQ, and the larger counterproliferation (CP) community with an understanding of how the current network functions, its strengths and weaknesses, and how it can be improved. The research starts by examining prominent theories of international relations to understand cooperation within the network. Afterward, social network analysis (SNA) is used to define the Counter Nuclear Smuggling–Europe (CNS-E) network and characterize its structure. Lastly, the function of the network is assessed using realistic vignettes based upon current threats in Europe.

The results of this research indicate that the CNS-E network is highly decentralized and dense. Cooperation is abundant, though not sufficiently strong to ensure that information is shared. This research concludes by making the following recommendations: 1) The U.S. government should focus on strengthening existing relations, not creating new relations; 2) The network should centralize capabilities and information in regional hubs; 3) USSOCOM and NSHQ should establish strong relationships with law enforcement agencies; 4) USSOCOM and NSHQ can contribute to nonproliferation efforts by conducting threat assessments of European chemical biological radiological nuclear (CBRN) facilities.

14. SUBJECT TERMS	15. NUMBER OF PAGES
weapons of mass destruction, counterproliferation, nonproliferation, social network analysis, nuclear smuggling, Europe, counter-terrorism	115
	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

COOPERATION AMONG NATIONS: UNDERSTANDING THE COUNTER NUCLEAR SMUGGLING NETWORK IN EUROPE

Counterproliferation Capstone Team, Defense Analysis

LT Ricardo Estrada, USN MAJ Andrew Kochli, USA MAJ Paul Minnie, USA

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2016

Reviewed by:
Leo Blanken
Project Advisor

Zachary Davis
Project Advisor

Accepted by:
John Arquilla
Defense Analysis Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research identifies and characterizes a U.S.-centric counter nuclear smuggling network in Europe, and recommends ways to improve its cooperation and effectiveness. The purpose is to provide USSOCOM, NSHQ, and the larger counterproliferation (CP) community with an understanding of how the current network functions, its strengths and weaknesses, and how it can be improved. The research starts by examining prominent theories of international relations to understand cooperation within the network. Afterward, social network analysis (SNA) is used to define the Counter Nuclear Smuggling–Europe (CNS-E) network and characterize its structure. Lastly, the function of the network is assessed using realistic vignettes based upon current threats in Europe.

The results of this research indicate that the CNS-E network is highly decentralized and dense. Cooperation is abundant, though not sufficiently strong to ensure that information is shared. This research concludes by making the following recommendations: 1) The U.S. government should focus on strengthening existing relations, not creating new relations; 2) The network should centralize capabilities and information in regional hubs; 3) USSOCOM and NSHQ should establish strong relationships with law enforcement agencies; 4) USSOCOM and NSHQ can contribute to nonproliferation efforts by conducting threat assessments of European chemical biological radiological nuclear (CBRN) facilities.

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

CBRN	chemical biological radiological nuclear
CIA	Central Intelligence Agency
CIS	Commonwealth of Independent States
CNS-E	Counter Nuclear Smuggling-Europe
COE	centers of excellence
CT	counterterrorism
CTBTO	Comprehensive Nuclear Test Ban Treaty Organization
CTR	cooperative threat reduction
CP	counterproliferation
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOS	Department of State
DTRA	Defense Threat Reduction Agency
EU	European Union
EUROPOL	European Union's Law Enforcement Agency
EXBS	Export Control and Related Border Security
FBI	Federal Bureau of Investigation
FLN	Front De Libération Nationale (National Liberation Front)
FRONTEX	*Frontières Extérieures* (European agency for the management of operational cooperation at the external borders of the member states of the European Union)
GICNT	Global Initiative to Counter Nuclear Terrorism
GMS	global material security
GP	global partnership
GTRI	Global Threat Reduction Initiative
HEU	highly enriched uranium
IAEA	International Atomic Energy Agency
IGO	intergovernmental organization
INTERPOL	International Criminal Police Organization

IS	Islamic State
JSOC	Joint Special Operations Command
LOE	line of effort
NATO	North Atlantic Treaty Organization
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Center
NGO	nongovernmental organization
NIE	new institutional economics
NMS	National Military Strategy
MNC	multi-national corporation
NP	nonproliferation
NSG	Nuclear Suppliers Group
NSHQ	North Atlantic Treaty Organization Special Operations Headquarters
NSOI	Nuclear Smuggling Outreach Initiative
NSS	Nuclear Security Summit
OSCE	Organization for Security Cooperation in Europe
PLO	Palestinian Liberation Organization
PSI	Proliferation Security Initiative
RAM	rational actor model
SELEC	Southeast European Law Enforcement Center
SNA	social network analysis
SOF	special operations forces
UN	United Nations
UNSCR	United Nations Security Council Resolution
USEUCOM	United States European Command
USG	United States Government
USSOCOM	United States Special Operations Command
WMD	weapon of mass destruction
ZANCOM	Zangger Committee

ACKNOWLEDGMENTS

This project could not have been made possible without the valuable input from professors, interagency professionals, and our families. It would be impossible to recognize everyone who impacted our research, but we would like to recognize a few individually. We would first like to thank our advisors and mentors, Dr. Leo Blanken and Dr. Zachary Davis, who are both experts in their field as well as incredible instructors. Your input and dedication to this project were instrumental in translating our ideas into an academic product. We are better students and officers for having worked with you through this process. We would like to thank our sponsors from the Office of the Assistant Secretary of Defense, Nuclear, Chemical, and Biological Defense Programs for bringing us onto the team and giving us the freedom to explore this difficult subject. We would like to extend a special thanks to Director Jim Stokes, Mr. Michael Scott, and Ms. Christina Filarowski Sheaks for your trust and support. We would like to thank Colonel Mike Richardson and the many people at the NATO Special Operations Headquarters who provided us with valuable insight and direction on European security. Additionally, we would like to thank Bill Flesher for his willingness to shed some light on USSOCOM's ongoing partner engagement efforts. We would like to thank the many professors who have influenced our project from the Defense Analysis Department. We would specifically like to thank Dr. Gordon McCormick, Dr. John Arquilla, and Colonel Guy LeMire for their dedication and leadership within the department. Your commitment to the students and faculty of this unique department has made it possible for all of us to become better defense professionals. Finally, we would like to thank our families. Their willingness to support our many travels, meetings, and long hours researching, writing, and editing is truly appreciated.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Islamic State (IS)–inspired terror network that carried out the March 2016 terror attacks in Brussels and the November 2015 attacks in Paris managed to move its members to and from Syria, while planning and executing high-visibility attacks, in spite of sophisticated Western intelligence.[1] Equally disturbing, evidence has recently emerged indicating that the IS cell responsible for the attack had monitored the activity of a senior researcher at a Belgian nuclear facility, while other reports suggest that IS may have interest in acquiring weapons of mass destruction (WMD) material in Iraq and Syria.[2] The Islamic State's apparent interest in WMD terrorism is problematic for Europeans due to Europe being the target of recent attacks, the freedom of movement for individuals within the European Union's Schengen Area, and the massive flow of migrants from the Middle East to Europe.[3] U.S. President Barack Obama has called the possibility of nuclear terrorism "the single biggest threat to U.S. security," while the need to keep the "worst weapons out of the hands of the worst people" is embraced by virtually all Western political leaders.[4] Although IS is not known to have acquired or employed WMDs, the Islamic State's ability to plan and resource sophisticated terror attacks in Europe demonstrates the asymmetric advantage of terror networks over traditional

---

[1] Alicia Parlapiano et al., "The Expanding Web of Connections among the Paris Attackers," *New York Times*, March 18, 2015, accessed April 25, 2016, http://www.nytimes.com/interactive/2015/11/15/world/europe/manhunt-for-paris-attackers.html?_r=2.

[2] Patrick Malone and R. Jeffrey Smith, "The Islamic State's Plot to Build a Radioactive 'Dirty Bomb,'" *Foreign Policy*, February 29, 2016, accessed March 14, 2016, http://foreignpolicy.com/2016/02/29/the-islamic-states-plot-to-build-a-radioactive-dirty-bomb/?utm_source=Sailthru&utm_medium=e-mail&utm_campaign=New%20Campaign&utm_term=%2AEditors%20Picks; Ahmed Rasheed, Aref Mohammed, and Stephen Kalin, "Exclusive: Radioactive Material Stolen in Iraq Raises Security Concerns," Reuters, February 17, 2016, accessed March 14, 2016, http://www.reuters.com/article/us-mideast-crisis-iraq-radiation-idUSKCN0VQ22F.

[3] Keturah Hetrick, "How Bad Would a Radiological Terror Attack Be?" *Defense One*, April 1, 2016, accessed April 30, 2016, http://www.defenseone.com/threats/2016/04/how-bad-would-radiological-terror-attack-be/127188/.

[4] Ashton Carter, "How to Counter WMD," *Foreign Affairs* 83, no. 5 (Sept.–Oct., 2004): 72–13; Alex Spillius, "Nuclear Terrorism Is Gravest Threat to Global Security, Barack Obama Warns," *Telegraph*, April 12, 2010, accessed April 30, 216, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7580210/Nuclear-terrorism-is-gravest-threat-to-global-security-Barack-Obama-warns.html.

intelligence, counterterrorism (CT), and counterproliferation (CP) organizations. This paper, therefore, examines both obstacles to and opportunities for enhanced CP collaboration and cooperation in Europe.

A. THE THREAT

The modern information age has enabled both the growth of terror networks and increased access to WMD material. This potentially catastrophic nexus was partially achieved by the A. Q. Khan network, which enabled Pakistan to gain nuclear weapons.[5] Historically, the few instances of WMD terrorism have been due not to a lack of interest on behalf of terrorists but to the sophisticated technology required to produce such weapons.[6] The threshold to begin proliferation may be lowering, however, due to the prevalence of nuclear, biological, and chemical dual-use technologies, as well as other emerging technologies such as additive manufacturing.[7] Additionally, the numerous means of sharing information in the modern era raise concerns over the ease with which one can transfer intellectual property related to WMD technology. Cumulatively, these changes mean that the traditional pathways to proliferation may now be achieved in fewer steps. Rather than needing to compile several sensitive components that historically only a state could produce, a rogue actor in the near future may acquire the technology and expertise needed to assemble WMDs anywhere in the world.

B. PURPOSE / OUTLINE

To prevent the proliferation of WMDs among terror networks, the international CP community must behave more like a network. The United States' 2015 National Military Strategy (NMS) directs that the United States must "team with multinational and

---

[5] William Langewiesche, "The Wrath of Khan," *Atlantic*, November 2005, accessed March 15, 2016, http://www.theatlantic.com/magazine/archive/2005/11/the-wrath-of-khan/304333/.

[6] Rolf Mowatt-Larssen, "Al-Qaeda's Pursuit of Weapons of Mass Destruction," *Foreign Policy*, January 25, 2010, accessed March 14, 2016, http://foreignpolicy.com/2010/01/25/al-qaedas-pursuit-of-weapons-of-mass-destruction/.

[7] "What Is Additive Manufacturing?" Wohlers Associates, 2010, accessed April 30, 2016, https://www.wohlersassociates.com/additive-manufacturing.html; Jennifer Snow, "Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies" (master's thesis, Naval Postgraduate School, 2015).

U.S. interagency partners to locate, track, interdict, and secure or destroy WMD, its components, and the means and facilities needed to make it, wherever possible."[8] The United States and its allies must therefore form the critical core of a CP network, with intergovernmental organizations (IGOs), nongovernmental organizations (NGOs), and private-sector businesses contributing. Because networked organizations perform better than hierarchies in complex environments, we proceed by examining the modern environment and the difference between networks and hierarchies.[9] Next, we look at the use of networks by terror organizations, as well as efforts by the CT community to behave more like a network post-9/11. We then examine the relationship between the CT and CP communities and recent efforts to foster collaboration between U.S. CP organizations. The implications of U.S.–centric CP studies form the basis of our analysis of the international CP community. Rather than waiting for terrorists to employ WMDs before overhauling the CP enterprise, this paper examines the potential for enhancing the international CP network now.

C. MATCHING ENVIRONMENTS TO ORGANIZATIONAL STRUCTURES: NETWORKS VERSUS HIERARCHIES

The modern information age and associated globalization have led to a rise in complexity for organizations.[10] The difference between complicated and complex environments may appear trivial; however, the distinction is significant for modern organizations. Building an automobile is a complicated process involving numerous specialized steps. Once the model is created, though, it is relatively easy to replicate. Complexity, on the other hand, deals with varied relationships and interactions between many entities, meaning that blueprints or models cannot be used. In complex

[8] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015*, Washington D.C., 2015.

[9] Richard Daft, *Essentials of Organization Theory and Design* (Mason, OH: South-Western/Thomson Learning, 2003); Stanley McCrystal, *Team of Teams* (New York: Penguin, 2015). General McCrystal discusses complexity, networks, and hierarchies in detail. His argument is that the best organizational constructs are dependent upon their environments.

[10] Moises Naim, *The End of Power* (New York: Basic Books, 2013), 2, 54–64. Naim argues that traditionally powerful organizations and individuals are losing their control of power because it is now easy to attain, difficult to use, and easy to lose (2). He cites three revolutions that are enabling this change: the more, mobility, and mentality revolutions (54–64).

environments, like the weather or the stock market, numerous seemingly insignificant actions can collectively have profound effects.[11] Complex environments require organizations to adjust rapidly, causing leaders to delegate decision making to lower levels. As a result, many modern organizations are decentralizing operations in order to deal with international markets, rapid innovation, and lightning-fast communications.

The networks emerging in the information age share certain characteristics that distinguish them from traditional organizations. Modern terror networks can be described as having three characteristics: unspecified and situation-specific communication and coordination systems, linkages between individuals within the network and outside organizations, and relationships that are based on shared values rather than hierarchic authority.[12] In the study of organizational design, the concept of a network is associated with what Henry Mintzberg calls an adhocracy. Adhocracies emphasize direct interaction between highly autonomous and specialized nodes, enabling mutual adjustment between individuals and groups.[13] As all this suggests, modern networks operate in decentralized and flexible manners, without the need for strict organization or state sponsorship. This lack of rigid structure enables collaboration, innovation, and rapid change, making networks ideally suited for complex and dynamic environments.

Modern hierarchical organizations came to prominence in the early 20th century as specialization of labor enabled cheaper manufacturing due to the reduction in transaction costs associated with a shift from decentralized to centralized manufacturing and operations. In the private sector, the work of visionaries like Frederick Winslow Taylor demonstrated that large centralized organizations could standardize work, skills, and outputs through reductionist processes in order to refine the execution of tasks, thus creating great efficiency.[14] In the public sector, the needs of modern warfare demanded

---

[11] McChrystal, *Team of Teams.* See Chapter 3 for more detail on the differences between complex and complicated environments.

[12] Michele Zanini and Sean Edwards, "The Networking of Terror in the Information Age," in *Networks and Netwars*, eds. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 2001).

[13] Henry Mintzberg, "Organization Design: Fashion or Fit?" *Harvard Business Review*, January–February 1981. 10.

[14] Francis Fukuyama, *The Great Disruption* (New York: Touchstone, 2000), 197, 354; McCrystal, *Team of Teams,* Chapter 2.

that nations engage in ever-increasing mobilization, centralization, and application of men and material.[15] The hierarchical organizations that arose from these shifts are typified by a pyramid structure, with a group of leaders on top, several layers of managers and support staff in the middle, and an operating core at the bottom. Naturally, hierarchies take on varying shapes and sizes depending on their intended outputs and outcomes. These include simple structures in the case of small businesses, robust operating cores in the case of manufacturing, and large support staffs for professional bureaucracies.[16] The U.S. interagency structure, primarily built during the Cold War, is an iconic example of a group of organizations that are ideally suited for the complicated but relatively routine affairs of diplomatic engagement (Department of State), intelligence and counterintelligence activities (Central Intelligence Agency and Federal Bureau of Investigation), and preparing to fight the Soviet Army in Eastern Europe (Department of Defense). The hierarchic organizations that dominate big businesses and governments are therefore well suited for certain environments but not for complex tasks outside of their traditional areas of responsibility.

The changes in information management created by the Internet and the information age are enabling networks to grow while creating challenges for hierarchic organizations. In hierarchic organizations, leaders exercise control based on what Max Weber called legal authority, while workers perform tasks for incentives.[17] As numerous authors have pointed out, emerging networks tend to interact based on shared norms and values rather than hierarchical authority or compensation.[18] Additionally, hierarchic systems perform best when leaders manage limited and compartmentalized information; however, the sheer quantity of information flowing in the modern era overwhelms

---

[15] For the case of the U.S., see Sheldon D. Pollack, *War, Revenue, and State Building: Financing the Development of the American State* (Ithaca: Cornell University Press, 2009).

[16] Mintzberg, "Fashion or Fit?"

[17] Max Weber, "The Three Types of Legitimate Rule," in *The Theory of Social and Economic Organization*, trans. A. M. Henderson and Talcott Parsons (New York: The Free Press, 2009), 324; Robert Gibbons, "Incentives in Organizations," *Journal of Economic Perspectives* 12, no. 4 (Fall 1998), 115–17.

[18] Zanini and Edwards, "The Networking of Terror"; Fukuyama, *The Great Disruption*, 194; Shankar Vedantam, "How Terrorist Organizations Work Like Clubs," *Washington Post,* August 4, 2008, accessed March 14, 2016, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080301529.html.

organizations, leading to a need for decentralized control. Perhaps the most fundamental difference is that hierarchies place primacy on efficiency, while networks enable effectiveness. Describing the difference between efficiency and effectiveness in the information age, General Stanley McChrystal wrote, "The Task Force had built systems that were very good at doing things right, but too inflexible to do the right thing."[19] Because of this rigidity in hierarchic structures, networks are better suited for complex environments where spontaneous reaction is preferable to well-deliberated and rehearsed action. Although more power is now being diffused from traditional hierarchic organizations to smaller networked organizations, the modern era still requires bureaucracies.[20] It is how dynamic an organization's environment is that determines which structure is preferable.

D. TERROR NETWORKS AND THE EVOLUTION OF COUNTERTERRORISM

Increased Internet connectivity in recent years has helped terror networks to grow in size, reach, and impact. The earliest terror groups were more hierarchic than the terror networks common today. Traditional hierarchies such as the Algerian National Liberation Front (FLN) and Palestinian Liberation Organization (PLO) gave way to increasingly hybrid groups including Hamas, Hezbollah, and the Islamic State, in addition to pure networks such as al Qaeda. Al Qaeda, which relies less on hierarchic organization than on common ideology, uses Internet connectivity for recruitment, information sharing, and operational planning, all of which can now take place in virtual space. Smartphones, with their various means of communication, also enable groups to coordinate and synchronize activities while remaining physically autonomous from one another. These organizations can then "swarm" and rapidly dissipate, rather than mobilizing and operating in a traditional military sense.[21]

---

[19] McChrystal, *Team of Teams*, 81.

[20] Naim, *End of Power*; Manuel Castells, *The Power of Identity*, 2nd ed. (Malden: Blackwell, 2004), 304.

[21] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars*, eds. John Arquilla and David Ronfeldt (Santa Monica: RAND, 2001).

No cataclysmic event has forced the CP community to integrate, but the attacks on 9/11 did provide the catalyst for a major change in CT organizations. *The 9/11 Commission Report* and other studies revealed that the U.S. national security apparatus was largely stovepiped, meaning interagency collaboration was rare, and limited in its effectiveness to counter terrorist networks. Created during the Cold War, the numerous intelligence, law enforcement, and military components were best suited to counter state-on-state aggression rather than nimble and adaptive networks. Recognizing the asymmetry between U.S. CT organizations and terror networks, John Arquilla and David Ronfeldt recommended in *Networks and Netwars* that governments adopt similar organizational models to their adversaries', because "it takes networks to fight networks."[22] Because governments often cannot, and should not, completely restructure, they instead will have to blend networked processes with existing infrastructure to create hybrid approaches.[23]

The U.S. government began to realize the need to counter terrorism through more networked approaches following the attacks on September 11th, 2001. *The 9/11 Commission Report* recommended numerous U.S. national security reforms, including the creation of unifying offices and a flattening of the interagency. Many of these recommendations were adopted, resulting in the creation of the National Counterterrorism Center (NCTC), the introduction of the director of national intelligence, and unifying of CT efforts in a "network-based information-sharing system that transcends traditional governmental boundaries."[24] By centralizing CT efforts at the NCTC and intelligence activities at the director of national intelligence, the U.S. government (USG) attempted to connect and integrate the interagency community under joint headquarters. Similar to the Department of Defense's Goldwater-Nicholas legislation in 1986, the recommendations of the *9/11 Commission Report* intended to create a joint culture within the intelligence community's interagency. Many of these

[22] Arquilla and Ronfeldt, "The Advent of Netwar," 46.

[23] Arquilla and Ronfeldt, "The Advent of Netwar."

[24] National Commission on Terrorist Attacks, *The 9/11 Commission Report* (New York: M.W. Norton & Company, 2004), 400.

efforts were geared toward streamlining CT operations by centralizing strategic-level collaboration.[25]

Special Operations Forces (SOF), who play a pivotal role in CT activities, have gone to great lengths to foster collaboration at the strategic and operational levels while decentralizing execution at the tactical level. Within the Department of Defense (DoD), the United States Special Operations Command (USSOCOM) is charged with leading the fight against terrorism. SOF, who are uniquely selected, trained, and employed to conduct an array of activities, are better suited for precise operations against terror networks than large conventional forces.[26] With the responsibility of leading U.S. CT efforts, USSOCOM and its subordinate commands have implemented measures to act more like networks.

General Stanley McChrystal, as commander of USSOCOM's elite Joint Special Operations Command (JSOC), recognized the inability of hierarchical organizations to deal with fluid battlefields and enemy networks. He reorganized and removed layers of bureaucracy by flattening JSOC in order to build a team of teams. General McChrystal found that his organization was highly specialized—the best in the world—at individual tasks. Being the best at individual tasks, however, did not always add up to JSOC's being the most effective overall; and it was not winning the fight against terror networks. General McChrystal built a team by forcing independent units to learn the roles, responsibilities, and challenges of those in other parts of the organization. By understanding the other nodes in the network, mid- and junior-level leaders gained a greater sense of purpose and were empowered to take swift and necessary action when appropriate. This ability to rapidly employ forces and share intelligence through coordinated operations and decentralized control enabled JSOC to operate less like a hierarchy and more like a network.[27]

---

[25] National Commission on Terrorist Attacks, *The 9/11 Commission Report*.

[26] Steven Bucci, "The Importance of Special Operations Forces Today and Going Forward," in *2015 Index of U.S. Military Strength*, ed. Dakota Wood (Washington, DC: The Heritage Foundation, 2015), 47–14.

[27] McChrystal, *Team of Teams.*

In addition to USG efforts to collaborate and to fight networks with networks, the international community has made progress in information sharing and CT cooperation. Like the USG, NATO initiated intelligence-sharing reforms following the attacks on 9/11.[28] NATO also established a SOF headquarters (NSHQ) in order to centralize and unify SOF development, coordination, and direction. In an effort to develop its Global SOF Network, USSOCOM built an international operations center called the J3-International (J3I) to facilitate collaboration with worldwide partners. Despite efforts by the USG and international CT communities to cooperate more effectively, the recent attacks in Paris and Brussels reveal that there is still space for improvement.

E. THE NEED FOR A COUNTERPROLIFERATION NETWORK

The threat of terrorists employing WMDs demands cooperation between CT and CP communities that, despite overlapping objectives, are in many cases very different. Originating in the Cold War, nonproliferation treaties were designed to control the spread of nuclear weapons among states. After the conclusion of the Cold War and the dismantling of the Soviet Union, the focus shifted to CP policies that emphasize preventing the spread of nuclear material and technology to rogue states and non-state actors.[29] Post 9/11, the CP community instituted reforms similar to the CT community's, which included creating the National Counterproliferation Center (NCPC) under the director of national intelligence. The nexus of CT and CP challenges was articulated in the Commission on the Prevention of WMD Proliferation and Terrorism's Report, *World at Risk*. The report addressed the threats of nuclear and biological terrorism, recommending significant reforms and additional oversight from the executive and legislative branches of government.[30]

---

[28] Michael Rühle, "NATO Ten Years After: Learning the Lessons," *NATO Review Magazine*, accessed April 30, 2016, http://www.nato.int/docu/review/2011/11-september/10-years-sept-11/EN/index.htm.

[29] "U.S. Counterproliferation Policy," Wilson Center International Security Studies, last modified January 27, 2005, accessed March 15, 2016, https://www.wilsoncenter.org/event/us-counterproliferation-policy.

[30] Bob Graham et al., *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (New York: Vintage Books, 2008).

Recent studies examined the U.S. CP community as a network finding that, despite the U.S. interagency's expansive size and reach, the community faces numerous obstacles to collaboration.[31] These challenges stem from differing perspectives and legal authorities, a lack of incentives to cooperate, and differences in organizational culture. While the division of legal authorities is necessary to run a large bureaucracy, friction can occur when problems spill over into more than one agency's legal jurisdiction. Crosscutting issues such as international terrorism, drug trafficking, and CP are most effectively countered through the skillful cooperation of numerous agencies that cannot achieve success alone, but together can affect the problem. Unfortunately, the interagency lacks a unifying strategy; each agency pursues its own agenda.[32] This means challenges can arise when one agency lacks authorities but wants to act, and an interagency counterpart possesses authorities but lacks incentives to cooperate. Looking at this, it becomes clear that the interagency needs a change of system—agencies must begin to collaborate in advance of a crisis in order to enable cooperation at a critical moment. In other words, they must get in the habit of operating as a network.

Previous research into enhancing collaboration among the U.S. CP community found that informal relationships existed across the interagency but formal hierarchical relationships prevailed during crises. The findings of this work recommended "formalizing the informal" interorganizational relationships that enable the interagency to behave more like a network than a bureaucratic hierarchy. In order to counter organizational culture that is resistant to collaboration, this research found that the best method for collaboration pre-crisis was to create communities of practice that utilize both academic environments and virtual space for collaboration and information sharing.[33]

If we apply the findings from the U.S. interagency study to the international CP community, we find that the international community is far more complex. Rather than

---

[31] Derek Lothringer et al., "Countering Weapons of Mass Destruction: A Preliminary Field Study in Improving Collaboration" (master's thesis, Naval Postgraduate School, 2016).

[32] *Interagency Collaboration: Key Issues for Congressional Oversight of National Strategies, Organizations, Workforce, and Information Sharing,* United States Government Accountability Office, September 2009.

[33] William Cunningham et al., "Too Big to Fail: The U.S. Government Counter Weapons of Mass Destruction Enterprise" (master's thesis, Naval Postgraduate School, 2014).

dealing with one interagency community that resists collaboration, in NATO we find 27 additional interagency communities. Furthermore, numerous intergovernmental organizations (IGOs) must be considered, including NATO itself, the EU, and the EU's law enforcement agency, Europol. In order to consider the international CP community as a network, we must recognize that relationships exist between states, between states and IGOs, and IGO to IGO. Our research aims to better understand these relationships by examining the existing counter nuclear smuggling network in Europe. Over the course of our research, we attempted to address the questions that follow.

F. RESEARCH PLAN

Our research question was: what are the obstacles to cooperation and collaboration in the execution of counter nuclear smuggling efforts in Europe, and how can the established system be improved or better utilized to address the current threats?

Additionally, this work aimed to address the following questions through empirical research:

1. Who are the members of the counter nuclear smuggling network in Europe?
2. What are the characteristics of the Counter Nuclear Smuggling–Europe (CNS-E) network, and which members are most significant?

Through analysis of the CNS-E network, we attempted to answer the following questions:

3. Where do opportunities exist to enhance CP cooperation/collaboration?
4. What are the characteristics or attributes of successful cooperation/collaboration?
5. What is or should be the role of USSOCOM and NSHQ in networking the CNS-E?

We proceed by reviewing literature related to international collaboration. This includes a review of realism, liberalism, and constructivism, as well as models of state behavior. Next, we provide a framework for our data collection and analysis. We provide information on Social Network Analysis (SNA), our data pool, how it was collected, and the attributes utilized to build our network. The third step involves depicting and

describing the network. We highlight significant findings and observations. These findings enable us to draw conclusions and recommendations for USSOCOM, NSHQ, and policy makers in general. The conclusions from our research serve to further understanding of the CP network in Europe and the potentials to enhance this network. Although the products of SNA are not generalizable to other networks, our conclusions regarding CP collaboration are generalizable for the larger CP, special operations, and European communities.

II. REVIEW OF RELEVANT LITERATURE

A. INTRODUCTION

Deeper analysis of the CP efforts in Europe requires preliminary answers to two big questions. First, what is the inherent difference between cooperation in the international environment and within a state? Second, what are the main domestic influencers that can impact international cooperation? To describe the international environment, we explore several prominent international-relations schools of thought: realism, neoliberal institutionalism, and constructivism. Recognizing that international relations is influenced by domestic actors, the second half of this chapter will identify theories that explore how leaders and government institutions make decisions and how those decision impact international cooperation. The theoretical foundation will provide tools with which to analyze counter nuclear smuggling in Europe, explaining the complex international environment and allowing better understanding of international CP efforts.

This theoretical foundation will apply to three main areas of our research. First, the theory informs our bounding of the current network and how we quantified the relationships. Second, the theory provides different lenses with which to interpret the outcomes of our research. Finally, the presented theoretical arguments assist in generalizing the CP findings to the broader international security environment.

B. INTERNATIONAL RELATIONS THEORY

The international environment differs from a state's due largely to the idea of ultimate state sovereignty, which leads to anarchy in the international arena. As Kenneth Waltz describes it, "domestic systems are centralized and hierarchic" while "international systems are decentralized and anarchic."[34] Anarchy typically is defined in international relations as the absence of a higher authority to act as a third party to regulate activity.[35] This creates a situation where states can keep their true intentions private, leading to

[34] Kenneth Waltz, *Theory of International Politics* (McGraw-Hill Inc., 1979): 88.

[35] James D. Fearon, "Rationalist Explanations for War," *International Organization*, 49, no. 3 (Summer 1995): 381.

difficulty communicating true intent and incentivizing active misrepresentation of that intent, which ultimately cause commitment problems between states.[36] The international relations theories of realism, neoliberal institutionalism, and constructivism view the international environment differently and compete with one another to some degree; while they all generally agree that the international system is anarchic, providing challenges to cooperation, the theories disagree on the significance of anarchy to cooperation in the long term. Each of the theories provides a different lens with which to analyze CNS-E. Realism argues that international cooperation is threat based; neoliberal institutionalism contends that cooperation is utilitarian and cost effective to states; and constructivism claims that norms of cooperative behavior can be developed over time.

1. The Realist Outlook on International Cooperation

Having its root in one of the oldest accepted theories of international relations, going back to Thucydides, Thomas Hobbes, and Hans Morgenthau, realism has the most negative view of the potential for extended cooperation. Beyond assuming that the international system is anarchic, realism assumes anarchy gives reason for states to fear each other's efforts to secure their self-interests.[37] State survival is "the most basic motive driving states," and states make rational decisions that seek to maximize their outcomes.[38] States are therefore unable to fully trust any other state, since current friends will become tomorrow's enemies. This unavoidable "security dilemma," a term of art meaning that the actions one takes to improve defenses appear as threatening to others, is a central tenet of realist thought. The centrality of the security dilemma affects the desire and ability of states to cooperate in security matters, especially over long durations. John Mearsheimer argues that states do cooperate, but alliances are problematic to establish and maintain over any length of time because competing state interests eventually lead to policy differences.[39]

---

[36] James D. Fearon, "Rationalist Explanations for War."

[37] Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A Knopf Inc., 1973).

[38] J. J. Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (1994): 10.

[39] Ibid., 12.

From the realist perspective, cooperation is a temporary phenomenon that is possible only to address a shared threat; once the threat is removed, state self-interest will preclude engaging in alliances. The continued adherence to nuclear treaty obligations following the breakup of the Soviet Union is a challenge to typical realist arguments. However, the self-interested actions of Russia in 2014 and the ongoing debate about the United Kingdom's participation in the EU indicate that state self-interest continues to play a role in European international engagements, especially as the balance of power seems to be shifting away from a unipolar system.

2. Neoliberal Institutionalism: A More Optimistic View

Another major theory in international relations is neoliberal institutionalism. Neoliberals have a positive view of the potential for cooperation, basing their arguments on the writings of Enlightenment thinkers in the tradition of Rousseau and John Lock and classic liberal economic theorists such as Adam Smith. Neoliberal institutionalists assume states make rational choices and believe those choices lead states to "[abandon] independent decision making in favor of joint decision making."[40] This capacity for overcoming pure self-interest in favor of community good leads to a belief in commonly held norms and institutions and therefore in the efficacy of international regimes in shaping state behavior. Neoliberal institutionalists believe that international institutions perform three main functions that increase the likelihood of international cooperation: changing the payoff structure to increase mutual interest, increasing the time horizon of interactions, and mitigating the problem of free riders as the number of parties increases.[41] Thus, cooperation builds on itself and lessens the risks of collective action.[42]

[40] Arthur A. Stein, "Coordination and Collaboration: Regimes in an Anarchic World," in *International Regimes,* ed. Stephen D. Krasner (New York: Cornell University Press, 1983), 132.

[41] Kenneth A. Oye, *Cooperation under Anarchy* (Princeton: Princeton University Press, 1986).

[42] For a more in-depth discussion, see Keohane and Martin (1995); Krasner (1983).

3. Constructivism: Building Cooperative Potential

Constructivism takes a middle view on cooperation in the international environment, arguing that commonly held norms of society can impact the acceptance of international cooperation, especially over time. World order, constructivists contend, is a work in progress determined by historic patterns that shape a state's image of itself and others, and it can therefore be reimagined as norms change. This argument allows states to become less self-interested and more cooperative based on the establishment of shared norms over time. Domestic social norms also add complexity to the system by determining the limits of acceptable behavior in bargaining—domestic norms impact a state's behavior in the international environment.[43] All this makes anarchy a secondary consideration; Alexander Wendt argues that "anarchy is what states make of it."[44] Social structure, not anarchy, is the primary factor that determines the level of cooperation or conflict within the international system: an "anarchy of friends differs from one of enemies."[45]

Constructivism can help explain the change in cooperative potential of the international environment over time, both positive and negative. Soon after the development of nuclear weapons, Europe developed a shared belief in collective security as the way to prevent another world war. Constructivism would contend that the shift in the social structure established an environment of cooperation, not self-interest; the social structure of perceived friends enabled the development of the European Union, its affiliated institutions, and the CP treaties and regulatory institutions. Conversely, change in the social structure also has the potential to shift away from cooperation as states see others as threats. The level of internalization of cooperative norms could explain the varying views of the current world order, for example Russia acting in its perceived self-interest while Germany continues to act cooperatively.

---

[43] Lawrence Freedman, *Deterrence* (Malden: Polity Press, 2004), 69–70. For additional information on domestic social norms, see Katzenstein (1996); Gray (1999).

[44] Alexander Wendt, "Constructing International Politics," *International Security* 20, no. 1 (Summer 1995): 77.

[45] Ibid., 77–78. For a more in-depth discussion, see Wendt (1994); Wendt (1995); Adler (1997); Copeland (2000).

C. DOMESTIC INFLUENCES ON INTERNATIONAL COOPERATION

In the interconnected environment of the 21st century, states are not unitary entities interacting at a single point of contact. There are a number of influencers within each state that can impact cooperation in the international arena. Collectively, these cooperation nodes create an interconnected web of communication between and among states. Relevant to CP efforts are two domestic players that influence a state's international cooperation: leaders and government institutions.[46] The different domestic influences that have bearing on international cooperation must be taken into account by those attempting cooperative CP endeavors. Domestic actors can trigger internal pressures, making cooperation much more difficult.

1. Leaders: Cognitive Limitations to Rational Decision Making

Leaders of states have an obvious impact on the trajectory of the states they represent, so it is important to recognize the cognitive limits of state leaders and how they impact leaders' willingness to cooperate in CP efforts. Historically, the rational actor model (RAM) has been used to explain and predict how individuals and states act in their own self-interest with consistent and stable preference orderings to determine optimal outcomes based on available options.[47] Bounded rationality, however, recognizes that individuals are not able to identify and process all of the applicable data to make fully rational decisions. Research in bounded rationality asserts that leaders rarely have complete or certain information, and even if they do, they are unable to process the amount of information that leads not to optimal solutions but to satisfactory ones.[48]

Prospect theory contends that states that are happy with the status quo, known as being in a gains frame, are generally risk adverse, while states that are unhappy with the

---

[46] Austin Long, *Deterrence from Cold War to Long War: Lessons from Six Decades of RAND Research* (Santa Monica: RAND, 2008), 57–58.

[47] Herbert A. Simon, "Rationality in Political Behavior," *Political Psychology* 16, no. 1 (March 1995): 48.

[48] Herbert A. Simon, "Human Nature in Politics: The Dialogue of Psychology with Political Science," *American Political Science Review* 79, no. 2 (June 1985).

status quo, known as being in a losses frame, will be more risk acceptant.[49] The leaders in Europe tend to be content with the status quo and therefore are unlikely to risk participation in proliferation activities. Analyzing leaders' frames of mind could help explain the variation in behaviors toward the established CP institutions. Leaders that are unhappy with the status quo and not seeing the benefits of adhering to the CP norms of behavior may be more risk acceptant and risk proliferating nuclear programs, as was the case with Muammar Gaddafi and Saddam Hussein.

2. Government Institutions: Structural Impacts on Cooperation

Because of the complexity of an interconnected international environment, implementing proposed international-cooperation efforts requires interaction beyond individual leaders. Broader government institutions affect the international arena, both directly and indirectly. There are many theoretical approaches that seek to describe the effects of these organizational decision-making processes on cooperation. We will discuss three that each provide a different way to understand the network of international relationships in Europe: the organizational behavior model, the bureaucratic politics model, and new institutional economics theory.

Organizational behavior models describe the state itself as a complex organization that produces outputs, rather than clear choices as the RAM suggests. Organizational models suggest that the head of state alone does not make decisions; instead, a robust structure of specialized organizations contributes to the leader's understanding and decision making. Organizational models emphasize that numerous factors, including structure, technology, culture, and the environment, all influence an organization's output.[50] The combined effect of these factors can result in outcomes that differ from the leaders' and decision makers' original intent.[51] One can look at CP efforts in Europe as a system through this model and determine if the structure fits the environment. By

[49] Jeffrey D. Berejikian, "A Cognitive Theory of Deterrence," *Journal of Peace Research* 39, no. 2 (March, 2002): 170–171. For further discussion of prospect theory, see Kahneman and Tversky (1979); Tetlock and Mellers (2002); Berejikian (2002).

[50] Mintzberg, "Fashion or Fit?"

[51] For additional information, see Allison and Zelikow (1999); Mintzberg (1981); Sathe (1983); Robbins and Judge (2013).

analyzing the organizational structure, technology, culture, inputs, and outputs the model provides a way to judge effectiveness of the CP system in Europe.

The bureaucratic politics model emphasizes the competing motives of organizations, or bargaining games, rather than the outputs of organizational behavior. The bureaucratic politics model assumes that each suborganization within a state government has its own self-interests which affect how the suborganization thinks and acts.[52] Viewing the state as an organization with limited resources, suborganization leaders must consider how their actions affect national, organizational, and personal goals.[53] Foreign policy, therefore, is often the result of personal bargaining and compromising rather than rational debate.[54] This model is useful when analyzing the complex domestic stakeholder struggles that take place when seeking to execute international CP initiatives. When Germany engages with Poland on instituting CP policy, they have both internal stakeholders that will complicate their ability to cooperate; understanding who the powerful stakeholders are and how they impact decision making can be helpful when bargaining in the international arena.

New institutional economics (NIE) is a broad theory that argues that economic and political institutions mutually impact each other and must be studied together to conduct comparative polity analyses.[55] Democratic peace theory, one subset of NIE, contends that higher political and economic freedom reduces potential conflict between states of similar structure.[56] Selectorate theory, another subset of NIE, postulates that state leaders' decisions are determined not by the best interest of the state but by a desire

---

[52] Graham T. Allison and Morton H. Halperin, "Bureaucratic Politics: A Paradigm and Some Policy Implications," *World Politics* 24 (Spring 1972).

[53] Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999), 255.

[54] For additional information, see Kant (2006); Allison and Zelikow (1999); Allison and Halperin (1972).

[55] Oliver E. Williamson, "The New Institutional Economics: Taking Stock, Looking Ahead," *Journal of Economic Literature* 38, no. 3 (September 2000); Jeffrey S. Banks and Eric A. Hanushek, introduction to *Modern Political Economy: Old Topics, New Directions*, eds. Jeffrey S. Banks and Eric A. Hanushek (New York: Cambridge University Press, 1995).

[56] Zeev Maoz and Nasrin Abdolali, "Regime Types and International Conflict, 1816–1976," *Journal of Conflict Resolution* 33, no. 1 (March 1989).

to remain in power;[57] therefore, the structure of the government, whether democratic or autocratic, affects cooperation potential.[58] Audience cost, too, can play a role in predicting state cooperation, democratically elected leaders find it easier to signal private intentions and commit to a course of action, since the electorate will punish them in the future for not following through on commitments. Authoritarian leaders, conversely, suffer more limited audience cost by not adhering to commitments, which leads authoritarian leaders to be less credible in international bargaining.[59] The various elements of NIE theory provide multiple tools with which to analyze the countries in Europe.

Through these different models, it may be possible to determine which countries are more likely to cooperate in CP efforts and which to oppose efforts based on the structures of their domestic political and economic institutions. Many of the entrance requirements of the EU and the North American Treaty Organization (NATO), for example, are efforts to democratize the allied states to facilitate future cooperation in CP as well as in security and economic initiatives. As the NIE theories indicate, states with democratic political policies and liberal economic policies tend to negotiate instead of go to war, leaders are held accountable for actions to a broader population, and audience cost facilitates communication of truthful intent, all of which facilitates cooperation.

D. CONCLUSION

Many different schools of thought can be useful when considering cooperation in the international arena. International relations theories provide different ways to view the system and to analyze past, present, and future interactions. Looking at the ways in which domestic influences impact international relations provides additional tools to understand how the interconnected nature of the current system impacts cooperation. The realities of Europe in the early 21st century seem to exhibit evidence of many of the schools of

[57] Bruce Bueno de Mesquita, "Domestic Politics and International Relations," *International Studies Quarterly* 46, no. 1 (March 2002): 4.

[58] For a more in-depth discussion of selectorate theory, see Morrow et al. (2008); Bueno de Mesquita and Smith (2011).

[59] James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88, no. 3 (September 1994): 587.

thought. Self-interests, international institutions, established norms of international behavior, leadership personalities, and differing bureaucratic politics combine to create a complex environment.

Our research will utilize these analytical tools as we seek to describe the international CP environment in Europe. The theoretical principles described in this chapter are instrumental in informing the bounding of the network as well as in selecting and quantifying the relational links within that network. Additionally, the theoretic arguments provide different lenses with which to interpret the outcomes of our quantitative and qualitative research. Finally, the presented theory will inform the generalization of our findings regarding the CNS-E network to the broader international security environment. The following chapters will first conduct a quantitative analysis of the CNS-E utilizing social network analysis methodologies and then conduct a qualitative analysis utilizing counterfactual cases. Both methodologies will be informed by the international and domestic theory discussed in this chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE COUNTER NUCLEAR SMUGGLING–EUROPE: NETWORK ANALYSIS

A. INTRODUCTION

This chapter is focused on the social network analysis (SNA) conducted on the Counter Nuclear Smuggling–Europe (CNS-E) network. SNA provides a collection of methods useful for studying the structure and function of networks. The first section discusses how the network was constructed—how the boundaries were defined, what relationships were measured, and how data was collected. The second section discusses the analysis of the CNS-E network and various subnetworks. The findings indicate the CNS-E network can be considered an organic structure, decentralized, relatively informal, and highly dense.[60] This configuration is generally well suited for the CNS-E network's task and operating environment. While state-bilateral relations account for the majority of ties in the network, the graphs and metrics clearly indicate regional IGOs are the most effective institutions for facilitating strong relationships.

B. SECTION I: CONSTRUCTING THE NETWORK

1. Bounding

The first challenge in defining a network is establishing its boundaries. The realist and nominalist strategies are two methods of deciding who fits within a network. The realist strategy allows actors within the network to identify others members and is a more subjective approach. The nominalist strategy allows the researcher to bound the network according to the requirements of the research.[61] We used a combination of the two strategies to build the CNS-E network.

Starting with a nominalist strategy, we narrowed the scope of the network to fit the research question regarding counter nuclear smuggling in Europe. Consequently, we

---

[60] Steven McShane and Mary Von Glinow, *Organizational Behavior* (McGraw-Hill Higher Education, 2012), 238.

[61] Sean F. Everton, *Disrupting Dark Networks*, vol. 34 (New York, NY: Cambridge University Press, 2012).

started with a geographic and functional boundary. From this point, we considered which type of actors or stakeholders had the most immediate impact on the issue of counter smuggling, including states, IGOs, and substate agencies. All European states were included, less the microstates, as they are the primary stakeholders in the network. The U.S. was included because the research is primarily intended to support U.S. countersmuggling efforts. Significant international government, military, and law enforcement organizations were included based on perceived influence on the network. Regarding the inclusion of U.S. agencies and programs, selection was largely determined by drawing from a 2014 congressional report *The Evolution of Cooperative Threat Reduction: Issues for Congress.*[62] Other U.S. military and law enforcement nodes were included to fit the focus of the research and based on their perceived influence on the network.

From this starting point, we then applied a realist approach (not to be confused with international relations realism) to our research by using material provided by actors to identify other important actors, such as by looking at an actor's working agreements or strategic partnerships. This led to the inclusion of some actors and validated the presence of others. Given the immense potential size of a CP network, we also excluded numerous types of actors like universities, corporations, influential individuals, and others whom we assessed fell below the threshold of influence for CP decision making and operational capability.

There are three broad types of actors that comprise the CNS-E network; state actors, intergovernmental organizations, and substate agencies/ programs (Table 1).

[62] Mary Beth Nikitin and Amy F. Woolf, *The Evolution of Cooperative Threat Reduction: Issues for Congress* (Congressional Research Service, 2014).

Table 1. CNS-E Network Actors by Type

States		IGOs	Sub-State Agencies/ Programs
Albania	Lithuania	CIS	DHS CSI
Armenia	Luxembourg	CTBTO	DoD DTRA
Austria	Macedonia	EU	DoD EUCOM
Azerbaijan	Malta	G7 GP	DOE GTRI
Belarus	Moldova	GICNT	DOE GMS
Belgium	Montenegro	IAEA	DOS EXBS
Bosnia and Herzegovina	Netherlands	Interpol	DOS NSOI
Bulgaria	Norway	NATO	EU CBRN COE
Croatia	Poland	NSS	Europol
Cyprus	Portugal	NSG	FBI
Czech Republic	Romania	OSCE	FRONTEX
Denmark	Russia	PSI	
Estonia	Serbia	SELEC	
Finland	Slovakia	UNSCR 1540 COM	
France	Slovenia	UN	
Georgia	Spain	ZANCOM	
Germany	Sweden		
Greece	Switzerland		
Hungary	Turkey		
Iceland	Ukraine		
Ireland	United Kingdom		
Italy	United States		
Latvia			

2. Relationships

Relational data makes up the structure of a network and is considered the most important factor in determining behavior.[63] There are two distinct sets of relations in the

63 Alexandra Marin and Barry Wellman, "Social Network Analysis: An Introduction," in *Handbook of Social Network Analysis*, eds. Peter Carrington and John Scott (London: Sage, 2010).

CNS-E network. The first set describes bilateral state relations. The second set describes non-state bilateral relations and non-state to state relations.

The bilateral state relationships analyzed in the network were selected using elements of national power known as DIME (diplomatic, information, military, economic).[64] We elected to forgo collecting data specific to the information element due to the difficulty quantifying it individually as well as the understanding that information plays a role in each of the other elements' power.[65] To keep the data relatively consistent, we used common country reports from a single source. The relational data that was collected is from a fixed report date and subject to change with the dynamic international environment. The existence of the European Union (EU) complicates the quantification of bilateral relations within Europe, as it is a non-state actor that has significant influence on its member states' policies and so blurs the categorical distinction. In an effort to take the prominence of the organization into account while also recognizing the fact that the member states have individual foreign policies, we established a standardized metric to judge the cooperative mechanisms in place. Membership in the EU inherently increased bilateral relations between member states, especially in the economic realm, but did not preclude differentiation in relations between members or with non-members.[66]

To measure the diplomatic element, we identified the existence of diplomatic engagements, the level of cooperation displayed by heads of state, and the existence of diplomatic disagreements. States were assumed to have normal relations with the other states unless there was a particular area of conflict or positive relation indicated in the report. In measuring the military element of national power, we looked at the level of shared military equipment, the presence of foreign forces, the existence of security agreements, participation in combined exercises, foreign military or police training

64 Alan G. Stolberg, "The International System in the 21st Century," in *U.S. Army War College Guide to National Security Issues: Volume II – National Security Policy and Strategy*, ed. J. Boone Bartholomees (Carlisle Barracks: Strategic Studies Institute, 2012), 144.

65 John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica: RAND, 1999), 55–62.

66 Christopher Hill and William Wallace, "Introduction: Actors and Actions," in *The Actors in Europe's Foreign Policy*, ed. Christopher Hill (New York: Routledge, 1996); Ian Manners and Richard Whitman, conclusion to *The Foreign Policies of European Union Member States*, eds. Ian Manners and Richard Whitman (Manchester: Manchester University Press, 2000).

programs, and the existence of open military conflict. Given that the modern environment requires international cooperation to address shared security risks which are at times more appropriate for police forces,[67] both military and police foreign engagement were considered part of the military element of national power. Economic relations were determined based on three main ties: major economic trading partners, the existence of free trade agreements, and international sanctions. Relations between all EU members were automatically considered strong due to the established free trade agreements, shared borders, and other economic incentives in place throughout the EU.

Each of the elements of national power was scored independently, and an aggregate score was then determined to represent the overall relationship between states, with equal weight given to each element. The final process in determining the bilateral relational scores involved taking the average relation between states, which symmetrized the data. This was necessary because the non-state data was symmetrical. In order for both sets of data to be combined into a one-mode network all data had to be symmetrical.

The bilateral non-state and non-state to state relations were selected upon observing the type of cooperation necessary for the network to carry out its purpose. These include typical functions of international police organizations.[68] The relevant types of relation are membership/participation, operational cooperation, and information sharing. Membership/participation describes a state's commitment to a non-state actor. The level of commitment was measured using two criteria. The first measured a state's status with a non-state actor—a member, observer, or participant. The second focused on the strength of relation gained from participation. For instance, a membership in the EU was judged to produce a stronger tie than participation in the CTBTO.

Operational cooperation broadly describes a relationship of partnered activities, be they training, support, or partnered operations. It is measured based on the perceived

---

[67] David H. Bayley and Robert M. Perito, *The Police in War: Fighting Insurgency, Terrorism, and Violent Crime* (Boulder: Lynne Rienner Publishers, 2010); Terrence K. Kelly et al., *A Stability Police Force for the United States: Justification and Options for Creating U.S. Capabilities* (Santa Monica: RAND Corporation, 2009).

[68] Hikmet Yapsan, *International Police Cooperation on Countering Transnational Terrorism* (2012), 3.

level of cooperation needed to conduct those activities. Examples of operational cooperation include training conducted by DOS NSOI, inspections conducted by the IAEA, or multilateral peacekeeping operations by the OSCE. This relation seeks to differentiate non-state actors that have an operational role from those that solely offer best practices.

Lastly, information sharing describes the sharing of sensitive or operational information. This is perhaps the most important relationship for this network to be effective. Transnational problems inherently require information sharing across borders. The strength of information sharing was measured based on three questions. First, is information sharing a primary task of the non-state actor? Second, does the non-state actor have information-sharing systems? Third, how effectively is information shared? All three relations were graded on the same scale and then aggregated to get an overall relationship strength.

Relational data presented two challenges for building the network, which largely stemmed from the different actor types within the network. First, the actors lacked a common set of relations. Second, the data collected was a mix of symmetrical and asymmetrical. It was necessary to represent multiple actor types in a one mode network so that the whole CNS-E network could be analyzed. To overcome the lack of common relations, two sets of relations were examined. To ensure equal weighting of the relations, the same scale was used for all relations. To overcome the mix of data, all bilateral state data were made symmetrical (by averaging) to match the non-sate data.

3. Data Collection

Data collection was divided into two efforts and conducted over two months. State-to-state relations were gathered almost entirely from IHS Jane's country reports. A score for each node was coded into a 72 x 72 one-mode matrix. Each relation was coded on a separate spreadsheet and then aggregated into one matrix. This produced the bilateral state relations matrix. Relations between states and non-state actors were gathered from a combination of official websites, articles, and government reports. The scores were coded for each node in a two-mode matrix. Each relation was coded on a

separate spreadsheet and then aggregated. This produced a 27 x 72 two-mode matrix for state to non-state relations. The two aggregated matrices were then combined to produce the compiled one-mode matrix used for the CNS-E network.

C. SECTION II: CNS-E ANALYSIS

1. Analysis Overview

The analytical framework applied to the CNS-E network evaluates three key aspects of a network: content, composition, and structure.[69] This framework parts from the strict structural analysis common in SNA by also considering other important factors like environment and context. The advantage of this approach is a wider accounting of factors that influence the network, which leads to a more thorough understanding of the network and an increased ability to identify problems and solutions. The content of a network includes its purpose and the environment in which it operates. The composition includes the actors in it and the relations that make up the ties between those actors.[70] The structure includes a variety of metrics illuminating two key characteristics: density and centralization. These structural characteristics largely determine the organizational configuration of a network, which determine what it will be good (or bad) at accomplishing.

In addition to the key aspects of the CNS-E network, four subnetworks are extracted for analysis. These subnetworks are differentiated by lines of effort (LOE) that correspond to the range of CP/NP activities. The LOEs are divided as follows: LOE 1, contain nuclear material; LOE 2, prevent transnational shipment of nuclear material; LOE 3, secure borders; LOE 4, interdict nuclear material. Reducing CP/NP activities into lines of effort allows for a more detailed analysis of the whole network. This approach lets us identify key actors across the range of CP/NP activities, which actors are involved in multiple activities, and the lines of communication necessary to track an incident from LOE 1 to LOE 4.

---

69 Deborah E. Gibbons, “Social Networks” (PowerPoint Slides, Naval Postgraduate School, 2016).

70 Ibid.

2. CNS-E Network

The CNS-E network comprises 72 nodes including states, substate agencies/programs, and international governmental organizations (Figure 1). There are two sets of ties in the network. The first set defines *state-to-state* relationships. The second set defines *state-to-non-state* and *non-state-to-non-state* relationships. As we have discussed, state-to-state ties are aggregated from three relations—diplomatic, economic, and military—and state-to-non-state ties are aggregated from three different relations—membership/participation, operational, and intelligence sharing. All relations are weighted the same. The majority of ties between states and non-states is due to membership/participation, followed by operational, and finally information sharing. The Counter Nuclear Smuggling–Europe network sociogram depicted in Figure 1 shows the whole network. The ties represent overall aggregated relationship scores. The nodes are colored by type: blue are states, red are IGOs, and black are substate agencies/programs. Each node is sized by its overall betweenness; a measure of network centrality that will be discussed later in this section.

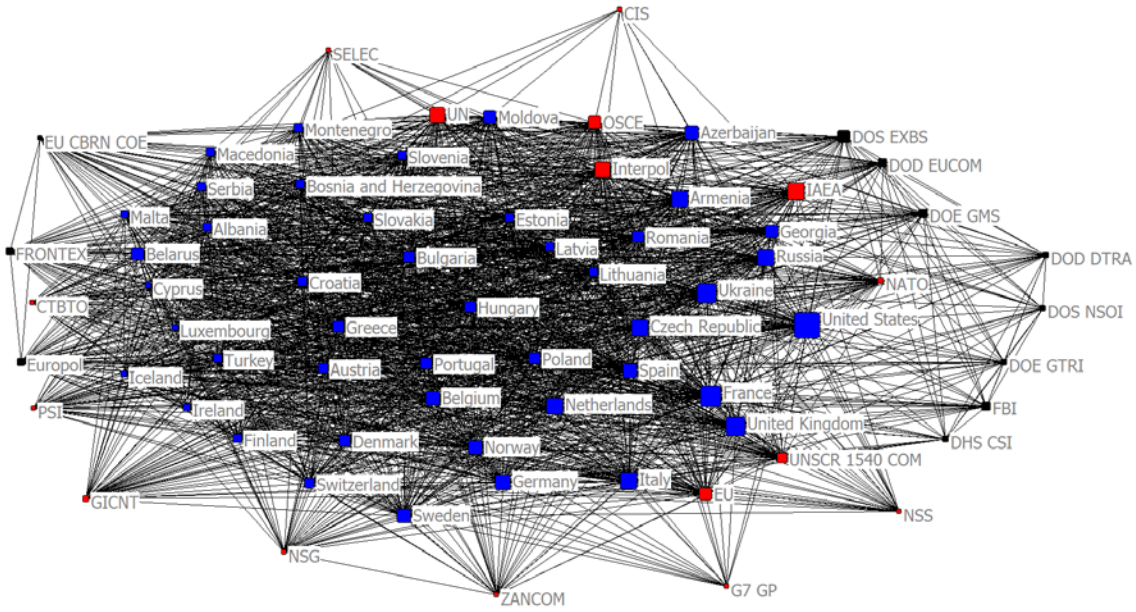

Figure 1. The Counter Nuclear Smuggling–Europe Network

Analyzing a network's content is critical to understanding its effectiveness. Network configurations are not inherently "good" or "bad," but have a good or bad fit according to their purpose and environment.[71] A highly centralized structure may be effective for an infantry platoon but completely ineffective for a marketing firm. Looking at the CNS-E network, its purpose is to prevent the smuggling of nuclear material with an end state of avoiding an unconventional nuclear attack, and it operates in an environment that can be characterized as complex, dynamic, and anarchic.

A complex network has many external variables influencing its outcome,[72] and the international environment, nuclear security, border security, intelligence, state relations, and enemy capabilities are just a few of the variables that influence the CNS-E network's performance. Many of the same variables cause the environment to be dynamic; that is, capable of rapid change.[73] The international environment, as a variable, is itself subject to rapid changes; take, for example, the sudden rise of ISIL in the Levant and its destabilizing effects in Syria and Iraq. The diffusion of technology has rapidly changed enemy—specifically non-state actors'—capabilities, forcing the CNS-E network to adapt. These two examples illustrate a small part of the environment's dynamism. The last characteristic of the CNS-E network's environment is the inherent anarchy that defines international politics.[74] There is no higher authority that has control or dictates the actions of the network. While some actors are more influential than others, the majority of actors in the CNS-E network make their own decisions, driven largely by their own interests. This absence of an executive or central authority makes the CNS-E network particularly interesting in organizational study, since existing work on CP network analysis is situated within a single state's authority.[75] This must be considered alongside the network's purpose and environment when analyzing its structure and effectiveness.

---

[71] Mintzberg, "Fashion or Fit?"

[72] McShane and Von Glinow, *Organizational Behavior*, 244.

[73] Ibid.

[74] Kenneth Neal Waltz, *Theory of International Politics*, (1979), 88.

[75] Cunningham et al., "Too Big to Fail."

The structure of the CNS-E network can be characterized as highly dense. Density reflects how connected a network is by dividing the actual number of ties by its potential number of ties.[76] The CNS-E network has a density score of .745, which means three-quarters of all potential ties are present in the network. This is abnormally high for a network of this size, as density tends to be inversely correlated to network size. Visually, the CNS-E network sociogram confirms that the network is highly connected; however, the connectedness is not evenly dispersed. The state nodes form a dense cluster, indicating they have more ties with one another than with non-state nodes. In fact, relations between state nodes are pervasive, even between states that are seemingly at odds. Density has several influences on a network. The more connected a network is, the more likely actors are to conform to norms and appropriate behavior. In part, this is because influence and accountability increase with additional ties.[77] For the CNS-E network, high density should translate into actor compliance with network norms. Therefore, the network should generally achieve compliance with widely accepted practices on CP/NP issues like nuclear facility security and safety, export control measures, and participation in NP/CP IGOs. This may help explain why there is such widespread participation in IGOs like the IAEA and treaties like PSI.

Density bestows two additional traits on networks: diffusion and resilience. Generally, a dense network can diffuse things, like information, faster than a sparse network.[78] Dense networks tend to be more compact, meaning the average distance between nodes and distance from one side of the network to the other (diameter) is shorter than in sparse networks. The ability for information to travel from one node to any other node in the CNS-E network within a few walks should significantly increase the network's effectiveness. A high degree of connectedness also increases a network's resiliency, because of the presence of multiple pathways between nodes.[79] In other words, removing one node will not fragment the network or stop transmission to any other node.

---

76 Robert A. Hanneman and Mark Riddle, *Introduction to Social Network Methods*, PDF ed. (Riverside, CA: University of California Riverside, 2005), 98.

77 Everton, *Disrupting Dark Networks*, 10.

78 Hanneman and Riddle, *Introduction to Social Network Methods*, 99.

79 Valdis E. Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24, no. 3 (2002): 43–52.

This is a tremendous benefit for the CNS-E network, as information sharing is a critical task. If the United Kingdom needs to pass sensitive information to Bulgaria, it can expect to have reliable communication through one of many paths. If bilateral relations are not strong enough, the UK can pass information through the EU, Europol, Frontex, NATO, or the OSCE.

The structure of the CNS-E network can also be characterized as decentralized. Centralization describes the power or influence distribution throughout a network.[80] Highly centralized networks concentrate power in one or several nodes. In contrast, decentralized networks disperse power throughout numerous actors. While there are actors in the CNS-E network that have more power and influence than others, most nodes retain a significant degree of power. This makes sense given that most nodes are sovereign states or IGOs that do not answer to a higher authority. Similar to actor centrality, centralization can be measured with different metrics depending on what constitutes power in a particular network.[81] In the CNS-E network, centralization is measured by degree and betweenness.

Degree centralization considers the number of ties an actor has as a reflection of power. The logic follows that the actor with the most ties has the most opportunity and is the least constrained.[82] In other words, more ties equal more channels of transmission. In the CNS-E network, nodes like the U.S. and Germany will likely have more power in the network because they have more connections than nodes like Belarus. The network level score is a percentage of degree inequality compared to the theoretical maximum of a perfectly centralized star network.[83] The CNS-E network has a degree centralization score of 21.93%. Roughly, this means power by degree is one-fifth as concentrated as it is in a star network. However, another metric indicates the network is more decentralized than this score may suggest. There is a significant range of degree centrality scores

80 Hanneman and Riddle, *Introduction to Social Network Methods*, 146.

81 Everton, *Disrupting Dark Networks*, 11–13.

82 Hanneman and Riddle, *Introduction to Social Network Methods*, 146.

83 Ibid., 150.

between the nodes, with CIS having 10 ties and the United States having 68 ties. This range increases the variance, moving it closer to the idealized network.

Betweenness centrality considers an actor in a position of brokerage, meaning that actor connects two nodes by the shortest path (geodesic), as having power.[84] Brokers control the flow of whatever the network is transmitting, be it friendship or information, and pass it to otherwise isolated nodes. The more isolated a node, the more power a broker has. Betweenness centralization is calculated by looking at how many geodesic paths between all node pairs travel through a given node. The network score is again given as a percentage of the theoretical maximum for a star network of the same size.[85] The CNS-E network shows a tiny .86% betweenness centralization score, indicating extreme decentralization. This makes sense given the mean ties per node is 52.8 out of a possible 71. So the average node is connected to three-quarters of the network without an intermediary.

This highly decentralized type of network is called a flat organization or heterarchy.[86] While many heterarchies still have authority figures, there is no central authority in the CNS-E network. The structure of the CNS-E network has many implications for its function, including several major advantages. The foremost advantage for the CNS-E network is the capacity to share information. Knowledge can originate in any part of the network and flow in multiple directions to rest of the network.[87] Considering the CNS-E network's environment, this capacity for timely transmission is crucial to effectively counter smuggling. For instance, Frontex can simultaneously notify multiple actors across the network if they discover ongoing smuggling, instead of reporting up a chain of command and waiting for the information to flow back down to relevant actors. In a highly centralized hierarchy, information tends to travel vertically, making information sharing through the network slow. This type of communication would not be effective for the CNS-E network.

---

84 Everton, *Disrupting Dark Networks*, 13.

85 Hanneman and Riddle, *Introduction to Social Network Methods*, 150.

86 Everton, *Disrupting Dark Networks*, 141–142.

87 McShane and Von Glinow, *Organizational Behavior*, 238.

Another advantage of decentralized systems is flexibility to deal with complex environments.[88] As we have discussed, complex environments are characterized by how many variables affect the outcomes of the network. In this type of environment, there are too many critical factors for any one authority to control. Decentralized networks, by widely distributing power, allow critical issues to be addressed by the actors most affected by a particular variable. Highly decentralized networks also tend to have less formalized rules and procedures. This is certainly true for the CNS-E network. The upside of decentralized, less formalized networks, also called organic structures, is adaptability.[89] Organic structures quickly adapt to changing environments precisely because they lack formalized rules on how they must deal with problems. State actors in the CNS-E network do not follow a set of international standard operating procedures when they are confronted by nuclear smuggling. States can adapt to threats however they deem necessary. This benefits the network in that a central node does not have to assess each actor's unique vulnerabilities and issue SOPs for how to deal with them. This would be not only inefficient but ineffective as well.

Microlevel analysis of the CNS-E network struggles to reveal much useful information about the power of individual actors. The density and decentralization of the network mean there are many well-connected actors and power is distributed among them. The most distinctive centrality measure, though, is betweenness. The United States has the highest (normalized) betweenness centrality score, 1.215 compared with a mean score of .366. However, the inclusion of numerous U.S. agencies makes this a U.S.-centric CP network, contributing to its central position. It may be more enlightening to look at the next most central actors, which are France (1.006), the United Kingdom (.909), and Ukraine (.895). Though these are very low centralization scores, they are significantly higher than the mean. Consequently, these actors are in the best positions of brokerage, meaning they have the greatest capacity to influence the network.

A more useful microlevel analysis can be gained by looking at the strongest relations in the network (Figure 2).

[88] Ibid., 244.

[89] Ibid., 238.

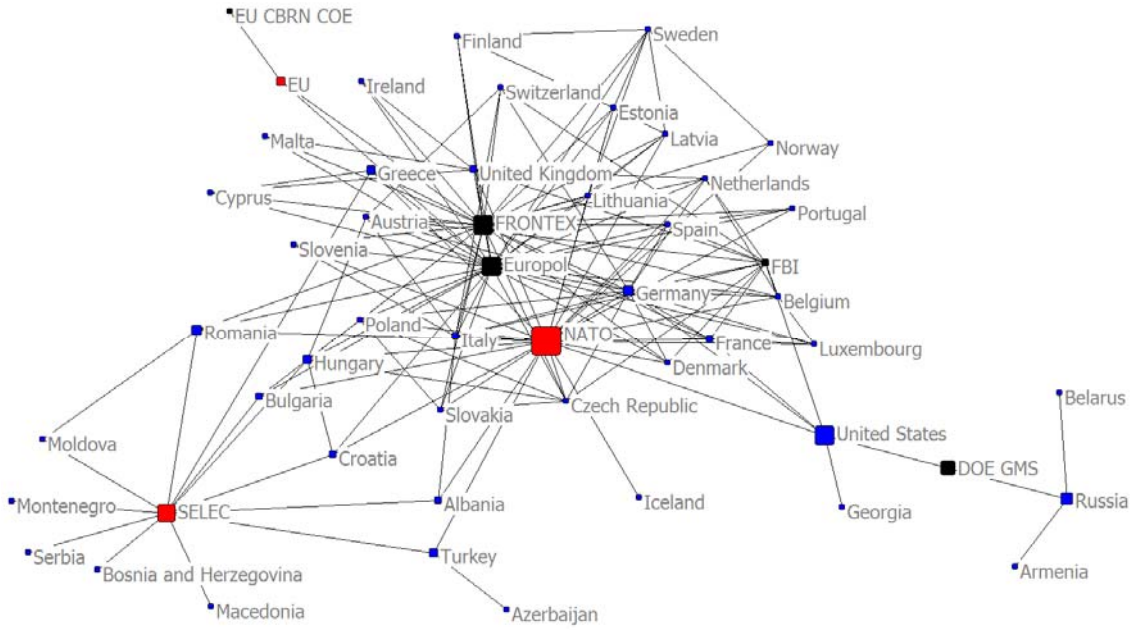

Figure 2. Strong Ties Sub-Network

To get a better microanalysis of actors, a subnetwork representing ties with a aggregate score greater than five (of a possible six) was extracted from the larger network; actors without strong ties were not included. We call this the strong ties subnetwork. Similar to the CNS-E network sociogram, the ties represent an aggregate relationship strength of three separate relations. The nodes are colored the same way (blue are states, red are IGOs, and black are substate agencies/programs) and are sized by betweenness centrality. The premise of this subnetwork is that cooperation in sensitive situations may only happen between actors with the strongest ties.[90] This network has significantly fewer actors and connections. This smaller, less dense network offers more useful analysis of key actors and relations, and looking at it reveals interesting ties between nodes. SELEC is a regional organization in a strong position of brokerage with Southeast European states. In theory, establishing strong relations with SELEC should increase cooperation with its member states. Perhaps more interesting is the brokerage position of the Department of Energy's Global Nuclear Security node. It connects the

90 James I. Walsh, "Intelligence-Sharing in the European Union: Institutions Are Not Enough," *Journal of Common Market Studies* 44, no. 3 (September 2006), 625–643.

United States to Russia, suggesting the strongest cooperation between the two countries is conducted through the Department of Energy. A further implication is that Russia is in a brokerage position between the DOE node and Belarus and Armenia. Thus, if the DOE needed a path to Armenia or Belarus, Russia is in a position to broker a relationship.

Three non-state actors occupy the center of the network: Frontex, Europol, and NATO. The quantitative metrics support the visual analysis both in degree and betweenness centrality. Frontex and Europol are tied for the highest degree centrality score of 29, and NATO is at 27. These are significantly higher than the mean ties per node at 6.21 (without isolates) and the median of 5. For betweenness centrality, NATO has the highest score with a normalized betweenness of 16.284, compared with Frontex at 9.3 and Europol with 9.24. For state nodes, Germany has the highest degree centrality with a score of 16. The United States has the highest betweenness centrality score of 8.535, despite having a low degree of 4. This can be explained by the unique broker position the U.S. occupies, connecting several peripheral nodes to the rest of the network. This positional advantage gives the United States' moderate influence in the network.

3. Line of Effort Sub-Networks

The following subnetworks were extracted from the larger CNS-E network by reducing the mission of countersmuggling into four LOEs. The LOEs reflect the range of CP/NP activities conducted by the network that contribute to countersmuggling and can be seen as linear in nature (though they do not have to be). The purpose of the LOEs is to examine the various stages of nuclear countersmuggling in greater detail and specifically to identify key non-state actors in each network. For this reason, states have not been included in the subnetworks. Including the states would fail to render a clear picture of important non-state actors, and states' significance can be assumed across the LOEs.

Two considerations must be remembered for this analysis. First, the influence of each node is based only upon its relations with other non-state actors. Thus, a node with many state ties, like OSCE, may appear less important here than nodes with few state ties, like the FBI. If influence needs to pass beyond the LOE subnetworks to states, it is then important to look at who has many or strong state ties. The second consideration is

that each node uniquely contributes to the network. This requires a qualitative understanding of how each node contributes to fully appreciate the analysis. For example, UNSC 1540 is influential in LOE 2, but that does not mean they are the node most capable of detecting shipping containers smuggling nuclear material.

In all of the following sociograms, the ties are aggregate relationship scores, red nodes are IGOs, black nodes are substate agencies/programs, and all nodes are sized by betweenness centrality.

4. LOE 1 Contain Nuclear Material

The purpose of LOE 1 is to contain nuclear material. This includes a variety of actions and agreements focused on reducing and safeguarding nuclear material both for military and civilian purposes. The military side of nuclear material containment can present challenges, as states are wary of agreeing to safeguards or inspections of nuclear materials. The sites housing weapons or the nuclear programs may be sensitive to national security, and the safeguards are expensive to implement.[91] On the civilian side, one challenge is the wide use of equipment containing nuclear material in unguarded locations. One estimate suggests there are over 13,000 buildings in over 100 countries that contain radiological sources large enough to make an effective dirty bomb.[92] Understanding the breadth of the problem LOE 1 seeks to address gives context to the make-up of the subnetwork. Each node in the subnetwork uniquely contributes to the mission of LOE 1 (Figure 3). However, the contributions can be generalized as one of the following: best practices for safeguarding or reducing nuclear material, inspection of sites containing nuclear material, or support to safeguards or reduction of nuclear material.

91 Aloise et al., *NUCLEAR NONPROLIFERATION: IAEA Has Strengthened Its Safeguards and Nuclear Security Programs, but Weaknesses Need to be Addressed* (Washington DC: Government Accountability Office, Oct 2005), 4–26.

92 Mathew Bunn et al., "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?" (project on managing the atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 2016), 98.

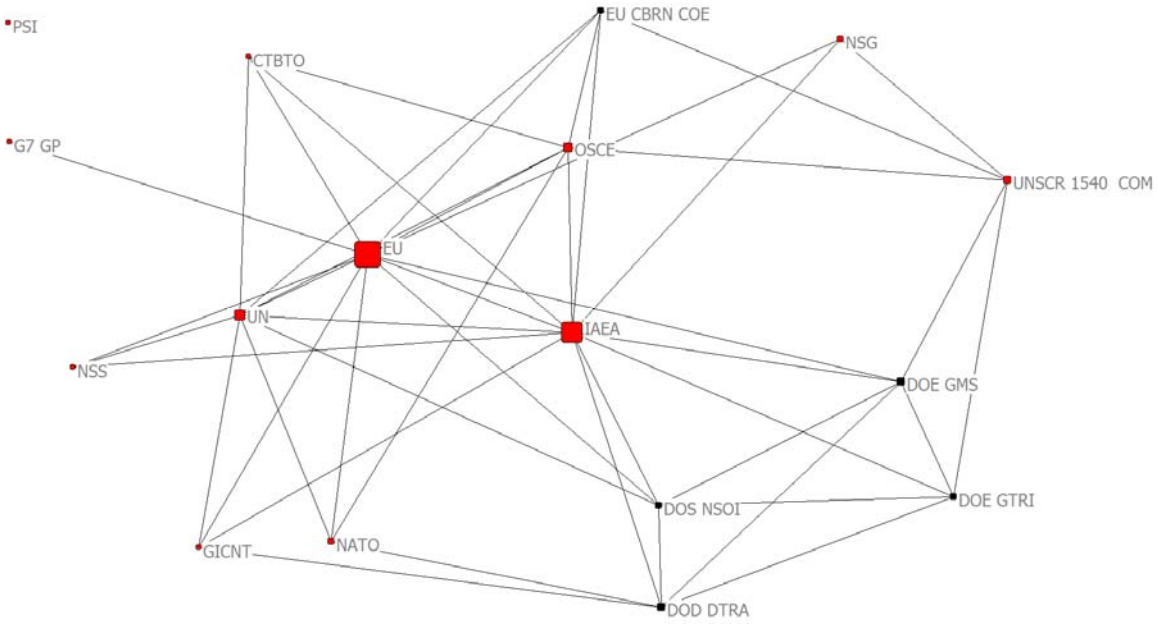

Figure 3. LOE 1 Sociogram

Visual analysis of LOE 1 shows a compact network with a few central actors. The subnetwork is moderately dense, with one-third of all possible connections present. PSI is isolated because it is an initiative to strengthen pre-existing laws which states commit to; it does not apply to non-states. The average path length between nodes is 1.658, and the diameter is 3. The compactness of the network along with its density can be interpreted as a moderate degree of cooperation in the LOE 1 subnetwork. With regards to central actors, it is important to note that centrality does not indicate what the node contributes to the network, only that it is central. For instance, the EU has the highest betweenness centrality score of 28.55 and a degree of 12. In terms of position in the network, the EU is the most central actor, which indicates a high degree of influence. However, their role is fairly limited to supporting best practices for CP/NP. On the other hand, the IAEA is the second-most central actor but adds much more capacity to the network, including establishing best practices, conducting inspections for site security, and supporting security enhancements in numerous countries. Thus, identifying central actors helps identify who can influence the network or disseminate information the quickest, but does not indicate the specific function of an actor.

5. LOE 2 Prevent Transnational Shipment

The purpose of LOE 2 is to prevent the transnational shipment of nuclear material. This includes various agreements and actions to detect nuclear material and stop it from exiting a country. If nuclear material is acquired in one state but another state is targeted for attack, it must be smuggled out of the country of origin. This presents a significant challenge, as the smuggled material will likely be a small quantity that is easily concealed and hard to detect.[93] The nodes in this subnetwork contribute to the LOE 2 mission in several ways: by establishing best practices for CP/NP in relation to radiological equipment exports, promoting best practices, and providing detection capability through equipment or training (Figure 4).

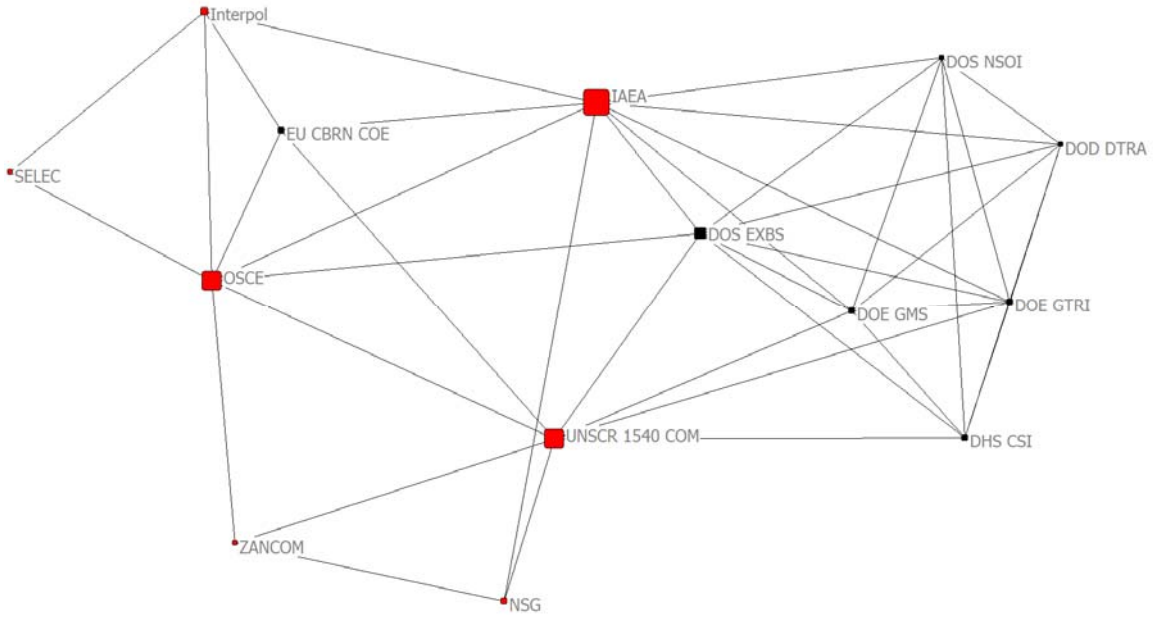

Figure 4. LOE 2 Sociogram

The LOE 2 sociogram depicts a moderately dense network with a tightly connected cluster comprising the various U.S. agencies/programs. The subnetwork has a density score of .44, with just shy of half of all possible ties present. It is compact, with an average path length of 1.659 and a diameter of 3, though it is more compact on the

[93] Ibid., ii.

right side of the graph than the left. The density and compactness can be interpreted as a moderate degree of cooperation throughout the network, with more cooperation on the right side of the graph and less cooperation between the nodes on the left and bottom of the graph. Given the overall diameter and connectedness, information should spread well throughout the network. Importantly, every node has more than one connection to the rest of the network. This reduces the likelihood that a problem at any one node would prevent transmission to the rest of the network. The IAEA is the most central node in the LOE 2 subnetwork, with the highest betweenness (18.863) and degree (9) scores. The UNSCR 1540 Committee and OSCE are the next-most central nodes in terms of betweenness, with scores of 13.476 and 13.405, respectively. The sociogram makes it clear, though, that UNSCR 1540 and the IAEA are in the best positions of brokerage between the U.S. nodes on the right and the European nodes on the left. It is worth noting that DOS EXBS is the next-most central actor, with a degree of 8 and a betweenness of 5.5521, and is the only U.S. node with a relationship to a European-specific IGO.

6. LOE 3 Protect State Borders

The purpose of LOE 3 is to protect state borders against illicit nuclear material. This LOE includes a variety of actions to prevent such material from entering a given country. Once nuclear material has exited a country, it still must make it to its final destination; if LOE 2 fails, then LOE 3 is the barrier. Stopping nuclear material at a border presents several obstacles. Specifically in the EU, there are miles of unprotected border that can be breached from land and sea. Even if smugglers are using established ports, airports, or border crossings, detecting nuclear material most often requires special equipment.[94] There are also well-developed smuggling routes in Europe which carry everything from cars to drugs to immigrants. The various nodes comprising the LOE 3 subnetwork contribute in the following ways: physical security of borders, capacity building, or generation of intelligence/information (Figure 5).

94 Ibid., 131.

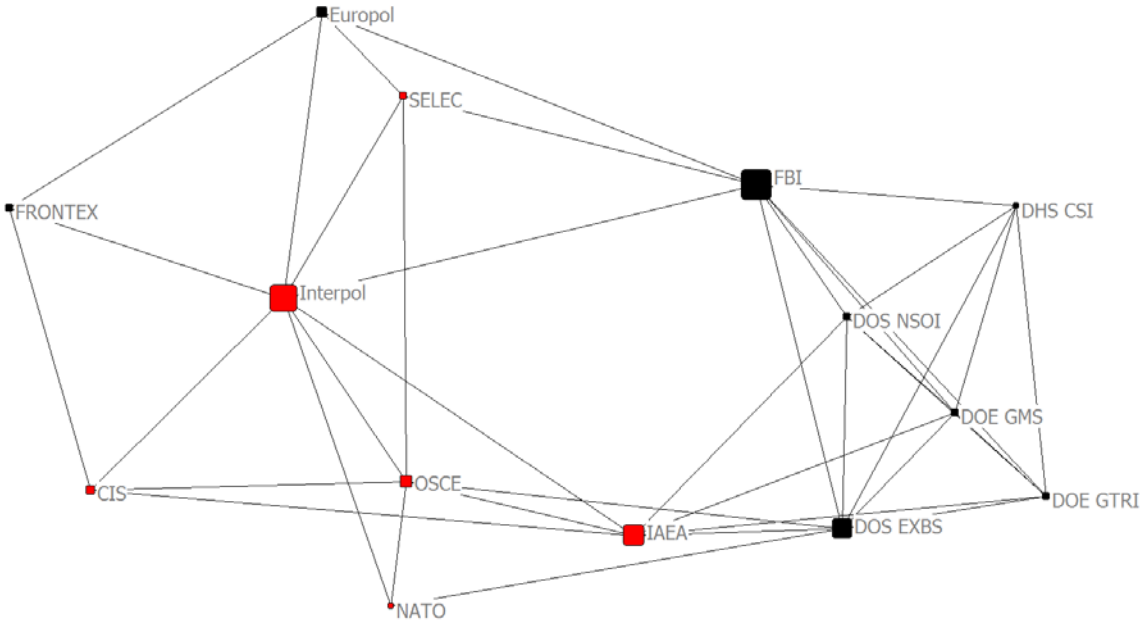

Figure 5. LOE 3 Sociogram

The LOE 3 subnetwork is similar in structure to LOE 2—it is also moderately dense and compact. This subnetwork has a density score of .429, and each node averages 5.57 ties. The network is compact; the average distance between nodes is 1.637, with a diameter of 3. Like in LOE 2, a cluster of U.S. nodes is present on the right side of the graph, creating uneven density and compactness in the network. Again, this can be interpreted as moderate cooperation throughout the network, with more cooperation on the right side than the left. An interesting difference is that the left side of the graph is centralized around Interpol. Interpol is slightly less central in the overall network than the FBI but would have more influence over the nodes on the left side of the graph. The FBI is the most central node in the LOE 3 subnetwork, with a degree of 8 and a betweenness of 15.202. The IAEA is the next-most central node and sits in between the two sides, with four ties to the right side and three ties to the left.

7. LOE 4 Interdict Nuclear Material

The purpose of the LOE 4 subnetwork is to interdict the nuclear material either during transnational movement or within the target country. Interdiction is unique amongst the LOEs because it is a mobile capability that can be implemented at any point

after the nuclear material is acquired, making it nonlinear. Interdiction can happen in the country of origin, during transnational movement, or after it has entered the target country. Which domain interdiction occurs in significantly impacts who conducts it and how. For example, the majority of recent nuclear material smuggling incidents have been interdicted in sovereign national space by domestic law enforcement or border security.[95] If interdiction occurs in international space, a military force is more likely to participate. The most challenging parts of interdiction are knowing that material needs to be interdicted at all and knowing where to find it. The tactical side of interdiction can be challenging but poses less of an obstacle. Once the nuclear material is located, most countries in the CNS-E network have the capacity to retrieve it. The nodes that comprise the LOE 4 subnetwork contribute to its purpose in the following ways: supporting existing legal CP/NP regulations, acquiring and disseminating intelligence, or supporting the interdiction mission (Figure 6).

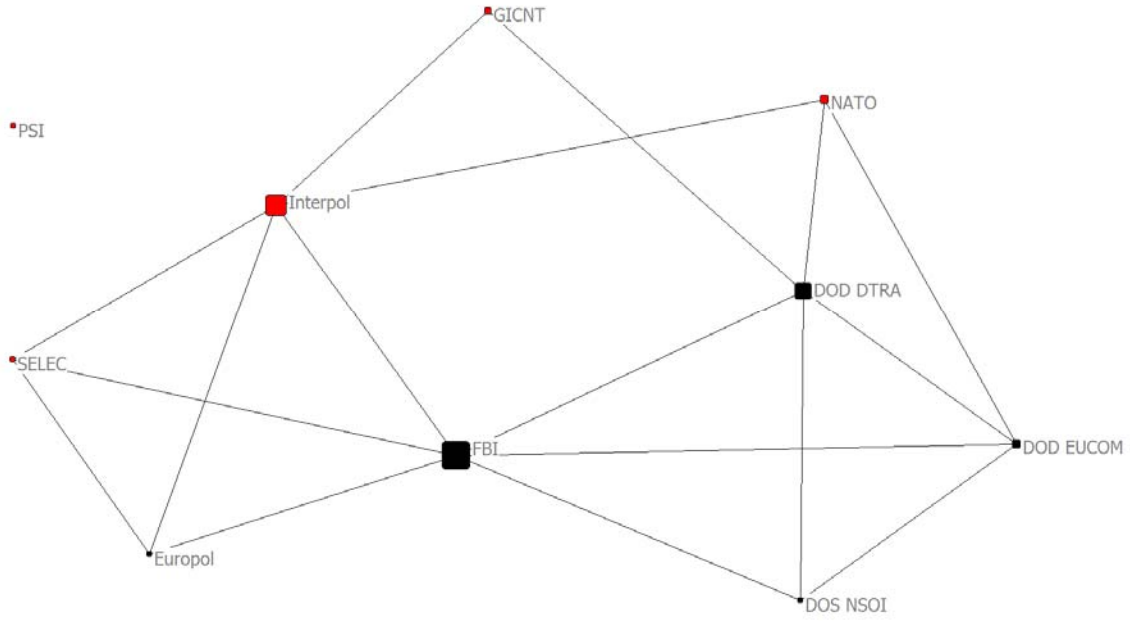

Figure 6. LOE 4 Sociogram

95 CNS Global Incidents and Trafficking Database Nuclear Threat Initiative (March 2016).

The LOE 4 subnetwork is the smallest of the four and is correspondingly more compact. It has an average distance of 1.528 and a diameter of 2. It has a density score of .378 and an average degree of 3.4 out of a potential 12. In light of the size of the network, these metrics suggest it is the least dense of the four LOEs. Like in the previous LOEs, the density is not dispersed evenly. There are two distinct clusters in the graph, one on the left and another on the right. This depicts high cooperation within the clusters and low cooperation throughout the network as a whole. The two sides of the network are mostly connected through the FBI. Consequently, the FBI is the most central actor in the network, with the highest degree (6) and betweenness scores (7.833). Interpol and DTRA are the next-most central actors, respectively. Their positions indicate that Interpol would be more influential among the European nodes on the left side of the graph and DTRA more influential among the U.S. agencies. Perhaps the most interesting insight gathered from the LOE 4 sociogram is a path of coordination between European and U.S. agencies through the FBI.

D. CNS-E NETWORK FINDINGS AND IMPLICATIONS

Applying SNA to the CNS-E network has illuminated the structure of the network in both metrics and graphs. The quantitative analysis reveals that the CNS-E network is highly dense and decentralized, and qualitative analysis confirms that the network is informal, meaning we can describe it as organic.[96] This is an important categorization for the CNS-E network, because we can use organizational theory to determine the strengths and weaknesses of organic structures and assess whether or not this structure is the right fit for the network. After interpreting the structural analysis, we will review key actors and insights from the subnetworks.

The characteristics that make the CNS-E network organic contribute to its effectiveness in numerous ways. High density allows information to transmit through the network quickly. It also adds resiliency to the network due to the presence of redundant paths between actors. This makes information flow reliable and unlikely to be interrupted by a single actor. The capacity for information sharing is crucial for a network dealing

96 McShane and Von Glinow, *Organizational Behavior*, 238.

with transnational problems, as it inherently involves multiple actors. High decentralization distributes power and decision making throughout the network. This is important in a complex environment, since there are more significant variables influencing performance than a small group of executives can control. By distributing power, the actors most affected by a problem and in possession of the most information can take immediate action as opposed to waiting for instruction. For instance, if nuclear material is stolen in Germany, they can immediately address the problem, whether by interdicting or informing other relevant players, without waiting for instruction from an executive body. This is a critical capability in time-sensitive cases. As we have discussed, decentralization also lends itself to informality, and the lack of standard operating procedures in informal organizations allows them to adapt to dynamic environments like counter nuclear smuggling. Bad actors will constantly search for new ways to obtain nuclear material. A network that can quickly adapt to emerging threats will be more successful than one entrenched in bureaucracy.

The same organic characteristics of the CNS-E network that contribute to its effectiveness can also make it inefficient. Decentralized networks tend to have several drawbacks. First, the absence of executive power can make it difficult to move the network in a common direction. This is especially true for the CNS-E network. Unlike a decentralized business, the CNS-E network is predominately made up of sovereign states existing in an anarchic environment. Without a single executive, the CNS-E network may struggle to form a coherent strategy for achieving its purpose. It may fail to motivate the whole network to sanction a rouge state, or fail to agree on how to allocate resources. Perhaps most importantly, no single actor can direct the network to perform critical tasks like information sharing. Decentralized networks also face a coordination challenge. Given the transnational and time-sensitive nature of counter nuclear smuggling, a high degree of coordination is required for the CNS-E network to be effective. To achieve this, the network must invest significant resources in coordination mechanisms like full-time

integrators, crossfunctional teams, and frequent multi-actor meetings.[97] Any effort short of these mechanisms will have much lower effectiveness.

Despite the weaknesses of the organic structure, it is the most effective configuration for the CNS-E network. The effectiveness of a network's structure depends on how well it fits the purpose and environment.[98] Preventing smuggling is a difficult task, and, again, the environment in which it occurs is complex and dynamic, meaning that to be effective in this environment, an organization must be adaptable and decentralized. The organic structure of the CNS-E network is both. Its informality enables it to adapt to a dynamic environment and smart opponents; its decentralized power enables it to process a multitude of variables. Furthermore, the density of the network can allow it to meet its robust coordination requirements. Though adaptability and decentralization come at the cost of efficiency, this is an acceptable tradeoff for the CNS-E network simply because whole-network efficiency does not lend itself to effectiveness in complex, dynamic environments. Therefore, the CNS-E network is structured appropriately for its purpose and mission, providing it puts sufficient resources into coordination.

The subnetwork analysis helped reveal key actors in each network. The strong ties subnetwork illustrates who is more likely to cooperate in situations that require strong ties. Key findings include:

- Frontex, NATO, and Europol are the most central (influential) actors in the strong ties subnetwork. Importantly, they are regional organizations. International organizations in the CNS-E network, like Interpol or the UN, appear to lack the strong connections of regional organizations.
- SELEC occupies a powerful broker position and represents an opportunity to gain stronger relations with Southeast European states (specifically via their law enforcement agencies).

97 Richard L. Daft, *Organization Theory and Design* (Mason, Ohio: South-Western Cengage Learning, 2010), 281.

98 Mintzberg, "Fashion or Fit?," 16.

- The United States occupies an important brokerage positon in the strong ties subnetwork, as it connects Eastern Bloc states such as Russia, Georgia, Belarus, and Armenia to the rest of the network.
- The DOE is the strongest connection between the United States and Russia and is best suited to enhance cooperation.
- Germany is significantly more influential in this network, in terms of the number of actors it is tied to, than any other state actor.
- Strong relationships are facilitated by IGOs.

The lines of effort subnetworks reduced countersmuggling into four missions. The key findings are:

- LOE 1 is the largest subnetwork, suggesting the majority of the CNS-E network's effort goes into nonproliferation activities.
- The IAEA appears to be the most significant player in the subnetworks, based on the position it occupies in LOEs 1, 2, and 3 and the capabilities it contributes to each.
- The FBI occupies central positions in LOE 3 and LOE 4. This implies that the FBI is the best conduit for cooperation between U.S. and European nodes for border-protection matters and interdiction.
- LOEs 2, 3, and 4 show strong cooperation among U.S. nodes and among European nodes, but significantly less cooperation between U.S. and European nodes. Intermediary actors connecting the two groups serve an important role if/when coordination is required. The IAEA, the FBI, and to a lesser extent NATO and DOS EXBS currently occupy these positions.

E. NETWORK ANOMALY

According to the analysis, the CNS-E network is structured to effectively counter nuclear smuggling and all associated tasks, but qualitative research contradicts this. There is an abundance of literature documenting, and seeking to explain, the failure of intelligence sharing between European actors.[99] As the CNS-E network predominantly comprises European actors, these findings also hold true for our network. The density of the network suggests information should travel through the network quickly and reliably,

99 Walsh, *Intelligence-Sharing in the European Union*, 625–643.

so the structure of the network does not account for or explain the failure of intelligence sharing. Intelligence sharing is arguably the most important task the CNS-E network must do well to be effective. Therefore, it is worthwhile to explore possible explanations for this structural anomaly.

The three IR theories each explain this anomaly differently. Realist theory would see the international institutions as mechanisms of the most powerful states and say that individual self-interest and security or power concerns limit the sharing of private information. Neoliberal institutionalist theory recognizes incentives for private information but would say that institutions have the potential to create an environment that would allow the sharing of sensitive information through changing the payoff structure, increasing the time horizon, and mitigating free riders. Constructivist theory would indicate that the lack of trust within the system is determined by the states themselves; a breakdown of sovereignty barriers would be possible if states elected to view the environment as friendly and not hostile.

Domestic theory also could provide insight into the lack of intelligence sharing. Prospect theory would indicate that some leaders within Europe may be in a losses frame of mind and unhappy with the status quo. Their participation within the institutions creates fear of them exploiting sensitive information, as they are more willing to risk upsetting the current international order. Selectorate theory would propose that state leaders are currently unable to provide the necessary intelligence due to a lack of public support from their winning coalitions. Concerns over privacy and sovereignty dominate the public discourse in this arena, and leaders that choose to go against the will of their supporters will invariably be punished in upcoming elections.

Now that the CNS-E network has been characterized using SNA, the function of the network can be assessed using vignettes based upon recent nuclear or terrorism incidents. The following chapter will assess the network in action based on two scenarios: nuclear threats originating in the European Union's Schengen Area, and smuggling nuclear material or weapons into the European Union.

IV. CASE STUDY ANALYSIS

In order to visualize the Counter Nuclear Smuggling–Europe network in action, we analyze two nuclear terrorism scenarios that would require the network's response. The first scenario involves an attack utilizing nuclear or radiological material acquired in the European Union's (EU) Schengen Area. The second scenario analyzes the network's response to terrorists acquiring nuclear or radiological material outside of the EU and then smuggling the material across borders or into the EU to conduct an act of terrorism. Both scenarios incorporate factual circumstances from recent terror attacks in Europe and aspects of current nuclear terrorism threats in the form of vignettes.

The framework for analyzing the scenarios involves identifying which nodes and LOEs will play significant roles in countering the threat, and analyzing the behavior of the network in a given scenario. The first step is to identify the operational and structural characteristics of the network when countering the specific threat. The second step is to analyze the individual LOEs, and the third step is to identify the significant actors in the scenario. The final step is to draw conclusions by assessing the interoperability of the actors across LOEs and inferring the strengths and weaknesses of the network in the scenario. Analyzing these cases and the network's responses enables us to recommend improvements that will enhance the network's response to similar scenarios in the future.

These situational analyses reveal that the network is not static but behaves differently based on where threats originate, how smuggling takes place, and the location of the target. If European citizens acquire nuclear material and carry out acts of terror within the open-border Schengen Area, the organizations that prevent transnational shipment of nuclear material (LOE 2) and that secure borders (LOE 3) will play a limited role, if any, in preventing an attack. On the other hand, if terrorists acquire nuclear or radiological material outside of the Schengen Area and attempt to cross borders or smuggle it into the EU, the entire network should behave sequentially by LOE. The scenarios enable an analysis of the interactions between critical nodes and LOEs beyond SNA. The insights provided by these scenarios should help inform USG policy makers

and military officials attempting to influence partner capabilities and address emerging threats.

A. SCENARIO 1: NUCLEAR THREATS ORIGINATING IN THE EUROPEAN UNION'S SCHENGEN AREA

The first scenario entails an attack on a nuclear facility in the Schengen Area, or an attack using nuclear or radiological material acquired in the Schengen Area. In this scenario, the three likely forms of nuclear terrorism are all possible. Terrorists can steal material and employ an improvised nuclear weapon, sabotage a nuclear facility, or detonate a radiological dispersion device, a "dirty bomb."[100] In order to conduct any of these attacks, the terrorists must first acquire material. Therefore, counterterrorism efforts in this scenario rely heavily upon efforts to safeguard nuclear and radiological material in Europe. In examining this line of effort, we discuss recent IS interest in nuclear and radiological material in Europe, the threat of sabotage, and nuclear security concerns in the EU.

By using actual recent history as vignettes, we can create a plausible analysis of a domestic or homegrown attack in Europe. Despite numerous international agreements, organizations, and protocols, nuclear security in European states varies. IGOs, therefore, can incentivize states to comply with norms, but generally are less likely to act during a crisis. This scenario illuminates how an outside agency could best affect nuclear security efforts pre-crisis and then assist an EU state during crisis.

1. Vignettes

a. Vignette 1. Monitoring Nuclear Researchers

Reporting indicates that IS actively monitored the activities of a senior nuclear researcher in Belgium prior to the November 2015 attacks in Paris. Belgian authorities, searching the home of a man connected to the terror cell, uncovered video surveillance of the researcher, who works at a facility with both highly enriched uranium (HEU) and

[100] Bunn et al., "Preventing Nuclear Terrorism," 4.

large quantities of radioisotopes.[101] Officials speculate that the terror cell intended to kidnap the researcher or members of his family in order to gain access to the nuclear plant.[102] Had the terrorists accessed material, they could potentially have used the HEU to construct nuclear weapons and the radioisotopes to construct a radioactive dirty bomb.

b. Vignette 2. Insider Threats and Sabotage

Rather than stealing material, terrorists could initiate a meltdown, which would require access to a nuclear reactor and knowledge of the facility's inner workings. In 2012, a Belgian nuclear facility worker named Ilyass Boughalab left his job to join IS in Syria. Boughalab worked at the Doel power plant for three years before joining IS and was ultimately killed in 2014.[103] Although Boughalab was no longer working at the nuclear facility in 2014, an unsolved incident—believed to have been sabotage—damaged and shut down a reactor, resulting in $100–200 million in damage.[104] This incident did not cause the reactor to melt down or place anyone in danger, but the potential exists that future accidents or acts of sabotage could cause a serious nuclear incident. It is also possible that Boughalab shared his knowledge of Belgian nuclear security protocol with IS leadership in Syria. Additionally, both Germany and the Netherlands have recently voiced safety concerns over aging Belgian facilities and recent efforts by the Belgians to re-open closed facilities.[105] Aging facilities, defecting workers, and unsolved incidents like this raise concerns over the threat of an insider attack.

---

[101] Matthew Bunn, "Belgium Highlights the Nuclear Terrorism Threat and Security Measures to Stop It," *World Post*, March 29, 2016, accessed May 10, 2016, http://www.huffingtonpost.com/matthew-bunn/belgium-nuclear-terrorism_b_9559006.html; Patrick Malone and R. Jeffrey Smith, "The Islamic State's Plot to Build a Radioactive 'Dirty Bomb,'" *Foreign Policy*, February 29 2016, accessed March 14, 2016, http://foreignpolicy.com/2016/02/29/the-islamic-states-plot-to-build-a-radioactive-dirty-bomb/?utm_source=Sailthru&utm_medium=e-mail&utm_campaign=New%20Campaign&utm_term=%2AEditors%20Picks.

[102] Bunn et al., "Preventing Nuclear Terrorism"; Malone and Smith, "The Islamic State's Plot."

[103] David Chazan et al., "Brussels Attacks: Nuclear Breach Fears as Two More Charged with Terror Offences," *Telegraph*, March 27, 2016, http://www.telegraph.co.uk/news/2016/03/26/brussels-attacks-nuclear-breach-fears-as-two-more-charged-with-t/.

[104] Bunn, "Belgium Hightlights the Nuclear Terrorism Threat"; Geert De Clercq, "Update 2–Belgian Doel 4 Nuclear Reactor Closed Till Year-End," *Reuters*, August 14, 2014.

[105] Arthur Neslen, "Border Tensions Rumble over Ageing Belgian Nuclear Reactors," *Guardian*, February 2, 2016.

Although this threat can be mitigated to some extent through security protocols, it is a concern not only for Belgium but for all countries with nuclear facilities.

c. Vignette 3. Security at European Nuclear Facilities

Security at Europe's numerous nuclear facilities differs drastically by state. A 2012 EU-sponsored nuclear facility assessment found significant disparities in nuclear security between facilities throughout the EU.[106] Additionally, political activists have breached security measures at Western European nuclear facilities to bring attention to nuclear dangers and the lack of security.[107] With half of the world's research reactors and nearly half of its active power reactors located in Europe, the EU is home to a significant amount of nuclear material in various forms and quantities. This provides terrorists with a target-rich environment for nuclear terrorism.[108]

2. The Network Structure

An attack utilizing nuclear material in the Schengen Area primarily involves the organizations in LOEs 1 and 4, because terrorists could acquire, assemble, and detonate a weapon in Europe while avoiding the organizations responsible for transnational shipping and border security (LOEs 2 and 3). LOE 1 (Figure 7), the organizations whose goals are the inspection and safeguarding of nuclear material, and LOE 4 (Figure 8), the organizations that interdict terrorists and secure loose material, are on opposite ends of the NP/CP spectrum, but they share characteristics such as emphasis on local law enforcement and physical security.

---

[106] Marcy Fowler and Alisa Carrigan, "Nuclear Security in European Union Member States," *EU Non-Proliferation Consortium Non-Proliferation Papers*, No. 44 (April 2015), 1–18.

[107] Lynn La, "Greenpeace Protesters Made Breaking into French Nuclear Power Plants Look Easy," *Business Insider Australia*, December 7, 2011.

[108] Fowler and Carrigan, "Nuclear Security in European Union," 1–18.

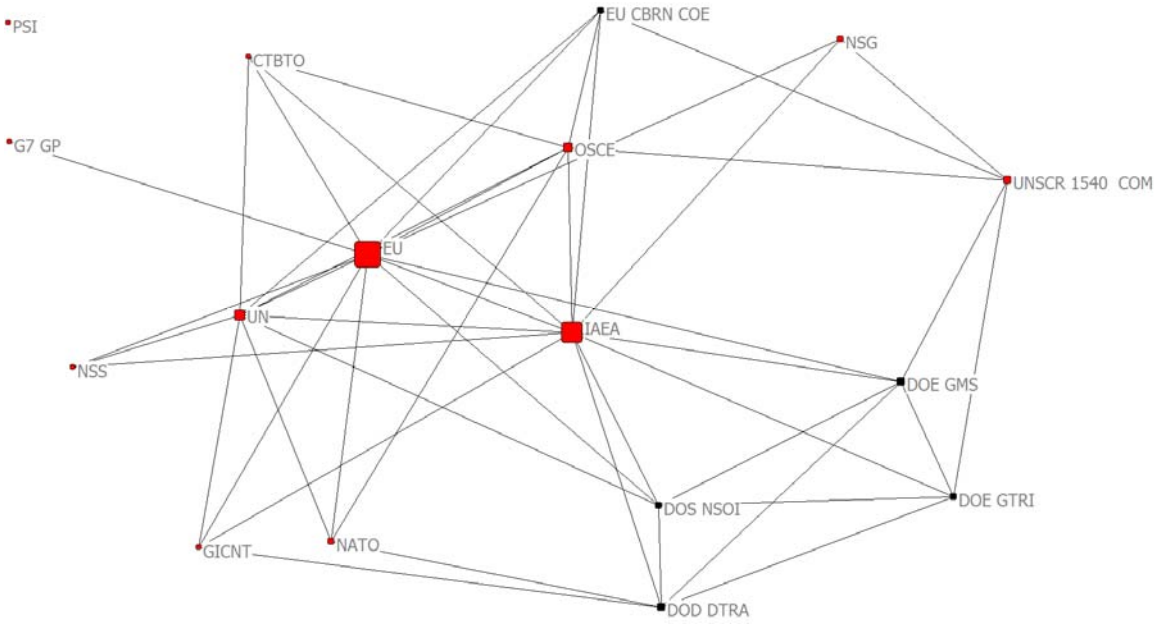

Figure 7. LOE 1 Sociogram

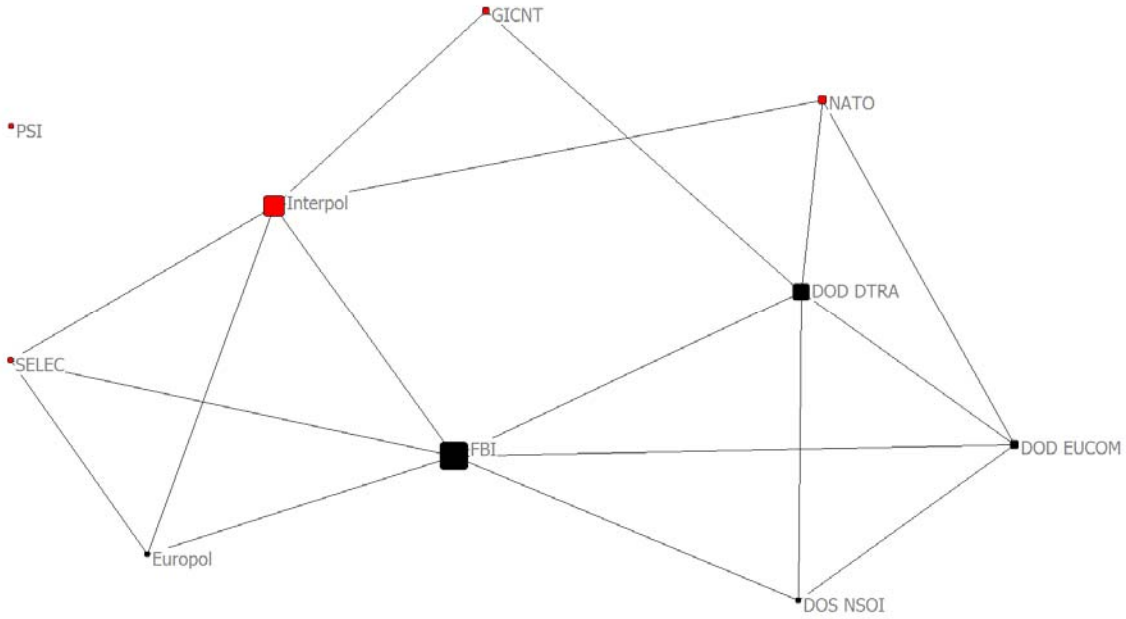

Figure 8. LOE 4 Sociogram

3. Analysis by LOE

Because terrorists must acquire nuclear material in order to conduct nuclear terrorism, significant resources are rightfully directed at securing nuclear facilities (LOE 1). As the sociogram depicts, the IAEA occupies the second-most central position in this network (behind the EU) and is assessed to be the most operationally active—however, the primary tasks of the IAEA and similar organizations such as EUATOM are establishing best practices and conducting routine inspections. The individual states must translate routine inspections and best practices into effective nuclear security policy. This means that despite the IAEA's central position in the network, the responsibility for implementing and executing effective security falls on the individual states.[109] This scenario presents challenges for the international CP community. Although securing nuclear material (LOE 1) is the most robust LOE within the network, with over three times as many nodes as LOE 4, LOE 1's effectiveness varies from state to state. As a result, countries within the Schengen Area are only as safe as the weakest member state.

This scenario requires a relationship between the many IGOs in LOE 1 that establish and regulate policy but operationally contribute little to security and the few organizations in LOE 4 that are charged with tracking, locating, and interdicting material. Interdicting nuclear terrorists (LOE 4) is, according to our network, the smallest LOE. LOE 4 could have the fewest nodes because preventing proliferation is preferred to interdicting proliferation, but it also may be because interdiction forces are generally the most unilateral—requiring sensitive intelligence and equipment. LOE 4 interdiction forces are the least likely to answer to an IGO, and therefore have limited nodes in our IGO network. Due to the United States-centric nature of the network, the FBI and Interpol are the most central organizations in this LOE. Based on centrality within the LOE, the best means for the USG to cooperate with European states and IGOs in LOE 4 is through the FBI.

[109] Ibid.

4. Critical Nodes

Cooperation between LOEs could be enhanced by linking the most central nodes in each network. Increased interoperability between the most central operational node in LOE 1, the IAEA, and the most central node in LOE 4, the FBI, should make the network more effective in countering this scenario. Though this would strengthen the network, it is unclear that security within individual states would improve. Ensuring that host nation security and interdiction capabilities increase may therefore require more proactive measures than linking the nodes most central to each LOE.

We could also improve the network's response to this scenario by identifying and enhancing nodes present in both relevant LOEs. Three nodes are present in both LOEs 1 and 4: DoD DTRA, DOS Nuclear Smuggling Outreach Initiative (NSOI), and GICINT. Both DTRA and NSOI provide a mechanism for bilateral engagement with the host nation rather than actual security or interdiction forces in their own right. The challenge with DTRA engagement is that partner-nation militaries likely play a limited role in domestic counterterrorism. Other than securing nuclear weapons on military installations, partner-nation militaries generally lack the authority to operate within their own borders. NSOI, on the other hand, engages with partner law enforcement agencies that are likely heavily involved in domestic CT activities. This means that while DTRA provides a military to military link, NSOI is the better means for engaging with local LEA that secure and interdict nuclear material.

5. Scenario 1 Conclusions

The strength of the network when countering this scenario is that the primary parties acting in both LOEs 1 and 4 are not IGOs but host-nation LEAs and security forces. Although outside organizations such as Interpol or Europol may assist with interdiction, operationally this scenario is extremely reliant on host-nation security. This should enable rapid and effective communication, as incentives to cooperation are high and barriers to information sharing are low among agencies within a given state. Through cooperation with international organizations and bilateral partnerships, the host nation

may be able to share and disseminate intelligence to heighten security in anticipation of future attacks.

The biggest challenge for the network in this scenario is that open borders can give terrorists freedom of movement within the Schengen Area—border and shipping security are minimal and the requirement for international cooperation between EU states is high. Fortunately, the EU is the most central node in LOE 1, which should facilitate collaboration in the steady state and cooperation between EU states during crisis. Numerous USG nodes also occupy central locations in both LOEs, enabling the USG to influence this scenario.

The IAEA and the FBI are the two nodes most central to this scenario, and DTRA, DOS NSOI, and GICINT are the only nodes in both LOEs. To enhance the network's response to a threat emanating from within the EU, threat-based exercises could aid in assessing security at nuclear facilities and likely target areas. Working with organizations such as the IAEA, FBI, and DOS NSOI, military and law enforcement personnel could analyze nuclear facilities and likely target areas for vulnerabilities in order to enhance security measures. While IGOs may not play active roles in actually stopping attacks, proactive collective measures today will enhance the host nations' responses tomorrow. Additionally, any efforts undertaken to enhance information sharing between states and through IGOs will enable the target states to better respond to acts of terrorism.

B. SCENARIO 2: SMUGGLING NUCLEAR MATERIAL ACROSS STATE BORDERS OR INTO THE EUROPEAN UNION'S SCHENGEN AREA

The second scenario involves terrorists smuggling nuclear weapons or material across state borders or into the Schengen Area in order to conduct an act of terrorism. This involves the entire network, but to better understand the progression of smuggling, we will still analyze the network by LOE. In this case, smuggling follows a linear progression as the smuggler attempts to defeat each LOE in sequential order. To further understand this scenario, we examine the nuclear black market in Eastern Europe, examples of lost or missing radiological and nuclear material, and trafficking routes in

Europe. We will see that while significant resources are devoted to each LOE, operationally there is limited overlap across LOEs and in general the network lacks unity.

1. Vignettes

a. Vignette 1. Nuclear Black Market in Moldova

According to recent reports, with assistance from the FBI, Moldovan authorities uncovered four attempts in the last five years to smuggle nuclear material to the Middle East through Moldova. The nuclear material is believed to be originating in Russia; however, the existence of a nuclear black market suggests that traffickers may have stockpiles of material left over from the Cold War. In the most recent instance, nuclear traffickers suggested that IS use the material to attack the West. Fortunately, the potential buyer was not an IS operative but an undercover agent.[110] The existence of actual buyers therefore remains uncertain. This interdiction of nuclear trafficking suggests that aspects of the CP network are performing effectively; however, with unknown quantities of nuclear material possibly on the market, there is potential that material could find its way into the hands of violent extremists.

b. Vignette 2. Missing Nuclear and Radiological Material

States have reported nuclear and radiological material missing all over the world. As recently as November 2015, Baghdad reported radiological material missing to the IAEA. The material, used by oil companies to test flaws in oil and gas, was stored in a facility in the southern Iraqi city of Basra. After an unclear amount of time, the material was later discovered only a few kilometers from its storage facility. Recovery of the level-two radiological material ended fears that IS had stolen it to create a dirty bomb, but does not answer questions about how the material went missing in the first place. This situation is indicative of a larger issue, which is the prevalence of dual-use nuclear and radiological material all over the world. Because radiological material is common in

110 "Nuclear Smuggling Deals 'Thwarted' in Moldova," BBC News, October 7, 2015, http://www.bbc.com/news/world-europe-34461732; Kathy Gilsinan, "Why Moldova May Be the Scariest Country on Earth," *Atlantic*, October 8, 2015; Desmond Butler and Vadim Ghirda, "AP INVESTIGATION: Nuclear Black Market Seeks IS Extremists," Associated Press, October 7, 2015.

research facilities, hospitals, and other high-technology industries, the potential for terrorists to acquire this material is relatively high.[111] Dr. ElBaradei, then director general of the IAEA, gave this warning to the United Nations General Assembly in 2008:

> The possibility of terrorists obtaining nuclear or other radioactive material remains a grave threat… The number of incidents reported to the Agency involving the theft or loss of nuclear or radioactive material is disturbingly high… Equally troubling is the fact that much of this material is not subsequently recovered. Sometimes material is found which had not been reported missing.[112]

c. Vignette 3. Smuggling in Europe

The recent attacks by IS in Paris and Brussels, as well as contemporary literature, reveal a nexus between terrorists, proliferators, and traffickers. According to reports, numerous members of the terrorist cell who carried out the Paris attack were directly affiliated with IS, including the mastermind behind the attack, who had served as an IS commander in Syria. Reporting indicates that having traveled from Europe to Syria, these known IS members were able to return to Europe undetected by Western intelligence. How these IS members, including the Paris mastermind and IS commander Abdelhamid Abaaoud, reentered the EU is unclear. Biometric data indicates that two individuals who participated in the Paris attack entered the EU as refugees, likely using stolen passports.[113] In addition to refugee migration, numerous forms of trafficking exist in Europe and within the EU. These include drugs, weapons, and human trafficking routes and networks. Although significant resources are directed toward countering these problems, trafficking persists because demand exists, and conceivably these same networks could facilitate transfers of nuclear materials.[114]

---

[111] "Fact Sheet on Dirty Bombs," United States Nuclear Regulatory Commission, last modified December 12, 2014, accessed May 19, 2016, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.html.

[112] Bob Graham et al., *World at Risk*, 43.

[113] Parlapiano et al., "The Expanding Web of Connections."

[114] Glenn Curtis and Tara Karacan, *The Nexus among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe* (Washington, DC: Library of Congress, 2002).

2. The Network Structure

This scenario involves the entire network, including all four LOEs (Figures 9–12) as well as bilateral and multilateral cooperation among the affected states. In this scenario, nuclear or radiological material being smuggled into Europe could originate anywhere in the world. With loose nuclear and radiological material believed to be unaccounted for globally, LOE 1 may play a limited role here, and LOEs 2 and 3 are critical to stopping nuclear smuggling. If nuclear terrorists were to enter the EU's Schengen Area, it appears that bilateral cooperation among the various states, with assistance from IGOs, is the most efficient means of identifying and interdicting those terrorists.

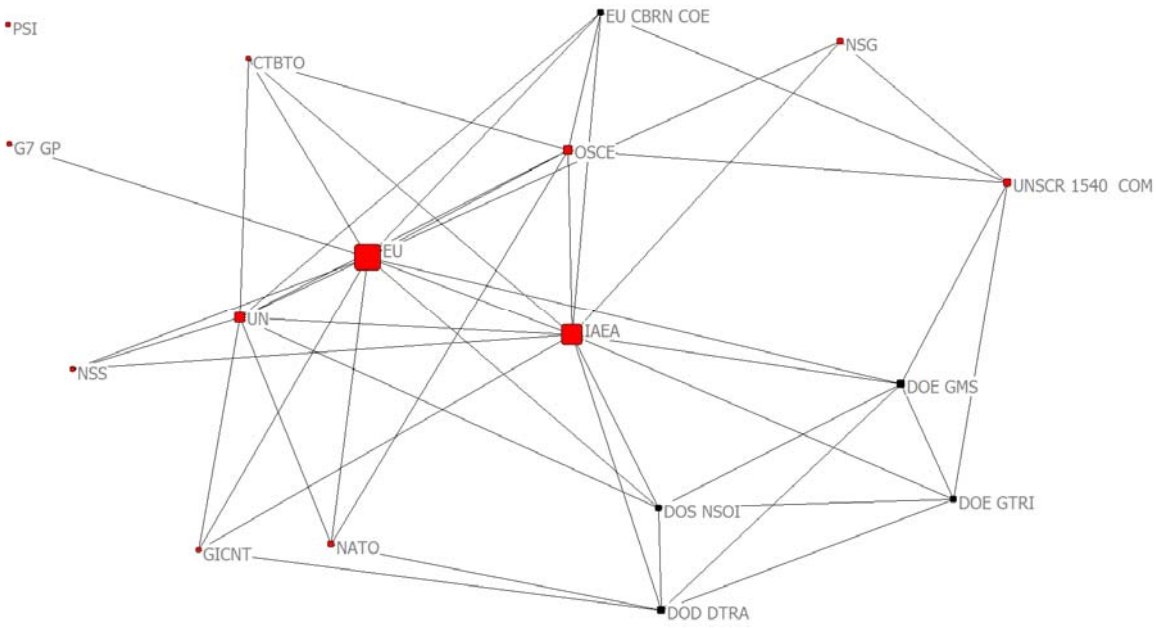

Figure 9. LOE 1 Sociogram

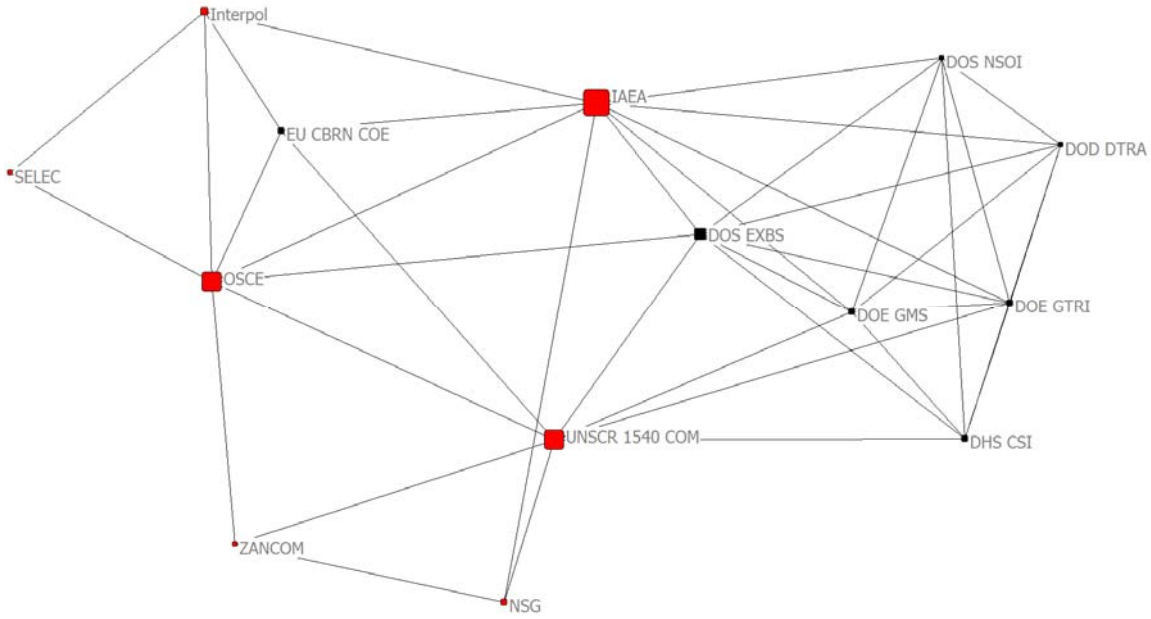

Figure 10. LOE 2 Sociogram

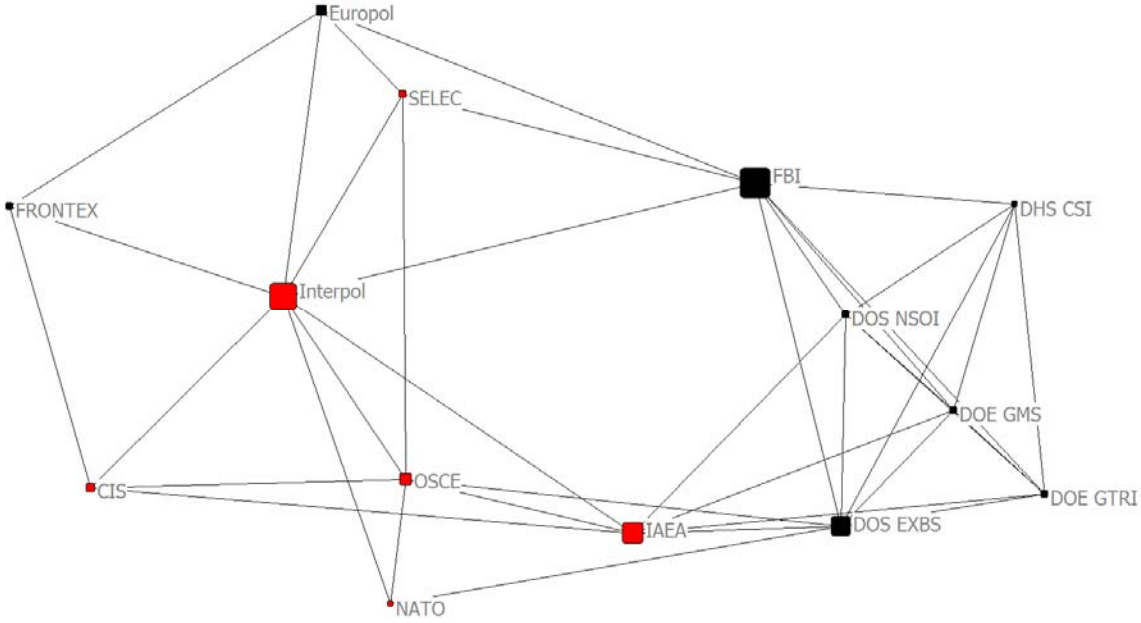

Figure 11. LOE 3 Sociogram

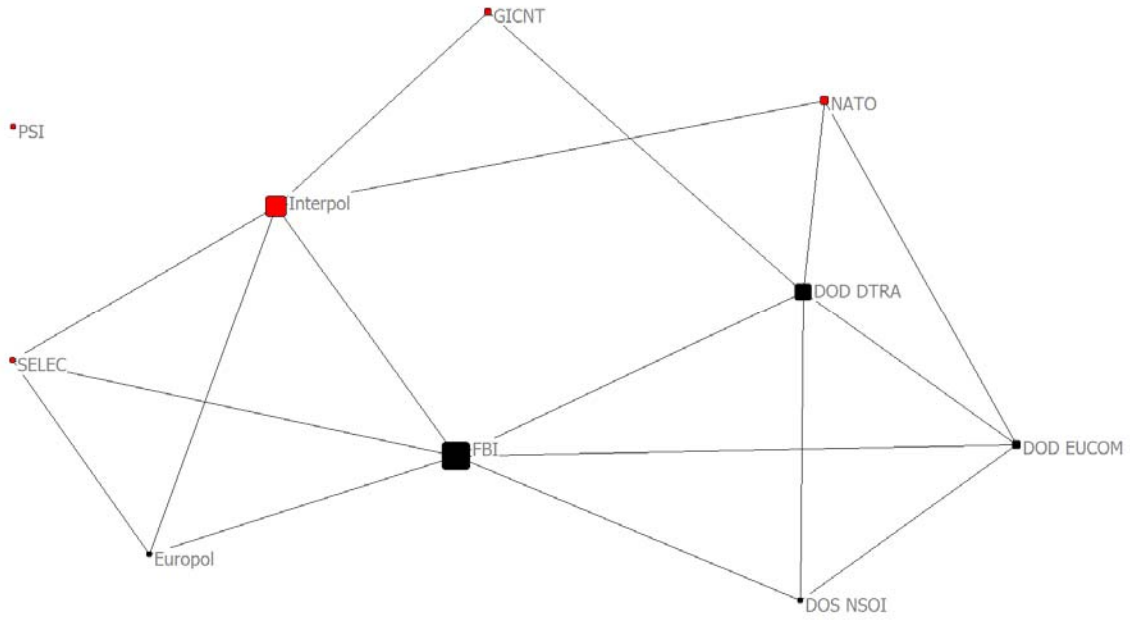

Figure 12. LOE 4 Sociogram

3. Analysis by LOE

Generally, LOE 2 involves cooperation between law enforcement and sensor-focused IGOs and between host-nation LEAs and security forces. Like in LOE 1, the IAEA is the most central node in LOE 2 (see Figure 10); however, numerous other nodes also have operational roles. These include USG programs such as the Department of State's Export Control and Related Border Security program, the Department of Energy's Global Threat Reduction program, and the Department of Homeland Security's Container Security Initiative. The prominence of USG organizations in LOE 2 indicates that there are numerous opportunities to influence European IGOs' and states' efforts to counter transnational shipping of nuclear material.

An emphasis on detection and interdiction of nuclear material links LOEs 2 and 3; however, the generally porous borders in Europe present challenges for LOE 3. Outside of the EU, European border security varies from state to state; the relative ease with which refugees can enter the Schengen Area is also a significant concern for international

CT and CP communities.[115] The open borders within the Schengen Area are intended to allow unobstructed movement between member states, but numerous states in the EU closed borders in early 2016 in order to curb the flow of migrants.[116] If there were a credible WMD threat in Europe, it appears possible that EU states would secure their borders to protect their citizens. Closing borders could enhance LOEs 2–4 temporarily; however, opening communication and information sharing between states is a better long-term solution to the threat of international terrorism.

In order for the nodes in LOE 4 to interdict targets, LOEs 1–3 must pass timely intelligence. Fortunately, both LOEs 3 and 4 are generally state focused, with the FBI and Interpol occupying critical positions in both. Interpol's huge membership, however, indicates that despite its central location in the network, actionable intelligence will most likely travel through another means. This is because states are reluctant to share sensitive intelligence in forums that include numerous diverse members such as the IAEA, which includes 190 member states. Due to the highly sensitive nature of this type of information, the FBI is the most likely organization to connect LOE 3 to the interdiction forces in LOE 4.

The Moldovan interdiction case is a successful application of LOE 4; however, strengthening European interdiction forces would enhance this LOE. The cooperative bilateral relationship between the FBI and Moldovan authorities may indicate that the USG has a robust global network of interdiction forces, but it could also be an unusually effective relationship due to geographic and threat-based requirements. Whether or not the FBI is deeply connected throughout Europe, U.S. CP efforts in Europe could be enhanced by creating redundant capabilities organic to European states. In other words, rather than relying on the FBI to interdict nuclear smugglers in Moldova, the U.S. government could strengthen the network by empowering European organizations with

---

[115] Homeland Security Committee, *Refugee Flows: Security Risks and Counterterrorism Challenges*, Washington D.C., (2015).

[116] Marianne Arens, "Austria Closes Its Borders to Refugees," Global Research Centre for Research on Globalization, January 26, 2016, accessed May 19, 2016, http://www.globalresearch.ca/austria-closes-its-borders-to-refugees/5503754; "Migrant Crisis: Hungary Closes Border with Croatia," BBC, October 17, 2015.

similar capabilities. Enhanced intelligence sharing between Frontex and Europol, both EU subagencies, could achieve this goal; however, in many cases, this would still require individual states to share intelligence with an IGO.

4. Critical Nodes

We see that several entities occupy central positions in numerous phases; however, no one organization is central throughout all the LOEs. The aggregate network showed that Frontex, Europol, and NATO are the most central organizations in the network, but none of these nodes are prominent in the LOE construct. When attempting to connect actors across LOEs, the most significant organizations are the IAEA in LOEs 1 and 2, and both the FBI and Interpol in LOEs 3 and 4. Fortunately there is overlap, as the IAEA is also a player in LOE 3 and Interpol is present in LOE 2. Thus, there is continuity across the LOEs, though no one actor is central to all four.

5. Scenario 2 Conclusions

The network's robust scope and reach are significant assets when countering nuclear smuggling originating outside of the EU; however, the size of the network and the drastically different purposes of its nodes result in the network lacking unity of effort. This could be fixed by identifying and empowering one node that would be central to all four lines of effort. As it stands now, no single IGO in our network has this holistic view of the other nodes and their activities. Therefore, unifying the network may fall to one of the three most central nodes in the strong ties subnetwork.

This scenario requires cooperation between numerous lines of effort, some of which interact only infrequently. In order for these organizations to effectively cooperate in crisis, centralized collaboration should take place pre-crisis. Coordination enables trust among the organizations, which is critical for strong cooperation across agencies, governments, and lines of effort. A European counterproliferation center, similar to the U.S. NCPC and NCTC, could achieve this aim. As a centralized repository for information related to NP and CP, such an agency could interconnect the disparate organizations operating across the four separate lines of effort.

C. CONCLUSION

The analysis and recommendations in this chapter do not address all aspects of the CNS-E network, but provide insights into its functions. The two scenarios provide the following critical takeaways:

- SNA shows that Frontex, NATO, and Europol are the most central actors in the strong ties subnetwork. Analysis of the scenarios revealed that while none of these organizations are prominent in more than one LOE, no organization in the network is prominent across all four LOEs. Therefore, Frontex, NATO, and Europol are the three organizations that may be best positioned to unify the network.

- We see that much of the EU is reliant upon Schengen Area border security. Similar to the U.S. approach to CT outlined in the NMS, the EU could be more proactive outside its own borders. According to SNA, strengthening relations with SELEC could partially achieve this goal in southeastern Europe, while SNA also shows us that the USG, specifically DOE, is in the best position to affect relations with Russia and other former Soviet states. Therefore, the EU could best engage with SELEC and Russia through USG assistance in order to affect security east of its borders.

- IGOs occupy the most central positions in LOEs 1 and 2; the FBI occupies the most central position in LOEs 3 and 4. This suggests that international cooperation is highest in nonproliferation, while bilateral relationships become more critical in CP. IGOs play a role in border security and interdiction; however, the FBI's prominent position in the network suggests that the USG can better affect these LOEs through bilateral relationships with specific states.

- Analysis of the scenarios reveals that, although countering threats emanating from within the Schengen Area involves NP and CP nodes, operationally this scenario is heavily reliant upon individual state security. Thus, proactive IGO involvement may be more efficient for Europe as a whole, but bilateral engagement is the most effective tool for countering nuclear terrorists in Europe.

This chapter enabled qualitative analysis of not only the network but also the findings from SNA. By applying the network to realistic threats in the European theater, we were able to draw conclusions that apply to the broader CP community. The next chapter applies these findings to the larger issues of international relations and interagency cooperation in order to formulate recommendations for policy makers.

V. FINDINGS AND RECOMMENDATIONS

The potential for nuclear terrorism continues to be a threat to Europe and the world. This research has studied the obstacles to cooperation and collaboration with CNS-E efforts and the opportunities that exist to enhance them. The environment in Europe is complex, requiring an agile and adaptive network to suit it. The U.S. and European efforts to address the evolving terrorism networks, which are increasingly less hierarchical and more organic, have become less compartmentalized and have improved their sharing of information. Even as the shared threat of terrorism has provided a common motivation to prevent it, reducing the barriers to cooperation, recent attacks show that improvement is still necessary. International CP efforts lack a shared view of the nuclear threat, which reduces the incentives to cooperate.

Our research sought to better understand how the CNS-E efforts relate to each other through quantitative and qualitative analysis. Through the use of SNA, we analyzed the network's organization and its strengths and weaknesses related to the CP environment. The case studies were a way to analyze the network using plausible scenarios that would reveal the network's current readiness and capability to address a terrorist threat in the future. This chapter will present both the empirical and analytical findings of our research. We will then provide potential recommendations and policy implications for the CNS-E and the broader international security environment. This chapter will conclude with a discussion of future research that is still necessary in this issue area.

A. SUMMARY OF FINDINGS

Our research has determined that, while the CNS-E network fits the mission and environment, it remains difficult for states to share relevant information within the network. Bilateral agreements have been utilized extensively to get around sharing information with the broader network, as was demonstrated in the successful Moldovan interdiction case. While the existence of bilateral agreements can be an indicator of trust between states, these agreements do not assist the broader network in collectively

addressing CP issues. There is a balance between sharing relevant information with the network, which trades efficiency for synchronization, and using bilateral relationships, which are efficient at the expense of network synchronization. The network currently tends to utilize bilateral intelligence sharing rather than networked solutions, which limits the cooperative potential of the network and hinders the synchronization of efforts.[117]

Our recommendations to structurally improve the network's cooperative potential and the policy implications of those recommendations were informed by four major findings. The first identifies that the CNS-E network fits the environment, but that comes at a cost. The CNS-E network is an organic structure. It is highly decentralized, dense, and informal, with no single actor exercising authority over the others. This structure should support quick and reliable information exchange through the multiple pathways between most nodes. Power is also distributed throughout the network, allowing nodes to quickly react to situations as they arise. The relative lack of rules governing the network enables rapid adaptation to the dynamic threats inherent to transnational crimes. Overall, the network is configured well in light of its task of countering nuclear smuggling and the complex and dynamic environment it operates in. On the downside, the lack of an executive authority makes it difficult to ensure the network is moving toward a unified goal and communicating effectively. The extreme decentralization of the network requires time and resource-intensive communication. Failure to coordinate can result in redundant work, or worse, ineffective practices.

Our second finding is that a major obstacle to cooperation and collaboration in CNS-E is the incentive for states to maintain private information. Even with the organizational mechanisms and the relationships in place, states tend to withhold sensitive information that would be helpful to other members of the network. James Fearon argues that a state's desire to have current or future issues resolved in its favor provides strong incentives to maintain private information and in some cases to

[117] For a detailed discussion on enhancing collaboration between actors, see Lothringer et al., "Countering Weapons of Mass Destruction."

misrepresent capability and readiness.[118] Some of the IGOs studied do attempt to share information, and by changing the payoff structure, increasing the time horizon, and mitigating free-rider problems, institutions are able to overcome some of the hurdles.[119] However, key elements of intelligence continue to be difficult to share with a broader community, particularly when doing so entails perceived violations of state sovereignty and sharing information about domestic citizens.[120]

Our third major finding is that the network could benefit from a move toward centralized organization. The current extreme decentralization of the CNS-E network creates several problems. The network lacks a single coherent strategy guiding all actors. The difficulty of coordination in such a decentralized network compounds the lack of strategy. The result is a diverse group of IGOs, agencies, and programs that often have redundant tasks and lead to wasted resources. Though it is unrealistic for any one actor to exercise executive authority over other actors, specifically sovereign states, empowering fewer nodes with broader authority and responsibility would reduce redundant efforts and entities, improve coordination, and make the network more effective.

Our final network finding indicates that the CNS-E network needs stronger relationships, not more relationships. Currently, there are an abundance of ties between actors, but far fewer *strong* ties between actors. Strong ties will facilitate better cooperation and, more importantly, intelligence sharing, which is the most critical task if the CNS-E network is to succeed. The trust needed for states to share high-level intelligence requires strong relationships as a prerequisite. Efforts should focus on strengthening key ties rather than creating more superficial ties.

International governmental organizations, especially regionally focused ones, facilitate strong relationships. Our strong ties subnetwork demonstrates that Europol and Frontex, both agencies of the European Union, account for a significant number of strong relationships in Europe. This is in contrast to international IGOs, like the United Nations

---

[118] Fearon, "Rationalist Explanations for War," 390–400.

[119] Oye, *Cooperation under Anarchy*.

[120] Claudia Hillebrand, *Counter-Terrorism Networks in the European Union: Maintaining Democratic Legitimacy after 9/11* (Oxford: Oxford University Press, 2012).

and INTERPOL. This suggests that regional IGOs are more suitable organizations for countering problems like transnational smuggling—that is, problems that require trust and intelligence sharing.

B. RECOMMENDATIONS AND POLICY IMPLICATIONS

Based on the significant findings, we have four recommendations or implications for policy makers. Our first two recommendations identify strategic policy possibilities to improve information sharing in the international environment while states still have an incentive to keep information private. The second two recommendations provide USSOCOM and NSHQ with operational ways that those unique organizations can impact the network's CP efforts.

Actors in the CNS-E network should focus on strengthening vital ties rather than building numerous weak ties. There are too many actors in the network to establish strong bilateral relations with each, and most actors lack the resources to do so. Furthermore, there is little value in establishing and maintaining superficial relations. Each actor should strategically target specific ties that contribute most to its policy objectives and strengthen those ties. The best ways to establish strong ties are highly dependent on the actor and situation. In general, bilateral efforts may provide the highest likelihood of achieving strong relations but are resource intensive. The next-best option is participation in regional IGOs. These organizations can provide strong multilateral relations and are more efficient than the bilateral approach.

In order for organizations in the network to enhance cooperation, communities of practice should exist both physically and in virtual space to facilitate the sharing of relevant information and intelligence when necessary. Major IGOs—potentially NATO, the EU, or SELEC—could serve as communications hubs to which other entities, sub-IGOs and states, send liaisons in order to create an environment where resources and authorities can be fused to create a whole greater than its parts. A regional or functional approach would reduce the number of participants and encourage broader information sharing within the communications hubs. Additionally, by centralizing the network, this could provide better unity of effort for planning while retaining agility in execution. The

USSOCOM J3I or Europol structure could act as a model for future communications hubs. In both cases, the sponsor agency provides a collaborative space where liaisons—senior representatives of their parent agencies—interact both formally and informally to facilitate the transfer of information and intelligence across the network to address current requirements as effectively as possible.

USSOCOM and NSHQ could have a positive impact in the CNS-E network by working with member-state law enforcement agencies to enhance interdiction capabilities. Limitations in legal authority often preclude partner SOF from operating within their own borders; therefore, engaging with LEAs enables SOF and other U.S. agencies to enhance partner-nation capabilities. In recent years, USSOF trained with European partners to enhance the partner nations' abilities to conduct expeditionary coalition operations and to counter traditional threats such as Russia. Historically, USSOF also conduct military engagements to counter partner-nation internal threats. Expanding these missions to include engagements with partner LEAs could enhance CT and CP interoperability and cooperation.

USSOCOM and NSHQ could enhance the CNS-E network by working with U.S. agencies, IGOs, and partner nations to assess and improve security in European states. Assessment teams, known as red cells, could identify vulnerabilities in order to enhance partner-nation security at nuclear facilities, as well as at possible targets. The red cells would plan attacks as if they were terrorists in order to test security and law enforcement response. These missions would provide valuable training for both the SOF unit reconnoitering and planning the attack and the security forces that must respond to a sophisticated threat. Red cell activities could include assessments of security at airports, train stations, stadiums, and cultural centers deemed to be likely targets. This could enhance both LOEs 1 and 4 by repurposing existing SOF engagements in Europe.

C. FUTURE RESEARCH

The CNS-E is complex and therefore presents many opportunities for future research. Countering nuclear smuggling requires interactions of multiple states, IGOs, NGOs, and multinational corporations (MNCs). Future research is necessary to better

understand the impacts of NGOs and MNCs on the CP network. Government-affiliated organizations are often denied access to areas that NGOs can access due to their politically neutral status. Better understanding NGOs' missions, areas of operation, and motivations could enhance the network's scope and reach. MNCs, on the other hand, vary in their willingness to cooperate with state governments and generally are motivated exclusively by profits; they are often also the vehicles for transfers of dual-use technologies that, in the wrong hands, could be used for nefarious purposes. An assessment of the MNCs in a given theater could identify potential proliferation risks and opportunities to engage with MNCs for CP purposes.

Further research is also necessary to determine ways in which the CNS-E could overcome the challenges of sharing sensitive information and timely intelligence to better cooperate in CP efforts. While we have made a few recommendations on ways to structurally change or adapt the network to facilitate intelligence sharing, fully exploring this subject was outside the scope of our project. Finally, additional research into the current nuclear smuggling threat would be helpful to better understand CNS-E requirements. As with many research efforts, countering nuclear smuggling is a dynamic field that is constantly adjusting as multiple entities seek to outmaneuver the others. Our research marks a beginning to understanding this complex issue area and providing ways to improve counterproliferation efforts in the international arena to address the evolving threat.

APPENDIX A. FUNDAMENTALS OF SOCIAL NETWORK ANALYSIS

SNA is an assembly of theories and methods from varying academic disciplines including sociology and statistics. It was developed to fulfill the need for an empirically based social science.[121] Though its beginnings are in sociology, today it is employed in many fields, from anthropology to economics. The goal of SNA is to study the causes and consequences of network structures through empirical methods; a fundamental assumption of SNA is that the behavior and values of an individual are determined not by individual characteristics but by the structure of the networks in which the individual is embedded.[122] For example, in explaining the different outcomes of two identical businesses located in different industrial cities, an individualistic approach would examine attributes of each business such as leadership, management, etc. SNA examines the structure of the networks of each business and the position each business occupies within its network. Perhaps the successful business was located in an industry hub with better access to important partners, like Silicon Valley. SNA works on the premise that this kind of analysis is vital to understanding the behavior and effectiveness of any given organization or entity.

A. BASIC TERMINOLOGY

All social networks consist of two elements: a limited set of actors and the relations between the actors. This includes a variety of common people groups, from families to businesses. A common mistake is to assume networks only include groups that have specific structural characteristics. Most commonly, it is assumed that only highly decentralized groups, such as terrorist groups, qualify as networks.[123] This is not the case. A company with a rigid hierarchy is still a network. Importantly, SNA is not limited to networks of individuals. The actors comprising the network, called *nodes*, can

[121] Everton, *Disrupting Dark Networks*, 4–5.

[122] S. P. Borgatti et al., "Network Analysis in the Social Sciences," *Science* 323, no. 5916 (February 13, 2009), 892–895.

[123] Everton, *Disrupting Dark Networks*, 142.

be individual people, groups of people, or institutions and are represented by dots on a sociogram (network map). The relationships between nodes are called *ties*, represented by lines on a sociogram. A tie can be any of a variety of relations including friendship, respect, communication, etc. Ties can also be directional; for example, they may show one-way communication between actors. Lastly, ties vary by strength. If a feeling of trust is scaled from 1–3, the strength of the tie can be represented visually and factored into the numerous metrics. *Attributes* are characteristics of a node and can include information such as age and gender for an individual or democracy score or gross domestic product for a country. The structure of the network is called *topography* and is characterized by several dimensions and determined by the arrangement of nodes and the ties between them.[124]

B. ASSUMPTIONS

In *Disrupting Dark Networks*, Dr. Sean Everton lists several assumptions as the foundation for SNA methods.[125] They are:

- Actors and their actions are interdependent on one another, not independent.
- Social structures are made up of patterns of ties between actors.
- Patterns of ties create social networks that exhibit their own characteristics and are more than the sum of their parts.
- An actor's behavior, beliefs, and norms are greatly influenced by their position in a social network.

C. ANALYTICAL PERSPECTIVES

Networks can be analyzed from different perspectives and at different levels depending on the researcher's needs. Each type of analysis illuminates separate characteristics of the network. SNA evaluates networks from two perspectives: roles and positions.[126] A role-based approach focuses on the direct and indirect ties between actors

[124] Ibid., 4–14.

[125] Ibid., 14–15.

[126] Ibid., 13.

and the effects those ties have on behavior. Ties between actors form a social structure, much like a physical structure, which exhibits varying configurations and behavior. A position-based approach looks for nodes or groups that occupy similar positions in the network, called structural equivalence. When actors have comparable ties to other comparable actors, they are considered structurally equivalent.[127] For instance, if one is analyzing a school district, one will find that the principals of each school have similar ties to other actors in the network, such as teachers and administrators. The social structure surrounding each principle will be similar, creating a structural equivalence. Importantly, it can be assumed that structurally equivalent nodes, even lacking connection, will behave similarly.[128]

The different levels of analysis include micro (individual), meso (group), and macro (organizational).[129] The microlevel of analysis is focused on individual nodes. The most common metrics applied at the microlevel are types of centrality. There are numerous measures of centrality, all of which assess the importance or influence of a node in the network. What determines importance varies depending on the type of tie and the function of the network. When trying to identify the actor with the most support in a trust network, degree centrality—that is, having the most direct ties—may be the most important factor. If trying to identify the actor who can most efficiently pass intelligence throughout an information-sharing network, betweenness centrality—that is, how frequently an actor lies on the shortest path between any pair of other actors in the network—may be the most important. Closeness centrality is another metric indicating importance and measures how close an actor is, by average distance, to all other actors in the network. Eigenvector centrality weighs ties by how central the actors are on the other end of the tie; ties to more-central actors are weighted more heavily than ties to peripheral actors.[130] In addition to centrality, brokerage is an important position at the node level. A broker connects otherwise separated actors or groups of actors. Given their

[127] Ibid.

[128] Ibid.

[129] Ibid., 5.

[130] Everton, *Disrupting Dark Networks*.

position, it is assumed brokers control the flow of information or resources.[131] Lastly, attributes of actors are often added to networks to help make sense of network structure. For example, when looking at friendship ties among university faculty, attributes such as gender, age, or department affiliation may correlate with structures within the network.

Analysis at the mesolevel is focused on subgroups within the network. A *subgroup* is a cluster of nodes that have strong ties with one another as compared with the rest of the network. It is assumed that subgroups, due to their stronger ties, will share norms and exhibit similar behavior.[132] There is an abundance of methods for detecting subgroups in a network, each with a different algorithm and definition of a subgroup. *Components* are subgroups composed of actors tied directly or indirectly to one another, but not tied to other subgroups. Components are better identified in directed networks and may not be a useful concept for undirected and dense networks. One type of component is a *clique*, a subgroup in which each actor is directly connected to all other actors. Cliques are considered a strong type of subgroup because of the direct and intense ties between all actors. However, in reality it is difficult to find subgroups that qualify as cliques because lack of complete connectedness. The concept of *K-cores* is a method for detecting subgroups. It identifies all actors who share a number (*K*) of ties. All actors in a three-core will have three or more ties to other actors in the three-core. The last subgroup detection method covered is *Newman groups*. This method identifies subgroups as those with more internal ties and fewer external ties than a randomized graph of equal size and number of ties would have.[133] In addition to ties, attributes can also be used to identify subgroups.

The macrolevel of analysis focuses on the structure, or topography, of the whole network. Understanding the structure of a network is crucial for two reasons. First, actors within the network and their behavior, opportunities, and constraints are largely determined by structure. Second, the structural characteristics determine what tasks a

[131] Ibid., 13.

[132] Ibid., 12.

[133] Ibid., Ch 6.

network will succeed or fail at.[134] The most important structural features are density and centralization. *Density* is the degree to which a network is connected. Highly dense networks have a greater degree of influence over their members and can share information more efficiently than sparse networks. *Centralization* is the degree to which a network is centered on a few actors; it is associated with hierarchy. Hierarchal networks exhibit greater control and can perform mundane tasks more efficiently than heterarchical networks.[135] Both density and centralization have their own measures; still, they should be considered side by side when analyzing structure. Other measurements including network size (number of nodes), diameter (the longest geodesic), and average distance between all nodes should also be considered. The structure of a network often conforms to one of several configurations identified by organization design theorists. Identifying the configuration of a whole network provides the analyst with significant insights into the strengths and weaknesses of the network.

Social network analysts look at networks from different perspectives—roles and positions—and at different levels—micro, meso, and macro. What underpins each type of analysis is structuralism. This tenet of SNA regards the social structure as a critical factor influencing actors in a network. Every measurement, in some fashion, provides information about the social structure of the network, either at the node, group, or network level. Analysts disagree, however, about how much influence structure has on actors.[136] The structural determinist considers structure as the sole cause of behavior and removes human agency as a factor. Conversely, structural instrumentalists recognize the significance of structure but allow for other factors, including rational choice and maximum utility. Structural constructionism also allows for human agency, but as it concerns norms, culture, and behavioral economics.

---

[134] Ibid., 10–11.

[135] Ibid., 136–142.

[136] Everton, *Disrupting Dark Networks*.

D. EXPLANATIONS

There are four mechanisms that explain how networks, or the position of nodes, cause certain outcomes.[137] The most widely applied mechanism is *transmission*. Transmission views ties within a network as conduits for the flow of physical and nonphysical things. Ideas, services, trust, disease, and communication are all examples of the types of things that can be transmitted through a network. This explanation typically looks at metrics that show how well a network transmits things and which actors control the flow of those things. The concept of *adaptation* states that nodes will exhibit the same behavior when they occupy similar positions in the network—that is, the structure of the ties and types of actors they are connected to are comparable. It follows that two actors in similar positions within a network will have similar opportunities and constraints. *Binding* occurs when two or more nodes join together and create something greater than the sum of their parts. When nodes bind together, a structure is created and a group with its own dynamics forms. Lastly, *exclusion* occurs when a tie between two nodes excludes a tie with a third node and further undermines the third node's relations with others. This is commonly seen in competitive situations like bargaining.[138] If a business is in dire need of an engineer and two engineers apply for the job, the business has its choice. However, if one of the engineers takes another job, now the choice is removed and the bargaining power of the remaining engineer is increased. These four mechanisms—transmission, adaptation, binding, and exclusion—underpin the majority of causal explanations in SNA.

[137] Marin and Wellman, "Social Network Analysis."

[138] Ibid.

APPENDIX B. NON-STATE ACTOR LIST

This appendix provides a brief description of the IGOs, international agreements, and sub-state actors in the CNS-E network.

Commonwealth of Independent States. The CIS is a regional association of states that aims to improve multistate cooperation in trade, finance, lawmaking, and security. It has an established free trade zone and a collective defense alliance that are open to all members.

Comprehensive Nuclear Test Ban Treaty Organization. The major tasks of the CTBTO are to promote the Comprehensive Nuclear Test Ban Treaty (CTBT) and to enhance the verification regimes. The CTBT bans nuclear explosions by all countries to impede the development of new or improved nuclear weapons.

DHS Container Security Initiative. CSI is a program implemented by the Bureau of Customs and Border Protection under the U.S. Department of Homeland Security. The purpose of the program is to mitigate threats from cargo containers bound for the United States. It achieves this by screening cargo containers at international ports.

DoD Defense Threat Reduction Agency. DTRA is an agency of the U.S. Department of Defense. It is the primary combat support agency for countering WMDs. DTRA's primary functions include threat reduction, threat control, and combat support.

DoD European Command. USEUCOM is a U.S. Department of Defense Combatant Command for the European theatre. Their key tasks include countering transnational threats, and maintaining ready forces for contingencies plans.

DOE Global Threat Reduction Initiative. GTRI is a program of the U.S. Department of Energy. Its primary mission is to prevent nuclear terrorism by converting, removing, or protecting vulnerable nuclear material at civilian facilities worldwide.

DOE Global Material Security. GMS is an office of the U.S. Department of Energy. Its mission is to prevent nuclear proliferation by helping partner countries secure

nuclear-related material and build the capacity to prevent the illicit trafficking of such material.

DOS Export Control and Related Border Security. EXBS is a program of the U.S. Department of State. Its mission is to prevent the proliferation of weapons of mass destruction by helping partner countries establish effective trade control systems and build capacity to enforce border security.

DOS Nuclear Smuggling Outreach Initiative. NSOI is a program of the U.S. Department of State. Its mission is to prevent international nuclear smuggling by partnering with select countries to increase their ability to prevent, detect, and interdict smuggled nuclear-related material.

European Union. The EU is a political and economic union of 28 European countries. Its establishment has enabled the free movement of people, goods, and money across most of the European continent. The EU has its own governing body that coordinates policy across the member states in the realms of security, justice, environment, human rights, and health.

European Union CBRN Centers of Excellence. The CBRN COE is a program of the EU. Its mission is to increase regional security by strengthening the capacity of states, external to the EU, to mitigate CBRN risks. It achieves this by providing expertise and funding to partner nations to overcome identified gaps in mitigation capabilities.

Europol. Europol is the law enforcement agency of the EU. Its mission is to maintain European security by assisting and facilitating cooperation between member states to fight serious transnational crime and terrorism.

Federal Bureau of Investigation. The FBI is the primary domestic intelligence and law enforcement agency for the United States. Its primary mission is ensuring U.S. national security by conducting counterterrorism and counterintelligence activities, as well as criminal investigations.

Frontières Extérieures. Frontex is the border security agency of the EU. Its mission is to help secure the European Union's external borders by promoting, coordinating, and developing border management practices between member states.

G7 Global Partnership. The G7 is an intergovernmental forum comprising seven major industrialized countries and the EU. It serves as the primary forum to discuss global issues such as international security cooperation and economic growth. The G7 supports non-proliferation through the Global Partnership Against the Spread of Weapons and Material of Mass Destruction.

International Atomic Energy Agency. The IAEA is an international organization established to be the world's center for nuclear cooperation. It is responsible for the safe and peaceful use of nuclear technology around the world. The IAEA conducts numerous activities to achieve their mission from establishing safety and security guidelines to inspecting nuclear facilities.

Interpol. Interpol is an intergovernmental organization with the primary task of fighting transnational crime such as terrorism, weapons smuggling, and drug trafficking. They facilitate international law enforcement cooperation and assist member states to combat crime.

North Atlantic Treaty Organization. NATO is a political and military alliance comprising mostly European countries, the United States, and Canada. The alliance promotes democratic values and cooperation in security and defense.

Nuclear Security Summit. The NSS comprised three international summits focused on preventing nuclear terrorism. The summits produced commitments and declarations of intent from attending countries to improve nuclear security.

Nuclear Suppliers Group. NSG is an intergovernmental organization comprising countries that export nuclear material or equipment. It aims to prevent nuclear proliferation by implementing guidelines for nuclear and nuclear-related exports.

Organization for Security Co-operation in Europe. OSCE is an intergovernmental organization comprising 57 countries from Europe, North America,

and Central Asia. The organization is focused on security cooperation across multiple dimensions including military, political, economic, and human.

Proliferation Security Initiative. PSI is an international agreement aimed at preventing the trafficking of WMDs and related material. Participating states commit to interdiction principles that include establishing the capacity to detect and interdict WMD material and establishing laws to facilitate the interdiction and seizure of such material.

Southeast European Law Enforcement Center. SELEC is a regional, intergovernmental organization facilitating cooperation between the law enforcement agencies of member states. The primary mission for SELEC is to prevent and combat transnational crime.

United Nations Security Council Resolution 1540 Committee. The UNSCR 1540 Committee is a sub-committee of the United Nations Security Council and is charged with the implementation of UNSCR 1540. UNSCR 1540 affirms the proliferation of CBRN weapons, or related material, is a threat to international peace. The treaty obligates members to legislate and enact various non-proliferation measures.

United Nations. The UN is an intergovernmental organization with a primary purpose of maintaining international peace and security. In addition, the UN encourages friendly relations between its member states to further international cooperation on a range of issues from humanitarian aid to human rights.

Zangger Committee. The Zangger Committee is an intergovernmental organization comprising 39 member states. The purpose of the committee is to offer guidance to its member states by interpreting Article III, paragraph 2 of the Nuclear Non-Proliferation Treaty which specifies that fissionable-related material must be subjected to IAEA safeguards prior to export.

APPENDIX C. DATA COLLECTION

To assess the Counter Nuclear Smuggling-Europe network, it was necessary to construct a data set that valued specific relations between actors in the network. This appendix lists the references that were used to build the data set. The majority of the references are information webpages proprietary to the actors in the network.

Anicon, Admirela. "Statement for the OSCE Workshop to Identify the Proper Role of the OSCE in the Facilitation of the UN Security Council Resolution 1540." Organization for Security and Co-operation in Europe. http://www.osce.org/secretariat/75143?download=true

"Assistance Programmes and Offers from International, Regional and Subregional Organizations and other Arrangement." United Nations 1540 Committee. http://www.un.org/en/sc/1540/assistance/offers-of-assistance/assistance-programmes.shtml

"CBRN Centers of Excellence." United Nations Interregional Crime and Justice Research Institute." http://www.unicri.it/topics/cbrn/coe/

"CBRNE." Interpol. http://www.interpol.int/Crime-areas/CBRNE/CBRNE

"COE – The Countries." CBRN Center of Excellence. http://www.cbrn-coe.eu/4.html

"Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenges." Government Accountability Office. http://www.gao.gov/assets/650/649759.pdf

"The Commonwealth" http://thecommonwealth.org/member-countries

"Commonwealth of Independent States (CIS)." GlobalSecurity.Org. http://www.globalsecurity.org/military/world/int/cis.htm

"Commonwealth of Independent States (CIS)." Interstate Statistical Committee of the Commonwealth of Independent States. http://www.cisstat.com/eng/frame_about.htm

"Container Security Initiative in Summary." U.S. Customs and Border Protection. http://www.cbp.gov/sites/default/files/documents/csi_brochure_2011_3.pdf

"Cooperation Agreement Between The Southeast Law Enforcement Center and the International Criminal Police Organization – Interpol." Interpol. http://www.interpol.int/contentinterpol/search?SearchText=SELEC&x=0&y=0

"Core Program." National Nuclear Security Administration. http://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-4

"Countries of Europe." Encyclopedia Britannica. http://www.britannica.com/topic-browse/Countries-of-the-World/Countries-of-Europe

"CTBTO to Share Data with IAEA and WHO." Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty. https://www.ctbto.org/press-centre/press-releases/2011/ctbto-to-share-data-with-iaea-and-who/

"Department of Defense Cooperative Threat Reduction Program Fact Sheet." Defense Threat Reduction Agency. http://www.dtra.mil/Portals/61/Documents/DoD_CTR_Fact_Sheet-2012NuclearSecuritySummit.pdf

"EU Agencies." FRONTEX. http://Frontex.europa.eu/partners/eu-partners/eu-agencies/

"EU Delegations and Offices Around the World." European Union External Action. http://eeas.europa.eu/top_stories/2015/infographic_eu_delegation_en.htm

"EU Increases its Financial Support to the CTBTO." European Union External Action. http://eeas.europa.eu/delegations/vienna/press_corner/news_un/2015/20151019_en.htm

"EU Member Countries." European Union. http://europa.eu/about-eu/countries/member-countries/index_en.htm

"EU Relations with the United States of America." European Union External Action. http://eeas.europa.eu/us/index_en.htm

"Eurasian Criminal Enterprises." Federal Bureau of Investigation. https://www.fbi.gov/about-us/investigate/organizedcrime/eurasian

"Europol Supports Huge International Operations To Tackle Organized Crime." Europol. https://www.europol.europa.eu/content/europol-supports-huge-international-operation-tackle-organised-crime

"External Cooperation." Europol. https://www.europol.europa.eu/content/page/external-cooperation-31

"Fiscal Year 2012 Budget Estimates Defense Threat Reduction Agency." Department of Defense Comptroller. http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2012/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/O_M_VOL_1_BASE_PARTS/DTRA_OP-5_FY_2012.pdf

"Global Initiative to Combat Nuclear Terrorism: Partner Nation List." Global Initiative to Combat Nuclear Terrorism. http://www.gicnt.org/content/downloads/partners/GICNT_Partner_Nation_List_June2015.pdf

"Global Nuclear Safety and Security Networks: Partners." International Atomic Energy Agency. https://gnssn.iaea.org/main/Pages/Partners.aspx

"Global Partnership Against the Spread of Weapons And Material of Mass Destruction ("10 Plus 10 Over 10 Program")." Nuclear Threat Initiative. http://www.nti.org/learn/treaties-and-regimes/global-partnership-against-spread-weapons-and-materials-mass-destruction-10-plus-10-over-10-program/

"GTRI: Reducing Nuclear Threats." National Nuclear Security Administration. http://nnsa.energy.gov/mediaroom/factsheets/reducingthreats
"GTRI's Convert Program: Minimizing the Use of Highly Enriched Uranium." National Nuclear Security Administration. http://nnsa.energy.gov/mediaroom/factsheets/gtri-convert

"International Cooperation." Defense Threat Reduction Agency. http://www.dtra.mil/Missions/PartnersandCustomers/InternationalCollaborationTowardReducingtheWM.aspx

"International Cooperation." International Atomic Energy Agency. https://www.iaea.org/INPRO/cooperation/

"International Organizations." FRONTEX. http://Frontex.europa.eu/partners/international-organisations/

"International Partners." Interpol. http://www.interpol.int/About-INTERPOL/International-partners/Public-partners

"Interpol and OSCE to Collaborate on Police Training Activities." Interpol. http://www.interpol.int/News-and-media/News/2014/N2014–092

"Jane's Sentinel Security Assessments-Country Profiles." IHS Janes. https://janes.ihs.com/Grid.aspx

"Legal Attaché Offices – Europe." Federal Bureau of Investigation. https://www.fbi.gov/contact-us/legat/legal_offices/europe

"List of Non-member States, Entities, and Organizations Having Received a Standing Invitation to Participate as Observers in the Sessions and the Work of the General Assembly." United Nations General Assembly. http://www.un.org/ga/search/view_doc.asp?symbol=A/INF/70/5

"Locations." Defense Threat Reduction Agency. http://www.dtra.mil/About/Locations.aspx

"Material Protection, Control, and Accounting Program." National Nuclear Security Administration. http://nnsa.energy.gov/mediaroom/factsheets/protectioncontrolaccounting

"Member States." International Atomic Energy Agency. https://www.iaea.org/about/memberstates

"Member States." Europol. https://www.europol.europa.eu/content/page/member-states-131

"Member States." United Nations. http://www.un.org/en/members/index.shtml

Mueller, Robert S. "Speeches: Global Initiative Nuclear Terrorism Conference." Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/nuclear-terrorism-prevention-is-our-endgame

"National Authorities." FRONTEX. http://Frontex.europa.eu/partners/national-authorities/

"National Guard State Partnership Program." Defense Threat Reduction Agency. http://www.eucom.mil/key-activities/partnership-programs/national-guard-state-partnership-program

"NATO Member Countries." North Atlantic Treaty Organization. http://www.nato.int/cps/en/natohq/nato_countries.htm

"NNSA Achievements: 2015 by the Numbers." National Nuclear Security Administration. http://nnsa.energy.gov/content/2015-year-review

"NSG 2014 Plenary." United Nations. http://www.un.org/en/sc/1540/pdf/NSG%20Letter%20re%20effective%20practices%202014.pdf

"Nuclear Smuggling Outreach Initiative: Results to Date and Highest Priority Projects Needing Funding." Department of State. http://www.pub.iaea.org/mtcd/meetings/PDFplus/2009/cn166/CN166_Presentations/Session%20%2010/044%20Stafford.pdf

"Nuclear Suppliers Group (NSG)." Nuclear Threat Initiative. http://www.nti.org/learn/treaties-and-regimes/nuclear-suppliers-group-nsg/

"OSCE Supports States to Stop Proliferation of Weapons of Mass Destruction." Organization for Security and Co-operation in Europe. http://www.osce.org/fsc/91950

"OSCE Training in Turkey Focuses on Detecting Forged Travel Documents." Organization for Security and Co-operation. http://www.osce.org/secretariat/118421

"Other Partners." Organization for Security and Co-operation in Europe. http://www.osce.org/networks/111486

"Overview of the Export Control and Related Border Security (EXBS) Program." Department of State. http://supportoffice.jp/outreach/2014/asian_ec/pdf/day2/1000_Mr.AndrewChilcoat.pdf

"Participants." Nuclear Suppliers Group. http://www.nuclearsuppliersgroup.org/en/participants1

"Participating States." Organization for Security and Co-operation in Europe. http://www.osce.org/states

"Partner States and Organizations." Organization for Security and Co-operation in Europe. http://www.osce.org/partners

"Partnership Programs." United States European Command. http://www.eucom.mil/key-activities/partnership-programs

"Partnerships: a Cooperative Approach to Security." North Atlantic Treaty Organization. http://www.nato.int/cps/en/natohq/topics_84336.htm

"Partnerships." International Atomic Energy Agency. https://www.iaea.org/technicalcooperation/Partnerships/

"Past Summits." Nuclear Security Summit. http://www.nss2016.org/past-summits/2014/

"PSI Endorsing States." Proliferation Security Initiative. http://www.psi-online.info/Vertretung/psi/en/03-endorsing-states/0-PSI-endorsing-states.html

"Southeast European Law Enforcement Center (SELEC) Anti-Terrorism Task Force." Harvard Law School Program on International Law and Armed Conflict (PILAC). http://pilac.law.harvard.edu/europe-region-efforts//southeast-european-law-enforcement-center-selec-anti-terrorism-task-force

"Staff Statistics." Europol. https://www.europol.europa.eu/content/page/staff-statistics-159

"Standing as an International Organization." Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty. https://www.ctbto.org/the-organization/ctbto-preparatory-commission/standing-as-an-international-organization/

"Status of Signature and Ratification." Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty. https://www.ctbto.org/the-treaty/status-of-signature-and-ratification/

"The EXBS Program: Export Control and Related Border Security." Department of State. http://www.state.gov/documents/organization/126248.pdf

"Third Countries." FRONTEX. http://Frontex.europa.eu/partners/third-countries/

Tolipov, Farkhod. "Ukraine and the CIS Perspective: Implications for Central Asia." The Central Asia-Caucasus Analyst. http://www.cacianalyst.org/publications/analytical-articles/item/12949-ukraine-and-the-cis-perspective-implications-for-central-asia.html

"U.S. and Armenia Mark Cooperative Efforts to Prevent Proliferation of Weapons of Mass Destruction." Embassy of the United States Yerevan, Armenia. http://armenia.usembassy.gov/news030614.html

"United States." United Nations 1540 Committee. http://www.un.org/en/sc/1540/assistance/states/USA.shtml

"World." Interpol. http://www.interpol.int/Member-countries/World

"Zangger Committee." FOI Swedish Defence Research Agency. http://www.foi.se/en/Customer--Partners/Projects/zc/zangger/

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allison, Graham T., and Morton H. Halperin. “Bureaucratic Politics: A Paradigm and Some Policy Implications.” *World Politics* 24, (1972): 40–79.

Allison, Graham T., and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis.* New York: Longman, 1999.

Aloise et al. *IAEA Has Strengthened Its Safeguards and Nuclear Security Programs, but Weaknesses Need to Be Addressed*. Washington, DC: Government Accountability Office, October 2005.

Arens, Marianne. “Austria Closes Its Borders to Refugees.” Global Research Centre for Research on Globalization, January 26, 2016. http://www.globalresearch.ca/austria-closes-its-borders-to-refugees/5503754.

Arquilla, John, and David Ronfeldt. “The Advent of Netwar (Revisited).” In *Networks and Netwars,* edited by John Arquilla and David Ronfeldt. Santa Monica: RAND, 2001.

Banks, Catherine M., and J. A. Sokolowski. “From War on Drugs to War against Terrorism: Modeling the Evolution of Colombia’s Counter-Insurgency.” *Social Science Research* 38, no. 1 (December 2009): 146–154. doi:10.1016/j.ssresearch.2008.08.001

Banks, Jeffrey S., and Eric A. Hanushek. Introduction to *Modern Political Economy: Old Topics, New Directions,* edited by Jeffrey S. Banks and Eric A. Hanushek. New York: Cambridge University Press, 1995.

Bayley, David H., and Robert M. Perito, *The Police in War: Fighting Insurgency, Terrorism, and Violent Crime*. Boulder: Lynne Rienner Publishers, 2010..

Berejikian, Jeffrey D. “A Cognitive Theory of Deterrence.” *Journal of Peace Research* 39, no. 2 (2002): 165–183.

Borgatti, S. P., A. Mehra, D. J. Brass, and G. Labianca. “Network Analysis in the Social Sciences.” *Science* 323, no. 5916 (February 13, 2009): 892–895.

Bucci, Steven. “The Importance of Special Operations Forces Today and Going Forward.” In *2015 Index of U.S. Military Strength*, edited by Dakota Wood. Washington, DC: Heritage Foundation, 2015.

Bueno de Mesquita, Bruce. “Domestic Politics and International Relations.” *International Studies Quarterly* 46, no. 1 (2002): 1–9.

Bunn, Mathew. “Belgium Highlights the Nuclear Terrorism Threat and Security Measures to Stop It.” *World Post*, March 29, 2016. http://www.huffingtonpost.com/matthew-bunn/belgium-nuclear-terrorism_b_9559006.html.

Bunn, Mathew, Martin B. Malin, Nikolas Roth, and William H. Tobey. “Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?” Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School (March 2016).

Butler, Desmond, and Vadim Ghirda. “AP INVESTIGATION: Nuclear Black Market Seeks IS Extremists.” Associated Press, October 7, 2015.

Carter, Ashton. “How to Counter WMD.” *Foreign Affairs* 83, no. 5 (September–October 2004): 72–13.

Chairman of the Joint Chiefs of Staff, The National Military Strategy of the United States of America 2015. Washington D.C., 2015.

Chazan, David, Henry Samuel, Rory Mulholland, and Camilla Turner. “Brussels Attacks: Nuclear Breach Fears as Two More Charged with Terror Offences.” *Telegraph*, March 27, 2016.

“CNS Global Incidents and Trafficking Database.” Nuclear Threat Initiative, March 2016. http://www.nti.org/analysis/reports/cns-global-incidents-and-trafficking-database/.

Cunningham, William T., Brain J. Dowd, Samuel Kim, Tad T. K. Tsuneyoshi, and Adam Woytowich. “Too Big to Fail: The U.S. Government Counter Weapons of Mass Destruction Enterprise.” Master’s thesis, Naval Postgraduate School, 2014.

Curtis, Glenn, and Tara Karacan. *The Nexus among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe*. Washington, DC: The Library of Congress, 2002.

Daft, Richard. *Essentials of Organization Theory and Design*. South-Western: Thomson Learning, 2003.

De Clercq, Geert, “Update 2-Belgian Doel 4 Nuclear Reactor Closed Till Year-End,” *Reuters*, August 14, 2014.

Everton, Sean F. *Disrupting Dark Networks*. Vol. 34. New York, NY: Cambridge University Press, 2012.

“Fact Sheet on Dirty Bombs.” United States Nuclear Regulatory Commission, December 12, 2014. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.html.

Fearon, James D. “Domestic Political Audiences and the Escalation of International Disputes.” *American Political Science Review* 88, no. 3 (1994): 577–592.

———. “Rationalist Explanations for War.” *International Organizations* 49, no. 3 (1995): 379–414.

Fowler, Marcy, and Alisa Carrigan. “Nuclear Security in European Union Member States.” *EU Non-Proliferation Consortium Non-Proliferation Papers,* No. 44, (April 2015): 1–18.

Freedman, Lawrence. “Norms and Criminality.” In *Deterrence*. Malden: Polity Press, 2004.

Fukuyama, Francis. *The Great Disruption*. New York: Touchstone, 2000.

Government Accountability Office. *Interagency Collaboration: Key Issues for Congressional Oversight of National Strategies, Organizations, Workforce, and Information Sharing*. GAO-09–904SP. Washington D.C., 2009.

Gilsinan, Kathy. “Why Moldova May Be the Scariest Country on Earth.” *Atlantic*, October 8, 2015.

Graham, Bob, Jim Talent, Graham Allison, Robin Cleveland, Steve Rademaker, Tim Roemer, Wendy Sherman, Henry Sokolski, and Rich Verma. Hanneman, Robert A., Mark Riddle. *Introduction to Social Network Methods*. PDF ed. Riverside, CA: University of California Riverside, 2005.

Graham, Bob et al. *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism.* New York: Vintage Books, 2008.

Hanneman, Robert A., and Mark Riddle, *Introduction to Social Network Methods*, PDF ed. Riverside, CA: University of California Riverside, 2005.

Hetrick, Keturah. “How Bad Would a Radiological Terror Attack Be?” *Defense One*, April 1, 2016. http://www.defenseone.com/threats/2016/04/how-bad-would-radiological-terror-attack-be/127188/.

Heuser, Beatrice. “The Cultural Revolution in Counter-Insurgency.” *Journal of Strategic Studies* 30, no. 1 (Feb 2007, 2007): 153–171. http://search.proquest.com.libproxy.nps.edu/docview/59759940?accountid=1270.

Hill, Christopher, and William Wallace, “Introduction: Actors and Actions,” in *The Actors in Europe’s Foreign Policy,* ed. Christopher Hill. New York: Routledge, 1996.

Hillebrand, Claudia. *Counter-Terrorism Networks in the European Union: Maintaining Democratic Legitimacy after 9/11.* Oxford: Oxford University Press, 2012.

Homeland Security Committee. *Refugee Flows: Security Risks and Counterterrorism Challenges*. Washington D.C., 2015.

Kelly, Terrence K., et al., *A Stability Police Force for the United States: Justification and Options for Creating U.S. Capabilities*. Santa Monica: RAND Corporation, 2009.

Kilcullen, David. "Counter-Insurgency Redux." *Survival* 48, no. 4 (January 2006): 111–130. doi:10.1080/00396330601062790

Krebs, Valdis E. "Mapping Networks of Terrorist Cells." *Connections* 24, no. 3 (2002): 43–52.

La, Lynn. "Greenpeace Protesters Made Breaking into French Nuclear Power Plants Look Easy." *Business Insider Australia*, December 7, 2011.

Langeweische, William. "The Wrath of Khan." *Atlantic*. November 2005. http://www.theatlantic.com/magazine/archive/2005/11/the-wrath-of-khan/304333/.

Long, Austin. "Deterrence Then and Now." In *Deterrence from Cold War to Long War: Lessons from Six Decades of RAND Research*. Santa Monica: RAND Corporation, 2008.

Lothringer, Derek, Mathew McGraw, Mathew Rautio, and Leif Thaxton. "Countering Weapons of Mass Destruction: A Preliminary Field Study in Improving Collaboration." Master's thesis, Naval Postgraduate School, 2016.

Malone, Patrick, and R. J. Smith. "The Islamic State's Plot to Build a Radioactive 'Dirty Bomb.'" *Foreign Policy*. February 29, 2016. http://foreignpolicy.com.libproxy.nps.edu/2016/02/29/the-islamic-states-plot-to-build-a-radioactive-dirty-bomb/?utm_source=Sailthru&utm_medium=e-mail&utm_campaign=New%20Campaign&utm_term=%2AEditors%20Picks.

Manners, Ian, and Richard Whitman, conclusion to *The Foreign Policies of European Union Member States,* eds. Ian Manners and Richard Whitman. Manchester: Manchester University Press, 2000.

Maoz, Zeev, and Nasrin Abdolali. "Regime Types and International Conflict, 1816–1976." *Journal of Conflict Resolution* 33, no. 1 (1989): 3–35.

Marin, Alexandra, and Barry Wellman. "Social Network Analysis: An Introduction." University of Toronto (2009).

McChrystal, Stanley. *Team of Teams*. New York: Penguin, 2015.

McShane, Steven, and Mary Von Glinow. *Organizational Behavior*. McGraw-Hill Higher Education, 2012.

Mearsheimer, John J. “The False Promise of International Institutions.” *International Security* 19, no. 3 (1994): 5–49.

“Migrant Crisis: Hungary Closes Border with Croatia.” BBC, October 17, 2015.

Mintzberg, Henry. “Organization Design: Fashion or Fit?” *Harvard Business Review* (January–February 1981): 1–16.

Morgenthau, Hans J. *Politics among Nations: The Struggle for Power and Peace*. 5th ed. New York: Alfred A. Knopf Inc., 1973.

Mowatt-Larssen, Rolf. “Al-Qaeda’s Pursuit of Weapons of Mass Destruction.” *Foreign Policy*. January 25, 2010. http://foreignpolicy.com.libproxy.nps.edu/2010/01/25/al-qaedas-pursuit-of-weapons-of-mass-destruction/.

Muana, Patrick. “The Kamajoi Militia: Violence, Internal Displacement and the Counter-Insurgency.” *Africa Development* 22, no. 3–4 (1997): 77–100.

Naim, Moises. *The End of Power*. New York: Basic Books, 2013.

National Commission on Terrorist Attacks. *The 9/11 Commission Report*. New York: M.W. Norton & Company, 2004.

Neslen, Arthur. “Border Tensions Rumble over Ageing Belgian Nuclear Reactors.” *Guardian*, February 2, 2016.

Nikitin, Mary B., and Amy F. Woolf. *The Evolution of Cooperative Threat Reduction: Issues for Congress*. Congressional Research Service, 2014.

“Nuclear Smuggling Deals ‘Thwarted’ in Moldova.” BBC, October 7, 2015.

Oye, Kenneth A. “Explaining Cooperation under Anarchy: Hypotheses and Strategies.” In *Cooperation under Anarchy*, edited by Kenneth A. Oye. New Jersey: Princeton University Press, 1986.

Parlapiano, Alicia, Wilson Andrews, Haeyoun Park, and Larry Buchanan. “The Expanding Web of Connections among the Paris Attackers.” *New York Times*, March 18, 2015. http://www.nytimes.com/interactive/2015/11/15/world/europe/manhunt-for-paris-attackers.html?_r=2.

Rühle, Michael. “NATO Ten Years After: Learning the Lessons.” *NATO Review Magazine*. Accessed April 30, 2016. http://www.nato.int/docu/review/2011/11-september/10-years-sept-11/EN/index.htm.

Simon, Herbert A. “Human Nature in Politics: The Dialogue of Psychology with Political Science.” *American Political Science Review* 79, no. 2 (1985): 293–304.

———. “Rationality in Political Behavior.” Special issue, *Political Economy and Political Psychology* (1995): 45–61.

Snidal, Duncan. “Relative Gains and the Pattern of International Cooperation.” *American Political Science Review* 85, no. 3 (September 1, 1991): 701–726.

Snow, Jennifer. “Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies.” Master’s thesis, Naval Postgraduate School, 2015.

Spillius, Alex. “Nuclear Terrorism Is Gravest Threat to Global Security, Barack Obama Warns.” *Telegraph*, April 12, 2010. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7580210/Nuclear-terrorism-is-gravest-threat-to-global-security-Barack-Obama-warns.html.

Stein, Arthur A. “Coordination and Collaboration: Regimes in an Anarchic World.” In *International Regimes*, edited by Stephen D. Krasner. Ithaca: Cornell University Press, 1982.

Stolberg, Alan G. “The International System in the 21st Century,” in U.S. Army War College Guide to National Security Issues: Volume II – National Security Policy and Strategy, ed. J. Boone Bartholomees. Carlisle Barracks: Strategic Studies Institute, 2012.

“U.S. Counterproliferation Policy.” Wilson Center, January 27, 2005. https://www.wilsoncenter.org/event/us-counterproliferation-policy.

Vedantam, Shankar. “How Terrorist Organizations Work Like Clubs.” *Washington Post*, August 4, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/08/03/AR2008080301529.html.

Walsh, James I. “Intelligence-Sharing in the European Union: Institutions Are Not Enough.” *Journal of Common Market Studies* 44, no. 3 (September 2006): 625–643.

Waltz, Kenneth N. *Theory of International Politics*. New York: McGraw-Hill Inc., 1979.

Weber, Max. “The Three Types of Legitimate Rule.” In *The Theory of Social and Economic Organization*, translated by A. M. Henderson and Talcott Parsons. New York: The Free Press, 2009.

Wendt, Alexander. “Constructing International Politics.” *International Security* 20, no. 1 (1995): 71–81.

Williamson, Oliver E. “The New Institutional Economics: Taking Stock, Looking Ahead.” *Journal of Economic Literature* 38, no. 3 (2000): 595–613.

Wohler Associates. Wohlers Report 2015. 2015. http://www.wohlersassociates.com/2015report.htm.

Yapsan, Hikmet. “International Police Cooperation on Countering Transnational Terrorism.” Master’s thesis, Naval Postgraduate School (2012).

Zanini, Michele, and Sean Edwards. “The Networking of Terror in the Information Age.” In *Networks and Netwars,* edited by John Arquilla David Ronfeldt. Santa Monica: RAND, 2001.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California