6-30-2021

Project 10: Training and Education Research and Implementation Strategies for Homeland Security Intelligence Community

Michelle Black
University of Nebraska at Omaha, michellblack@unomaha.edu

Lana Obradovic
University of Nebraska at Omaha, lobradovic@unomaha.edu

Elizabeth Bender
University of Nebraska at Omaha, elizabethbender@unomaha.edu

Claire Benedix
University of Nebraska at Omaha, cebenedix@unomaha.edu

Josie Nelson
University of Nebraska at Omaha

Recommended Citation

Black, Michelle; Obradovic, Lana; Bender, Elizabeth; Benedix, Claire; Nelson, Josie; Van Robays, Grant; and Youngberg, Christiane, "Project 10: Training and Education Research and Implementation Strategies for Homeland Security Intelligence Community" (2021). *Reports, Projects, and Research*. 28.
https://digitalcommons.unomaha.edu/ncitereportsresearch/28

Authors

Michelle Black, Lana Obradovic, Elizabeth Bender, Claire Benedix, Josie Nelson, Grant Van Robays, and Christiane Youngberg

Project 10:
Training and Education Research and Implementation Strategies for Homeland Security Intelligence Community

A Research Project Funded by
the Department of Homeland Security
Theme - Workforce Development

Principal Investigator:
Dr. Michelle Black, Ph.D.
Assistant Professor, Department of Political Science
University of Nebraska at Omaha (UNO)

Co-Investigator:
Dr. Lana Obradovic, Ph.D.
Associate Professor, Department of Political Science
University of Nebraska at Omaha (UNO)

NCITE NATIONAL COUNTERTERRORISM,
INNOVATION, TECHNOLOGY,
AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Project 10:
Training and Education Research and Implementation Strategies for Homeland Security Intelligence Community

A Research Project Funded by A U.S. Department of Homeland Security Center of Excellence National Counterterrorism Innovation, Technology, and Education Center (NCITE)
Theme – Workforce Development

Principal Investigator:
Dr. Michelle Black, Ph.D.
Assistant Professor, Department of Political Science
University of Nebraska at Omaha
6001 Dodge St.
Omaha, NE 68182
michellblack@unomaha.edu

Co-Investigator:
Dr. Lana Obradovic, Ph.D.
Associate Professor, Department of Political Science
University of Nebraska at Omaha
6001 Dodge St.
Omaha, NE 68182
lobradovic@unomaha.edu

University of Nebraska at Omaha Student Contributors
Elizabeth Bender, BA Criminal Justice and Political Science [2022]
Claire Benedix, MS Political Science [2022]
Josie Nelson, BA International Studies and Political Science [2021]
Grant Van Robays, BS Political Science [2022]
Christiane Youngberg, MS Political Science [2020]

Table of Contents

Executive Summary

Intelligence is vital to national security. Since 2001, there has been a significant movement to protecting U.S. borders and citizens from experiencing the devastating effects of terrorism, among other national security threats. Since its inception in 2002, the Department of Homeland Security has founded the creation of a national security framework based on intelligence. However, there remains significant gaps in the standardization of intelligence training and education. This may be due in part due to the differing missions of DHS components under the overarching umbrella of national security. From experience, it is known that homeland security not only encompasses counterterrorism, but also border protection, emergency management, cyber security, and more. Due to the multifaceted and ever evolving nature of homeland security, there are 17 DHS components to approach the broader issue of national security.

Scholars debate on how intelligence education and training should be taught, and who should teach this curriculum. When intelligence training was in its initial stages, most of it was conducted in-house by government agencies. As the demand for homeland security efforts have increased following 9/11, universities have developed homeland security intelligence programs to accommodate the instruction gap. A major issue with two separate entities creating courses to fulfill the intelligence demand is the variation in education and training content. While some scholars believe that a greater professionalization of intelligence careers would help better establish core competencies, others argue that not all levels and types of analysis require the same types of competencies (Bruce and George, 2015, p. 4; Moore and Krizan, 2009). There not only exists a lack of education standardization in the intelligence community, but also in core competency definitions.

Due to the overall lack of IC standards in both IC in-house training and university education, some programs fail to include content that is relevant to a professional intelligence career, which creates employee pipeline issues for DHS intelligence needs. This slows the hiring process and exacerbates the issues that come with understaffing, which include low employee morale, high turnover, and demand for more versatile employees. A lack of DHS-wide core competencies only feeds this issue with variation of DHS component missions. In response to the uneven education that employees may receive either from a university or instruction in-house, some agencies have established their own schoolhouses with separate competencies and standard training.

Through ethnographic interviews with Intelligence Community members including many DHS participants, as well as in-depth research and domain analysis drawing on scholarly literature and published government reports, Project 10 researchers found a lack of benchmarks for core competencies associated with intelligence analysis as well as multiple gaps in the current implementation of intelligence training and education. There was very little research and literature pertaining to intelligence analysis standards that also mapped how competencies are measured, implemented, and organized. With little guidance or uniformity, the intelligence community entry-level workforce talent demonstrates how knowledge, skills, and abilities vary in similar positions when core competencies are not utilized or enforced. The absence of standardization and structure highlights the need for core competency framework across the entire intelligence community that not only establishes intelligence analysis core competencies but also recommends how these practices and standards could be integrated in a meaningful manner that would positively affect DHS' mission performance.

Based on this analysis, the research team recommends the intelligence analyst working within DHS and its components should have the *basic six Core Intelligence Analysis Competencies*: Analytical Writing, Communication, Critical Thinking and Reasoning Methods, Collaboration, Project Management, and Basic Technology. In addition to the Core Intelligence Analysis Core Competencies, it is desirable for the intelligence analyst to have *Intelligence Fundamentals Skills* – this includes familiarity with national intelligence structures and policy, intelligence cycle, and intelligence writing and analytic tools. Despite recommendations provided in both the 2010 Common Competencies for State, Local, and Tribal Intelligence Analysts document by SLT Working Group and the 2015 Analyst Professional Development Road Map, there is no still no baseline standard of competencies that define the role and function of all entry-level intelligence analysts within DHS and its components. To this day, it remains fragmented and siloed, with each component providing only in-house specialized training that is relevant to their unique mission. Echoing the calls to action by both the academic works the research team reviewed and intelligence enterprise practitioners the team interviewed, our analysis demonstrates that being able to standardize this set of competencies is critical to the DHS's ability to provide and integrate timely intelligence and information, and not merely just a question of hiring and promoting potential job candidates.

Furthermore, the team found that the development and inclusion of a standardized Core Intelligence Analyst Competency Matrix that is integrated into the DHS Performance and Learning Management System, and utilizes the Intelligence Community Centers for Academic Excellence can increase the employment pipeline and academic needs, and improve retention and merit-based advancements through educational opportunities.

Terms of Reference

Analysis – The application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context (Johnston, 2005).

Counterintelligence (CI) - Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities. (ODNI, 2011).

Declassification – The authorized change in the status of information from classified information to unclassified information (ODNI, 2011).

Dissemination - The timely distribution of intelligence products (oral, written, or graphic form) to departmental and agency intelligence Consumer's is a suitable format (ODNI, 2011).

Intelligence Community (IC) – A federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States (ODNI).

Intelligence Oversight - A mechanism to ensure that the IC conducts intelligence activities in a manner that that achieves the proper balance between the acquisition of essential information and protection of individual interests. The oversight is performed by entities inside and outside of the IC, which allows the IC to account for the lawfulness of its intelligence activities to the American people, to Congress, to the President and to itself as ordered by Executive Order 1233 (ODNI).

National Intelligence - Intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that (1) pertains to more than one U.S. government agency; and (2) that involves (i) threats to the U.S., its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on U.S. national or homeland security (DHS, 2017).

National Security – Comprehensive program of integrated policies and procedures for the Departments, agencies, and functions of the United States Government aimed at protecting the territory, population, infrastructure, institutions, values, and global interests of the Nation (DHS, 2017).

Chapter One

Introduction

Building and strengthening the Department of Homeland Security's (DHS) workforce in counterterrorism operations starts with effectively trained and educated intelligence workers. However, identifying and establishing standards for effective training and curriculum for intelligence analysts can be a challenge. This research project was selected and funded by DHS to address this challenge and provide recommendations to implement for future DHS intelligence training. To assist with this challenge, researchers collected primary and secondary data across the Intelligence Community (IC), including current training and educational requirements, operational lessons learned, career progression and promotion within the workforce, intelligence data collection procedures, analytical techniques, and technological advances and applications. This final report provides the findings of the research project, along with guidance that will enhance DHS's capacity to identify and implement strategies to improve intelligence training and education within their organization.

The chapters in this report will specifically examine and address the following questions that were previously outlined in the proposal:

- What are the challenges, current trends, and best practices in intelligence training and education?
- What are the core competencies identified by the Intelligence Community?
- What specific core competencies must an intelligence analyst possess to be effective across multiple components and organizations of DHS?
- How can these core competencies be integrated into education and training effectively?

Structured around these questions and designed to review, analyze, and make recommendations, this report draws on the relevant scholarly literature, government documents, interviews, and practices within the IC. Through analysis and assessments of this data, the report provides a benchmark and recommendations for core competencies for homeland security intelligence training and education. By outlining these recommendations, it charts a path to build a more innovative and efficient intelligence workforce able to conduct analysis and develop intelligence products that contribute to the missions of DHS.

The scope of this report is limited to 1) establishing core competencies associated with intelligence analysis and 2) outlining feasible recommendations that will allow DHS to plan, provide, and evaluate training and education of its intelligence analysts in the years to come. In fact, this report is anticipated to be the first of many to address intelligence training and education for DHS. Overall, this first report presents findings on the larger training and education issues but focuses on addressing and implementing strategies for the core competencies. Follow-on research has been planned and will be expected to address some of the additional issues presented in this first report.

Chapter Two provides a baseline of intelligence training and education across the intelligence community. The creation of this baseline is important as it helps identify the benchmarks within different organizations and allows for a better identification of the challenges and issues associated with the training and education of intelligence analysts. First, this chapter situates the issue within the existing scholarly research on the core competencies for intelligence analysis education and training in general, and then within the larger IC and DHS Intelligence Enterprise context associated with workforce training and development. By reviewing the existing core competencies identified in guidance documents of different IC agencies, this section highlights the importance of knowledge that intelligence analysts need to perform their jobs.

Next, Chapter Three introduces and explains the relevance of our chosen methodological approach. It provides a detailed description of our data-collection process, tools and instruments used, as well as ethical and privacy considerations and precautions taken while conducting research. This chapter also contains a discussion of comparative analysis, ethnographic research, and domain analysis by using Atlas.ti content analysis software. Finally, it addresses the limitations that our research team encountered during our data-gathering phase.

Chapter Four presents and discusses the findings from our data collection and interviews, by outlining the overall training and education issues found throughout the analytical process. This discussion is vital to this and subsequent reports, as many of the issues, if not all, are interrelated. This chapter takes an overarching view of all the challenges related to intelligence training and education, but has a specific focus on the core competencies, as it was chosen for the theme for year one of Project 10. From Chapter Four, the report transitions into recommendations for core competencies.

Chapter Five provides clear and feasible recommendations that would improve DHS intelligence analyst training and education. More specifically, it identifies specific core competencies that were identified through the analysis process and proposes changes to the existing training content, and possible augmentation of existing courses and programs. This section of the report also provides agency resources within the intelligence community to integrate into DHS and accomplish requirements through already established programs and funding. Implementation of these recommendations would assist in solving challenges outlined in Chapter Two and Four. It is important to note that these are just suggestions, and some of the recommendations are flexible enough to implement due to the size and mission of DHS. There are no recommendations that all ‘must’ be implemented to be effective. The recommendations provided were designed to be flexible enough that the agencies could choose one over another if it fits their requirements. Furthermore, the recommendations provided lists outcomes, and measurements to help with tracking and reporting functions so that training departments can document their progress.

Finally, Chapter Six draws final conclusions and outlines follow-on research for Year 2 of Project 10. The initial findings from the first year identified new areas of concern for the intelligence workforce development, training and education, particularly as they relate to the impact of technology, strategic planning and programs, and management of information protection. In this chapter, the research team presents the plan for continuation of these efforts during year two but with a concrete focus on research, development, implementation, and assessment of technological training and education standards for the intelligence community members.

Chapter Two

Current Trends in Intelligence Analysis Training and Education

Introduction

When the National Security Act of 1947 established a post-World War II national security framework, the intelligence analysis component relied on those who have served in military intelligence units and those within the State Department who knew how to write analytic briefs. Not much attention was paid to developing intelligence analysis as a *profession* or creating educational programs, as those who were joining the IC already had the experience and drew on their undergraduate education in liberal arts and social sciences (Lowenthal, 2014). However, the highly critical Dulles-Jackson-Correa Report in 1948, which found a lack of intelligence activity coordination and failure to organize correlation and evaluation functions, among others, forced the Community restructuring and set the tone for education and training programs for years to come. Over the next couple of decades, most elements organized their own in-house and agency-specific programs, such as the Central Intelligence Agency's Sherman Kent School, the National Security Agency's National Cryptologic School, and the Defense Intelligence College. Although authors such as Peter Dorondo suggested the addition of a single course on intelligence to a university degree program like International Relations (1960), and Washington Platt advised students interested in intelligence careers to consider studying social sciences, such as political science, psychology, economics, and history (1957) - for much of the Cold War there were no major calls for the creation of a standalone intelligence program (Coulthart and Crosston, 2015). It was not until 1992 that Mercyhurst University established the first intelligence degree program of its kind with the goal to produce "analytic generalists" as opposed to traditional "specialists" with expertise in area studies, languages, and social sciences. However, the end of the Cold War, and the congressionally mandated reduction in personnel levels, led to an overall decline in interest and investment in intelligence education and training on the part of both the IC and academia.

However, since the September 11 attacks on the United States, and the consequent organizational, oversight and information-sharing reforms, the IC has been seeking to improve its analytic capacity and ensure that its workforce is adequately trained, educated, and equipped to accurately "connect the dots" (Burch, 2008). The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) sought to improve education, training and professional development of IC intelligence analysts, by setting standards, diversifying, encouraging university grants and scholarship that would allow for more cross-disciplinary preparation, language expertise, and improve analytic methods and training. This new security environment demanded changes, and the IRTPA led to an active movement to professionalize, streamline, and standardize the way intelligence agencies and academic institutions train and educate the next generation of intelligence analysts, capable of identifying and managing asymmetric and non-conventional attacks against the homeland and its interests.

But what does this project mean by intelligence analysis education and training, and where should they be obtained? To answer these questions, this chapter first maps the current debates and collaborative efforts between academia and the IC to provide intelligence training and education. It does so by providing an overview of their unique roles when it comes to the preparation of the workforce and highlights both successes and pitfalls of some of the main existing university-government partnerships. Next, it addresses the contemporary arguments regarding different types of knowledge, skills, and abilities intelligence analysts require to perform their jobs. Finally, the chapter identifies and compares the existing references to the core competencies in documents across the IC to assess whether different elements share a common understanding of intelligence analysts' education and training.

Intelligence Analysis Education and Training: Academic Programs

While "education" was traditionally conceptualized as foundational knowledge and theoretical grounding attained by attending courses and programs at universities, more specialized and job-related "training" was conducted in-house by government agencies and military services. The former was meant to provide a broader picture of the international relations security environment within which intelligence analysis and decision-making take place, while the latter was oriented toward gaining a better understanding of the analytical writing styles, covert operations methods, and counterintelligence (Johnson, 2019). According to Stephen Marrin, a former CIA analyst and leading scholar of intelligence studies, institutions providing *education* were viewed by the Intelligence Community analytical personnel:

> (1) as a place to recruit graduates with substantive knowledge and expertise of use to the Community; (2) as a place to send analysts for acquisition of more or different knowledge (i.e., continuing education); (3) as a place to acquire specific knowledge or expertise from academic experts; and (4) as a place to acquire information or advice in terms of managing the Intelligence Community from those who specialized in intelligence studies (frequently from either a political science or history perspective)." (2009)

However, in the post-September 11 era, Marrin argues, the lines between who gets to provide education and training are increasingly blurred and disappearing as the universities are expected to impart both practical generalist analytical training and intelligence studies theory – often at the expense of the more specialized, technical, area or language knowledge. In essence, as the government agencies began to reform, rethink and adapt their own training programs, we have witnessed a dramatic rise in demand and development of academic courses, degrees and certification programs in intelligence studies across the United States to meet that need (Campbell, 2011). What remains, however, is the debate regarding the value and contribution of such convergence to the development of individual intelligence analysts and intelligence as a profession (Landon-Murray, 2013). Some of the most prominent intelligence scholars, such as Arthur Hulnick, Mark Lowenthal and Carmen Medina, have argued that such intelligence education should remain part of the larger social sciences and liberal arts theoretical framework (Spracher, 2009). Yet, there are plenty of arguments in favor of smaller intelligence programs where courses are taught by former intelligence practitioners and aim to provide more hands-on, practical, and real-world training (Dujmovic, 2017). Those who support inclusion of training in student preparation focus on procedural knowledge, analytical competencies, and use of specific methods such as structural analytical techniques (Landon-Murray, 2013). The critics suggest that such a vocational approach to intelligence has been adopted at the expense of a more social science-oriented, theoretical and methodological preparation and subject matter education (Collier, 2005; Landon-Murray, 2011; Corvaja et al., 2016). Others add that we should be concerned with the overall sustainability and stability of such practice-focused intelligence programs, given that most faculty are non-tenure track or adjuncts/part-time instructors who are ranked low within academic hierarchy have little input when it comes to the governance of such programs and resources allocated to teaching intelligence within higher education institutions (Smith, 2013).

It is important to note that although the case was made in 1960, one can find intelligence analysis courses taught by practitioners in the 1970s, particularly following events such as the Watergate scandal and the Iran crisis (Rudner, 2009). The 1985 CIA's Officer-in-Residence program eventually became the "model for nurturing relations between intelligence and academia" (Hedley, 2005) and recruiting students straight from their classrooms. Although this program still exists, in 2016, the CIA expanded its presence on America's campuses by launching its newest initiative, the CIA Signature School Program. This allows intelligence professionals to interact regularly with students, advise them on career paths, provide simulations and exercises that focus on critical thinking and analytical skills, teach briefing techniques, and collaborate with the university faculty on course development and curriculum (Ortiz, 2016). While the effort was primarily aimed at ensuring and strengthening greater diversity and inclusion at the Agency, once again, the CIA is directly involved in shaping the education of the next generation of intelligence analysts before their employment. But the CIA is no longer the only IC element seeking to solve intelligence education and training challenges by directly engaging and teaching students, nor is it plowing the way for the rest of the Community.

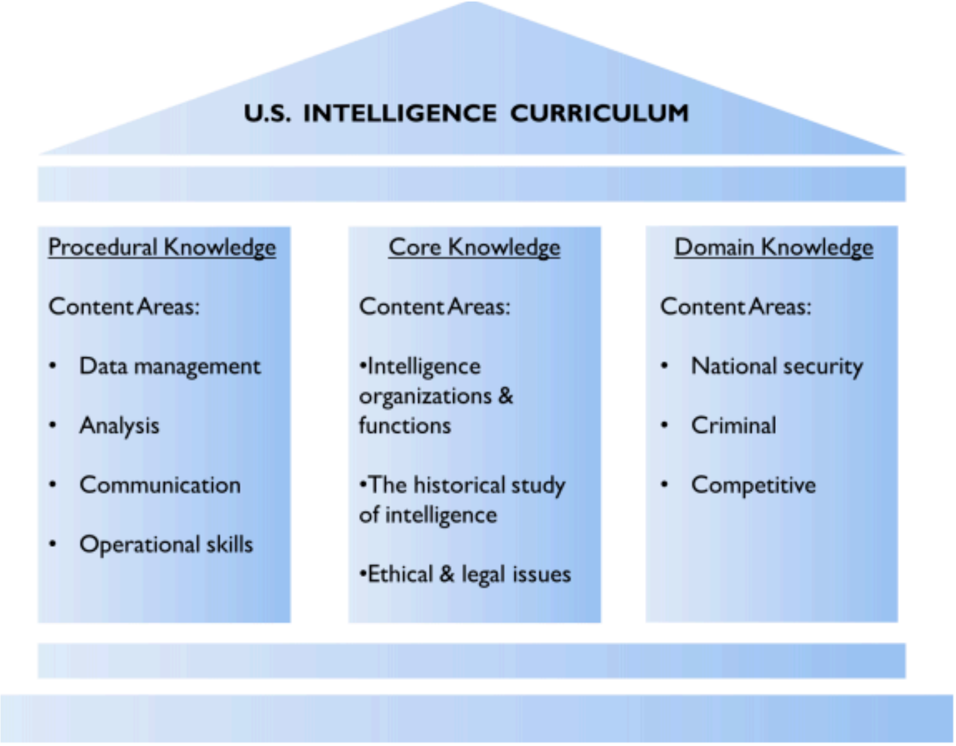
When the Homeland Security Act of 2002 gave the green light to the Department of Homeland Security to launch its own Centers of Excellence, the Department simultaneously started working with the university faculty to assist them in finding science and technology solutions and develop the much-needed workforce by preparing students to understand and manage threats to the homeland. The university faculty that was traditionally engaged in writing and publishing almost exclusively in academic journals, started to more actively support both education and training programs across the United States and provide applied research and expertise to the relevant DHS components. Today, there are 10 such Centers around the country, each providing direct access to the expertise of U.S. colleges and universities to solve increasingly complex homeland security threats and needs, and engage students in meaningful learning experiences, such as summer internship programs, research projects, professional symposia, workshops, and coursework.

Similarly, in 2005, the Intelligence Community Centers for Academic Excellence (IC CAE) Program was established with the goal of developing "a diverse, professionally competitive and knowledgeable workforce ...that will carry out the national security priorities and obligations" (ICCAE Strategy, 2020-2023). Primarily directed under the auspices of the Office of the Director of National Intelligence (ODNI) and the Defense Intelligence Agency (DIA), the program provided five rounds of grant awards starting in 2006. Universities were given seed funds to develop sustainable national security and intelligence education programs, with a specific focus on providing critical core competencies, such as intelligence analysis, writing and briefing, cultural and language expertise, and STEM skills. In turn, the IC received an easily accessible, diverse, capable and competitive talent pool to continue to support its mission. As a result of this investment and infusion of government resources "to meet the longer-term human resource needs of the intelligence services" (Rudner, 2009), the long-neglected, underfunded, and underdeveloped intelligence studies courses and programs finally proliferated. A recent study showed that by 2019, 49 intelligence degrees, certificates and minors were created at different IC CAE institutions - out of which 33 were at the undergraduate level - as well as more than 75 new courses, to complement the already existing relevant curriculum (Landon-Murray and Coulthart, 2020). The same study demonstrates that most of this new coursework emphasized intelligence organizational structures, processes, and domestic and global security threats, as well as provided more practical real-world simulations, exercises and skills such as analytics techniques, writing, and briefing.

By analyzing 17 different university programs, Coulthart and Crosston mapped out this new American intelligence education and summarized it in the following figure (*Figure 1*).

Figure 1

The Curricular Structure of U.S. Intelligence Education Program



Note. Adapted from Terra incognita: Mapping American intelligence education curriculum, by Coulthart and Crosston, 2015.

The authors demonstrate that academic programs have dramatically expanded their course offering to provide substantive core and domain education, as well as training in job-specific skillsets (2015). Within 15 years, new intelligence curricula have been developed and integrated into a variety of academic programs from political science and international relations to emergency management and homeland security, particularly at the large public institutions in minority-serving, as well as historically rural and under-resourced population colleges. It seemed as if the shortage of skilled intelligence analysts was going to be solved quickly, but as programs proliferated across the country, so did issues regarding oversight, assessment, documentation, performance measures, and participation of IC elements. The GAO 19-529 report found that the DIA has failed to develop results-oriented program goals or establish a clear and consistent strategy that would allow it to comprehensively collect data, evaluate the overall success of the program, and track, assess, and address the participation by the IC (2019). There were no clear milestones, not enough documentation, and performance measures went undefined. But most importantly, while universities across the country successfully transformed their offerings to meet the needs of the IC, many elements of the IC simply failed to engage and recruit via IC CAEs. In 2020 the program transitioned back to ODNI, and it is premature to conclude what changes, if any, have been made and implemented to ensure a return on investment. Most IC CAE institutions require their program participants to acquire many of these competencies as part of their degree or certificate program. Therefore, the expectation is that regardless of one's area of specialization, IC CAE graduates will have a solid foundation and preparation to analyze complex problems, develop creative solutions in collaboration with others and present them both orally and in writing. Proficiency is not achieved upon graduation. Through our conversations with both current and legacy IC CAE directors, it became clear that while they have sought to continually adapt to deliver the required program components and support the overall goals of the program, recruiters from many agencies, including DHS never reached out to increase their pool of eligible and knowledgeable applicants.

It is important to note that most of these academic programs are not concerned with providing curriculum for the law enforcement intelligence analysis but rather provide broader international and national security coursework meant for those interested in working for the federal agencies and private sector companies (Green, 2008). To fill the gap, we have witnessed equally fast growth of interdisciplinary "Homeland Security" programs that, according to Bellavita's study, were still struggling to figure out what that curriculum should include (2008). About 85% or more study participants' colleges agreed that such programs should include terrorism, critical thinking, collaboration, intelligence, strategy, all-hazards, critical infrastructure, emergency management, preparedness, risk management, and cyber security. On the other hand, 51% or more agreed on five additional topics: public administration/policy, resilience, national security/international affairs, immigration, and public health. Another study collected data from 2004 to 2013, from homeland security programs, and found that the most important competencies, listed from most to least important, were: strategic collaboration, critical thinking and decision-making, foundations of Homeland Security, analytical capabilities, leadership, legal issues, strategic planning, and cognate or specific knowledge (Pelfrey, 2013). Clearly, including a wide-ranging array of topics is difficult and demonstrates the need to establish a comprehensive and standardized framework of core competencies. In addition, there is a disagreement in terms of the appropriate level of education for these topics. While some find that undergraduate programs in Homeland Security were not only on the rise but also validated in process and efficacy via focus groups or advisory councils (Comiskey, 2015), others provide little support due to "the objectives and capabilities described to be most appropriate for graduate education" (Pelfrey, 2013, p. 3).

Finally, we are still lacking cumulative scholarly literature on intelligence education, and just as Sherman Kent argued, the field of intelligence itself, "its method, its vocabulary, its body of doctrine, and even its fundamental theory run the risk of never reaching maturing" (1955, p. 3). There is no doubt that developing core competencies and integrating intelligence analysis training into academic disciplines within higher education institutions is slowly becoming the new norm but there is a dearth of studies examining best practices, educational requirements, appropriate combination of foundational, theoretical and conceptual education and practical training for entry level candidates.

While the debate continues, it is important to note that there is a shared understanding that future intelligence analysts need to receive both – education and training. But there is no shared understanding of the degree to which graduates should be provided by universities with specialized topics knowledge, such as terrorism or language subject matter expertise on the one hand and more generalist intelligence analysis techniques on the other (Corvaja, 2016). The next section seeks to provide an overview of different in-house training programs provided by the IC elements to their newly hired intelligence analysts to address the questions regarding the complementarity and compatibility between what the academic programs and the IC are providing in terms of intelligence analysis training and education.

Intelligence Analysis Education and Training: Intelligence Community

Over the past two decades, various IC elements have established their own intelligence analysis education and training centers, including the CIA's Sherman Kent School for Intelligence Analysis, the Federal Bureau of Investigation's (FBI) College of Analytical Studies, the DIA's Joint Military Intelligence Training Center, as well as the National Intelligence University (NIU), which in June 2021 transitioned from the DIA to the Office of the Director of National Intelligence (ODNI). All of these in-house specialized training programs have evolved since September 11, 2001, as the threats and the corresponding core intelligence tradecraft education and training requirements have changed. Although training is conducted in a classified setting by the highly experienced and certified faculty, the scope, length, and topics vary. The NIU program, on the other hand, remains the only fully accredited federal undergraduate and graduate degree-granting institution with an academic curriculum offered to both government civilians and military with a mission "to enhance the desired analytical skills and competencies of intelligence analysis to include critical thinking, communications, engagement, and leadership." (https://ni-u.edu/wp/about-niu/).

The Department of Homeland Security (DHS) has also dramatically grown its own in-house intelligence analyst training programs. Since graduating its first class of 17 students from the eight-week Basic Intelligence Threat Analysis Course (BITAC) in 2007, the DHS Intelligence Training Academy has also become fully accredited by the Federal Law Enforcement Training Accreditation (FLETA) Board. This accreditation is necessary to ensure that the training delivered corresponds to intelligence analyst training and professional development requirements. Other courses are offered, including Critical Thinking and Analytic Methods (CTAM), Introduction to Risk Analysis Course, Intermediate Risk Analysis Course, and Principles of Intelligence Writing and Briefing. In addition, some regional Fusion Centers have also organized their own training programs, including Intermediate Fusion Center Analyst Training, while others only offer mentoring programs due to their small staffing numbers and limited resources.

Moreover, the Association of Law Enforcement Intelligence Units (LEIU) and International Association of Law Enforcement Intelligence Analysts have their own Foundations in Intelligence Analysis Training (FIAT) that is aimed primarily at law enforcement intelligence analysts. Provided at cost to the members of the two associations, this program was established in a consortium with the National White Collar Crime Center (NW3C) and the Regional Information Sharing Systems (RISS) Project Directors. This five-day training is meant to introduce the basics of law enforcement intelligence analysis. IALEIA also proposes a comprehensive list of requirements for basic analytical training, including Analytic Writing, Critical Thinking, Ethics and Logic among others. But in order to ensure that intelligence analysts have the necessary core competencies, particularly those that pertain to writing and research, both the National Criminal Intelligence Sharing Plan (NCISP) and the IALEIA recommend that all those hired should have a four-year degree or commensurate experience as such candidates will already have them. This would reduce training costs and bring skills that can be used immediately. However, fusion centers and law enforcement have hired analysts with only two-year degrees, and as New York State Intelligence Center Fusion Center Training Strategy Development points out, these are "hard to match in an on-the-job training situation" (2009, pg. 8). In fact, some only receive the five-day FIAT training and are put to work along with candidates with more advanced graduate degrees, often making collaboration, communication, and even project management difficult as they do not share the same skills or lexicon. Unfortunately, while a great majority of scholarly research has focused on the standardization, performance indicators, and improvement of training and education of intelligence analysts on the federal level, much of it ignores state, local, and tribal law enforcement intelligence analysis (Dorn, 2019). That does not mean that there are no conversations within the law enforcement intelligence community on the need for greater standardization, but just like the rest of IC intelligence analysis training, for the most part, training remains scattered and relatively basic. Therefore, it is no wonder that scholars such as Lowenthal argue that despite efforts and years of investments, intelligence education and training remain "uneven, episodic and stovepiped" (Lowenthal, 2014, p. 303).

The next section explores scholarship that discusses what competencies IC agencies should require for their intelligence analysts, and what levels of those competencies are necessary for the different kinds of analysis they must perform. Moreover, it reviews the existing IC documents to establish if scholarly arguments have been implemented. This in turn would allow us to identify the consequential gaps in the existing education and training efforts within the IC that undermine the overall homeland security mission.

Defining Core Competencies: Academia and the IC

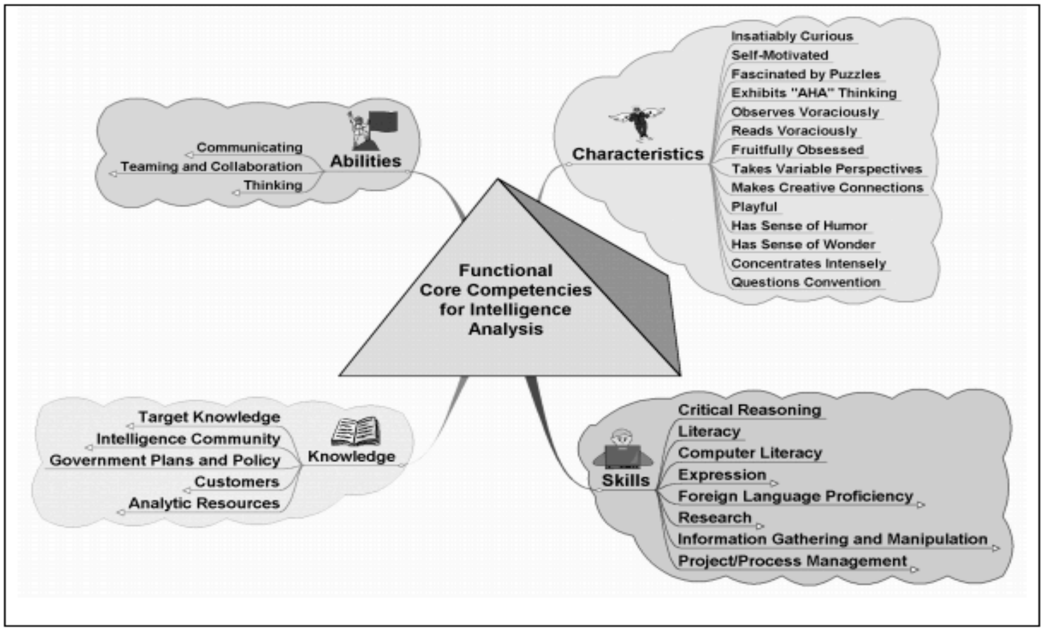
The IC recruits, hires, trains, and educates intelligence analysts charged with producing, gathering, evaluating, and examining information that supports policymaking, planning, and operations. Unlike most professions, where one's path is determined by academic degrees, licenses, and certifications, most intelligence analysts come from a wide variety of educational backgrounds. Some have extensive military and government experience; some have none. Others have extensive knowledge of history, politics, and languages of particular regions, while others cannot read a map but have advanced cryptologic skills. It is what Lowenthal called the "accidental profession", where this heterogeneity and diversity of people is its main analytical strength (2014). Lowenthal recognizes, however, that heterogeneity is also the main argument against prescribed academic undergraduate degrees and intelligence coursework at the universities, and it can pose a challenge to the way common understanding regarding practices, behaviors, and professional ethos are developed. Therefore, it is necessary to develop intelligence analyst core competencies – knowledge, skills, abilities, and attributes – that can be used as "cognitive requirements for effective performance, [to] provide standards that professionals from all member agencies should meet in order to be hired and promoted" (Spracher, 2009). This also requires a more comprehensive strategy and greater collaboration among IC elements first, and between the IC and academic community second.

Up until recently, very little literature was devoted to the intelligence analyst and the core competencies required by that analyst in order to be successful. One of the most coherent and systematic attempts to define functional core competencies for intelligence analysis was by Moore and Krizan, who break them down into four distinct categories: the characteristics of successful analysts, the sets of abilities, skills, and knowledge.

Figure 2 summarizes the core competencies that, according to Moore, "the analyst needs to be and to know" (Moore, 2005, p. 11).

Figure 2

Moore and Krizan's Functional Core Competencies for Intelligence Analysis

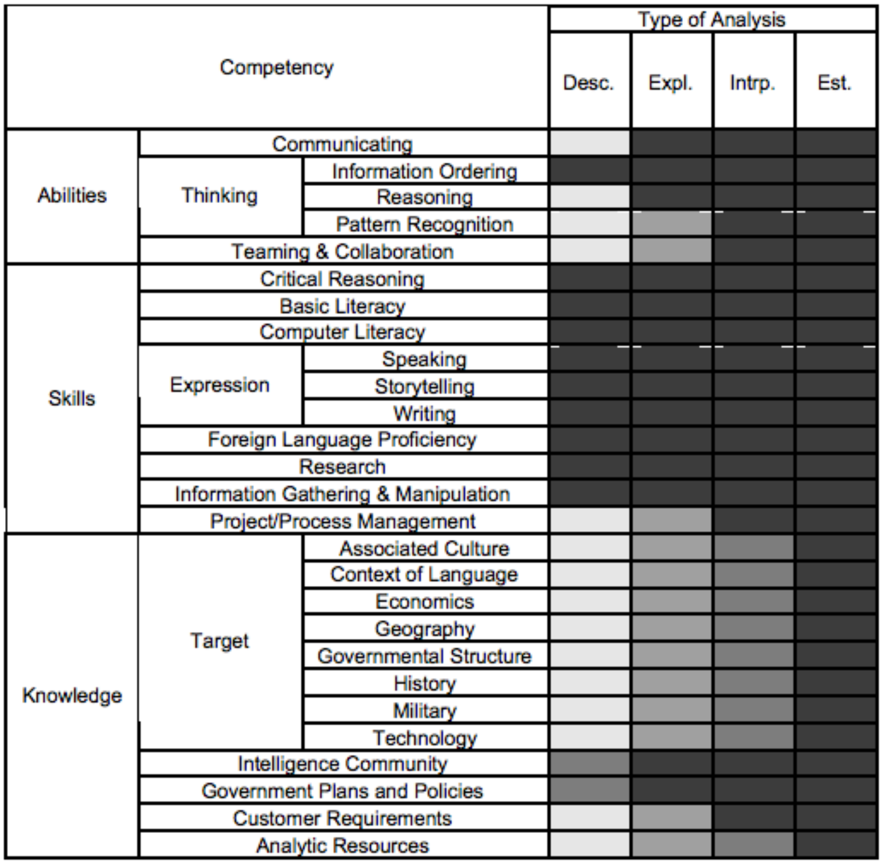


Note. Adapted from Evaluating intelligence: A competency-based model, by Moore and Krizan, 2005.

However, Moore and Krizan argue that it is not necessary to have the mastery of all competencies to be able to conduct each of the four types of intelligence analysis: descriptive, explanatory, interpretive, and estimative. Instead, they suggest that each type can be matched against the set of core functional competencies presented in *Figure 2*. While some core competencies are required for all four types, others are more specific and appropriate for different levels of analysis. They posit "that these lesser degrees of competency are starting points for analysts and that greater expertise will be sought as a matter of course through education, training, and experience" (Moore, 2005). In essence, many of the more complex competencies can be gained over the span of one's career through various professional development, continuing education, and training programs. *Table 1* provides an overview of the types of competencies associated with each level. The authors do acknowledge that "mastery" of a competency is entirely subjective, and that as the IC seeks to develop common core standards, the internal conversation needs to take place to establish different levels of mastery.

Table 1

Degree of Core Competencies Required for Different Levels of Analysis



Competency			Type of Analysis			
			Desc.	Expl.	Intrp.	Est.
Abilities	Communicating		░	█	█	█
	Thinking	Information Ordering	█	█	█	█
		Reasoning	░	█	█	█
		Pattern Recognition	░	▒	█	█
	Teaming & Collaboration		░	▒	█	█
Skills	Critical Reasoning		█	█	█	█
	Basic Literacy		█	█	█	█
	Computer Literacy		█	█	█	█
	Expression	Speaking	█	█	█	█
		Storytelling	█	█	█	█
		Writing	█	█	█	█
	Foreign Language Proficiency		█	█	█	█
	Research		█	█	█	█
	Information Gathering & Manipulation		█	█	█	█
	Project/Process Management		░	▒	█	█
Knowledge	Target	Associated Culture	░	▒	▓	█
		Context of Language	░	▒	▓	█
		Economics	░	▒	▓	█
		Geography	░	▒	▓	█
		Governmental Structure	░	▒	▓	█
		History	░	▒	▓	█
		Military	░	▒	▓	█
		Technology	░	▒	▓	█
	Intelligence Community		▓	█	█	█
	Government Plans and Policies		▓	█	█	█
	Customer Requirements		░	▒	█	█
	Analytic Resources		░	▒	▓	█

Note. Lighter hues of colors represent lesser degrees of acceptable competency. Data from Evaluating intelligence: A competency-based model, by Moore and Krizan, 2005.

Similarly, in his study, Spracher offers a detailed analysis of a survey on types of competencies young intelligence professionals have and need throughout the IC and concludes that core competencies ought to include engagement and collaboration, critical thinking, personal leadership and integrity, accountability for results, technical expertise, and communication. Among those listed, he finds that engagement and collaboration and technical expertise do not receive enough attention; the former tends to be gained via experience and practice, while the latter is often acquired through in-house specialized training. Furthermore, Spracher agrees with Moore that not all levels and types of analysis require the same types of competencies (2009).

Others, such as James Bruce and Roger George, also advocate a greater professionalization of the intelligence analysis and suggest that core competencies should:

“entail more than subject matter expertise, but rather involves good understanding of the operation and practice of intelligence itself, including the collection requirements and exploitation process, the epistemology and tradecraft required for accurate and reliable analysis, and the national security decision making process which intelligence analysis can ably support—or entirely miss the mark." (2015, p. 4).

Ultimately, the majority of scholars agree that there is a need for a greater standardization of core competencies to transform and improve intelligence analysis and gain access to and retain a wider and stronger pool of talent. Enhancing both education and training, whether at academic institutions, in-house through specialized training, or through a combination of both, is deemed a must if this project is to help prepare the next generation of intelligence professionals. Intelligence is a profession, and intelligence studies have become their own academic field, but both practitioners and scholars need to be part of the conversation in order to challenge each other's assumptions and develop more sustainable workforce pipelines.

In fact, there are several indications that standardization within the IC is desired by many of its elements. For instance, the Custom and Border Patrols' *Vision and Strategy 2020: U.S. Customs and Border Protection Strategic Plan* identifies as one of its objectives the need "to lead efforts to standardize processing requirements across all Federal agencies to support a whole-of-government approach" and acknowledges that "integrating intelligence, surveillance, and reconnaissance capabilities into the planning and execution of law enforcement operations is enabled by sound standards, procedures, and processes" (2015, p. 13). The Department of Homeland Security's *Office of Intelligence and Analysis Strategic Plan for FY 2020-2024* includes a goal to "create and implement synchronized approaches to improve the skills and integration of Homeland Intelligence professionals," by "optimiz[ing] DHS Intelligence training to minimize redundancy, and ensure employees obtain common foundational intelligence training at every level in their career, creating an agile intelligence workforce that meets the future needs of our employees and the IE's customers"(2020, p. 18).

But this is nothing new. In 2010, a working group, the Office of the Director of National Intelligence (ODNI), established the State, Local and Tribal (STL) Training Working Group that was chaired by the DHS Office of Intelligence and Analysis (I&A). They published the Common Competencies for State, Local, and Tribal Intelligence Analysts document that identified several common analytic competencies that should be exhibited by state, local, and tribal intelligence analysts working in state or major urban area fusion centers or similar analytic law enforcement entities. Building on the standards identified in the NCISP, the Minimum Criminal Intelligence Training Standards, and the Law Enforcement Analytic Standards, it proposed a nationally recognized set of competencies – critical thinking, fusing intelligence and law enforcement tradecraft, communication, collaboration, and concepts and principles (incorporating subject matter expertise) - and argued that these are essential to the use of both intelligence and law enforcement intelligence capabilities. Besides offering the baseline of analytical competencies for state and local fusion center analysts, this document mapped out corresponding behavioral indicators for each competency and suggested that intelligence analysts should also be familiar with a list of policies, principles, guidance, and concepts that appear in 18 different documents.

A few years later, the Office of the Director of National Intelligence established competency directories for the IC which aided in defining "component-specific competencies", but the DoD Office of Inspector General report suggests, "they did not provide common standards for developmental skill sets and basic knowledge of an IC professional" (2014, p. 2). As a result, the report finds that current standards vary from agency to agency, and the existing common tasks are not performed in an integrated fashion. In addition, it revealed that the training structures functioned in a fragmented manner without many joint structures, and therefore, with varied proficiency requirements, and leaving “critical skill gaps” (2014, p. 4).

Shortly thereafter, a 2015 Analyst Professional Development Road Map report by the Global Advisory Committee (GAC) aimed to focus on both the development and enhancement of analytic-related competencies and provide a career roadmap for intelligence analysts operating within state, local, tribal, and territorial organizations. It identified six separate common competencies for basic-level intelligence analysts. They are:

1. Legal issues surrounding the analytic process.
2. Thinking critically in the analytic cycle.
3. Sharing information and collaborating.
4. Fusing analytic tradecraft in a law enforcement environment.
5. Communicating analytic observations and judgments and generating analytic products to decision makers.
6. Turning concepts and principles into action.

These common competencies seem to build on those listed in the 2010 STL Working Group document. The Road Map not only focuses on different types of competencies, but it also breaks down different proficiency level – basic, intermediate, and advanced – and recommends training for each of those levels. The implementation of the detailed recommendations offered in these two documents would have certainly assisted in the professionalization of intelligence analysis, but even a cursory look at information our research team collected in the Appendix B reveals the wide array of competency designations and definitions that remain across the IC.

In sum, our preliminary review confirms what the 2019 Department of Homeland Security Office of Intelligence and Analysis Strategic Plan found - the IC elements currently do not synchronize education and training to improve intelligence professionals’ understanding of contemporary threats. Development of the intelligence workforce based on the levels of core competencies remains compartmentalized and departmentalized across the IC. Given the present state of intelligence education and training in the United States, and different ways in which core competencies are conceptualized by academia and IC elements, this chapter demonstrates that there is a continued need for a greater standardization of the process. It also identified the core competencies that various studies suggest the IC elements should focus on when recruiting and developing their intelligence analysis workforce through both in-house training and an external educational program. If intelligence analysis is to be professionalized as most experts suggest, the analysis suggests that most agencies are currently seeking candidates that at minimum have both written and oral communication, critical thinking, collaboration, and leadership skills. However, they do not always agree on their definitions, nor do they always provide clarification or guidance regarding different levels of proficiency.

Chapter Three

Research Design: Methodology and Data

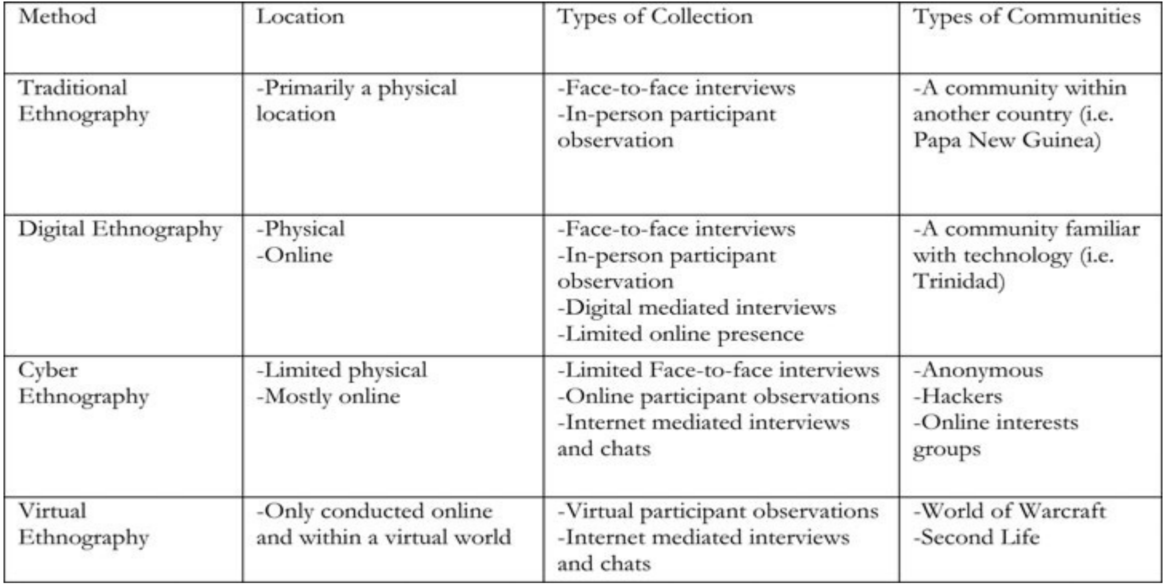
This study performed multi-method research that combined a comparative case study with ethnographic interviews and domain analysis. The research team first conducted an extended literature review to inform the research direction and data, setting the stage for the analytical framework. Data collected during this preliminary stage came from secondary sources, government reports, and documents provided by our stakeholders. These documents allowed the team to develop an understanding of the current trends in intelligence training and education across the entire intelligence community, allowing the team to compare current intelligence offerings at DHS. This part of the research project consisted of several phases, and it began by collecting data on existing intelligence training and education methods and practices across the Intelligence Community, as well as gathering information containing any projections regarding future intelligence analysis needs, threats, and challenges. This initial comparative analysis allowed the establishing of standard patterns and trends in intelligence training practices and competencies to reference throughout the ethnographic interview process. The team uncovered past reports, congressional reports, and syllabi that helped create a baseline of understanding on where training has been over the past 10 years, and some initial gaps in that process. The team also collected and used primary data during the second phase of the multi-method research, in order to investigate beyond the surface of the reports, triangulate the data, and validate some of the initial findings.

The second phase introduced ethnographic interviews, which allowed the team to gain insight into the environments of those engaged in the intelligence functions of the Department, and establish a greater understanding of their experiences, behaviors, meanings and interpretations of tradecraft, processes, training, tools, and policies. Ethnographic interviews were selected due to the nature of the questions and audience. Structured interviews would have proved limited in this research; therefore, open-ended questions and the freedom that ethnographic interviews allow research offered more flexibility. Additionally, these interviews create an informal and a more comfortable environment for the participants to discuss and engage on potentially sensitive topics, such as the quality of organizational, educational, and analytic standards, training proficiency, professional behaviors, and the expectations of employees within and personal feelings toward their organization.

Furthermore, the team utilized 'cyber ethnography' a form of interviewing that is different than traditional ethnography, due to most interviews being conducted online or through video conference calls (Black, 2016). As Black highlights, the Department of Defense should seek to incorporate online or cyber ethnography into their 'toolbox' as a method to reach inaccessible populations (2016). Traditional ethnographic methods require researchers to physically go to one location for an extended period of time, while cyber limits the physical movement and allows for collection through online or digital communication. *Table 2* identifies the different ethnographic methods that could aid in data collection online.

Table 2

Ethnographic Methods



Method	Location	Types of Collection	Types of Communities
Traditional Ethnography	-Primarily a physical location	-Face-to-face interviews -In-person participant observation	-A community within another country (i.e. Papa New Guinea)
Digital Ethnography	-Physical -Online	-Face-to-face interviews -In-person participant observation -Digital mediated interviews -Limited online presence	-A community familiar with technology (i.e. Trinidad)
Cyber Ethnography	-Limited physical -Mostly online	-Limited Face-to-face interviews -Online participant observations -Internet mediated interviews and chats	-Anonymous -Hackers -Online interests groups
Virtual Ethnography	-Only conducted online and within a virtual world	-Virtual participant observations -Internet mediated interviews and chats	-World of Warcraft -Second Life

Note. Adapted from Cyber ethnography: A critical tool for the Department of Defense?, by Black, 2016.

Due to the COVID-19 pandemic limiting travel and face-to-face interactions, the research team employed cyber ethnography to perform and collect all interviews. This gave the team significant flexibility in terms of location and schedules.

In order to conduct cyber ethnographic interviews, the team first created a selection of questions, informed by the first phase of research, theory and practice of intelligence analysis. The questions also contained openings for a narrative to unfold and for a greater examination of lived experiences in relation to the variables of interest to this study. Second, the team created an identity matrix that listed the names, positions, and organizations of all potential interviewees. This allowed the team to have a framework to contextualize each participant's perspective and unique position within the IC. The team originally sought to schedule 50 individual ethnographic interviews using Microsoft Teams. The research team understood and expected that the response rate would be low due to the pandemic.

The interviews were performed from December 2020 to March 2021, and overall the team managed to successfully conduct interviews with 17 individuals. Unfortunately, 33 participants either rejected or failed to respond to our requests, leaving us with a small gap in our intended representation of organizations. The research team tried to increase the participation rate of the DHS staff by sending follow-up requests via email, but a vast majority went unanswered. However, we found that our interviews did provide us with enough data to deliver this report, as they no longer produced new thematic trends. Our process of conducting the interviews included recording, transcribing, and storing all interviewee contact information on a secure cloud site. These interviews were assigned numbers to maintain interviewee anonymity throughout our analysis, including transcription and domain analysis.

The first set of interviews was conducted with a group of high-level DHS and IC officials to help identify the multipronged approach to intelligence within the U.S. government and provide the context that was not evident in the literature and document review. These interviews were used as a baseline to identify areas of improvement for DHS, which included core competencies and organizational values and goals, and tailor interview questions, particularly those aimed at intelligence analysts. The first set of interviews also identified gaps in content, quantity, and quality of training across the IC, diversity of training requirements and standards, and agency-specific initiatives that aim to improve knowledge and performance within the workforce.

At the end of each interview, participants were asked if they could suggest additional participants so that our research team could contact and interview them. Snowball sampling was utilized to allow for interviewers to network within an organization and expand the number of participants. Such sampling is commonly used by social scientists who study populations that are hard to identify and locate, such as the individuals within the IC workforce whose jobs require them to maintain a degree of anonymity. This project started with small sample of a population and sought to "snowball" them into a larger one over the course of this project. Snowballing is a non-probability sampling method, which ensures that there was no discrimination in interviewee selection. The snowball approach also allowed participants to decide whether they wanted to protect the anonymity to their colleagues by not providing contact information. Most preferred to make initial contact with colleagues before providing their contact information to our research team.

Once all 17 interviews were completed and transcribed, they were uploaded to *Atlas.ti,* a software tool used to systematically analyze large bodies of textual and multimedia data. Once the transcripts were uploaded, the project moved onto the next phase, or domain analysis. Domain analysis is "uncovering the system of cultural meanings that people use and involves a search for the larger units of cultural knowledge which are called domains" (Spradley, 1979). Once these larger units are identified, researchers search for semantic relationship. The semantic relationship is the linking of two categories or concepts together under one larger domain (or cover term). Semantic relationships provide the ethnographer with one of the best clues to the structure of the meaning in a particular culture. This research project's culture was the Intelligence Community participants and even more specifically, DHS.

Domain	A cultural meaning or term used for how things are done
Domain Analysis	The uncovering of cultural meanings that people use and involves a search for the larger units of cultural knowledge which are called domains
Semantic Relationships	The linking of two categories or concepts together under one larger domain

Semantic relationships lead directly to the larger categories that reveal the organization of cultural knowledge learned by informants (Spradley, 1979). Researchers identify the relationship in order to decipher the meaning of another culture and build a list of universal relationships. For example, this project went through all transcripts collected and started sorting out domains that represent certain concepts and cultural meanings to the participant. **Example: X is a kind of Y = An oak is a kind of tree.** The tree is a domain (cover term) for all x's, which is connected to the cover term or domain of 'y'. Another example: **Oak, elm, maple is a kind of 'Tree'**

When terms are identified, the researcher then starts identifying the type of semantic relationship the term has with the domain, which helps explains the cultural or communal understanding of the domain. Table 3 shows examples of relationships that can be identified during domain analysis.

Table 3

Semantic Relationships

Type (Semantic)	Relationship of X and Y
Strict inclusion	X is a kind of Y
Spatial	X is a place in Y, X is a part of Y
Cause-Effect	X is a result/cause of Y
Rationale	X is a reason for doing Y
Location for Action	X is a place for doing Y
Function	X is used for Y

Building on the first example, **Oak, elm, maple is a kind of 'Tree',** the 'is a kind of' is the type of relationship between the terms. This identifies what the categories mean to the overall domain.

It should be highlighted that domain analysis is a common method used when analyzing ethnographic interviews and transcripts. The research team decided to use domain analysis for this reason, and due to the fact that the IC has a cultural and communal knowledge that is not necessarily known to those outside of government. The team decided that breaking down their cover terms and units of cultural meanings in the field of intelligence training and education could help bring deeper insight than those conveyed only by the structured survey responses.

The research team began their domain analysis by first coding all common themes identified within the interviews, creating code trees that uncovered patterns in the participants' interview responses. This allowed the team to gain a much greater understanding of the way they conceptualized, lived, and practiced intelligence, and connected their core competencies to the broader mission. *Atlas.ti* analysis provided us with a visual map that linked different core competency code trees and gave us insight into whether the members of IC share the same understanding of analytic, writing, and critical-thinking skills, collaboration, and project management. Moreover, this project was able to identify how our interviewees prioritize other areas of importance and improvement such as technology and training/curriculum deficiencies.

Finally, despite having a small number of participants, our confidence in the reliability and generalizability of this study is further amplified by the high level of consistency in the findings identified in both ethnographic interviews and domain analysis. The combination of cyber ethnography with domain analysis, triangulated with secondary data, sets this research apart from previous reports and provides direct insight into the IC's challenges and best practices. Chapter Four explains and illustrates how the team used domain analysis for this research and specifically explains the relationships between the terms and domains found during the interviews.

Chapter Four

Findings

This chapter provides both the broader context of understanding DHS intelligence training and education and analysis of this year's theme - the core competencies for intelligence analysts. The research team found that it was necessary to do both in order to properly situate the issue of intelligence analyst training and education within a larger and more complex homeland security framework. After performing a comparative analysis of guidance and strategy documents regarding intelligence training and education programs Community-wide, and completing cyber ethnographic interviews, the team conducted domain analysis on the types of issues that impact DHS intelligence training and education. The analysis quickly revealed that **'training challenges and deficiencies'** is the cover domain for seven categories: **core competencies, specialized training, balancing demands, training delivery, communication and expectations, joint curriculum, and identity.** *Table 4* below summarizes those challenges and explains the semantic relationship with other terms, helping to answer the overall question outlined in Chapter One: What are the challenges, current trends, and best practices in intelligence training and education?

Table 4

Training and Education Deficiencies

Training and education challenges and deficiencies		
Main challenges (domains) identified	**Details on challenges**	**Associated challenge (associated domain) identified**
CORE COMPETENCIES	Lack of standardized DHS intelligence core competencies or basic entry-level training and education for intelligence analysts across all departments, organizations, and components. The core competencies are six key skills areas that analyst should know before assigned to their operational organization.	• Entry level training • Basic training • Technology • Communication (Briefing) • Writing (Critical writing) • Critical Thinking (Analysis & Research) • Project management (Leadership) • Collaboration (Engagement and Teamwork) • Technology (basic computer skills)
SPECIALIZED TRAINING	Lack or difficult to attend specialized training needed for an analyst to perform their job. Specialized training enhances the skill of an analyst in a specific functional or mission	• Forensics • Cyber • Open-Source training • Supervisor • Holistic Approach • FOUO

	area (i.e. counterterrorism or cyber).	- Executive - Cyber - Counterterrorism - Technical
BALANCING DEMANDS	Difficult to balance demands of training with operational needs. This domain puts training at a disadvantage, having it compete with the needs of the customer and placing training usually second on the priority list.	- Operational tempo - Customer needs - Throughput - Resources - Mission center - Operations - Non-standardized training to fill gaps (informal, private companies, Universities, contract or other organizational training)
TRAINING DELIVERY	Challenges in delivering training to all components, organizations of DHS, including state, local and tribal law enforcement.	- Training format – physical location - Blended learning - Training format – online - Co-locate
COMMUNICATION AND EXPECTATIONS	Challenges in defining DHS training expectations across the components and communicating training opportunities to organizations, supervisors and intelligence analysts.	- Advertise training - Leadership - Detail opportunities - Mentor - Proactive - Non-standardized training to fill gaps (informal, private companies, Universities, Contract or other organizational training) - Standardization of training (course development, guidance, tracking training, training feedback, required vs. not required, contractor cadre, workforce management)
JOINT CURRICULUM	Challenges in developing joint curriculum and training for the intelligence community and law enforcement.	- Culture - Intelligence community vs. Local law enforcement training - Different tasks and topics - Information sharing - Title 50 vs. Title 18
IDENTITY	Challenges in a collective identity due to Title 50 and Title 18 training requirements.	- State vs. Local mindset - Law enforcement working with intelligence - Title 50 vs. Title 18

These challenges (domains) help to understand the depth of issues that face DHS regarding intelligence analyst training and education program across its Departments, Components, and levels of government. This is not to be confused with issues and challenges facing DHS as an organization. Simply put, while seeking to learn more about the intelligence analyst core competencies, in the first year of research the team immediately identified a number of additional challenges posed to the overall intelligence analyst training and education. Although these were outside of scope for this specific research project, presenting these challenges (domains) is important as they highlight the need for DHS to understand that addressing core competencies is not enough to solve all the intelligence training and education problems. Secondly, these findings demonstrate the need for additional analysis and allow us to capture and organize all data collected through this initial investigation that can be used to contribute to follow-on years of research on the intelligence training and education.

In the following sections, this report discuss how this project identified and selected these specific challenges (domains) and then deconstruct each one of them individually to understand the overall context and core competencies.

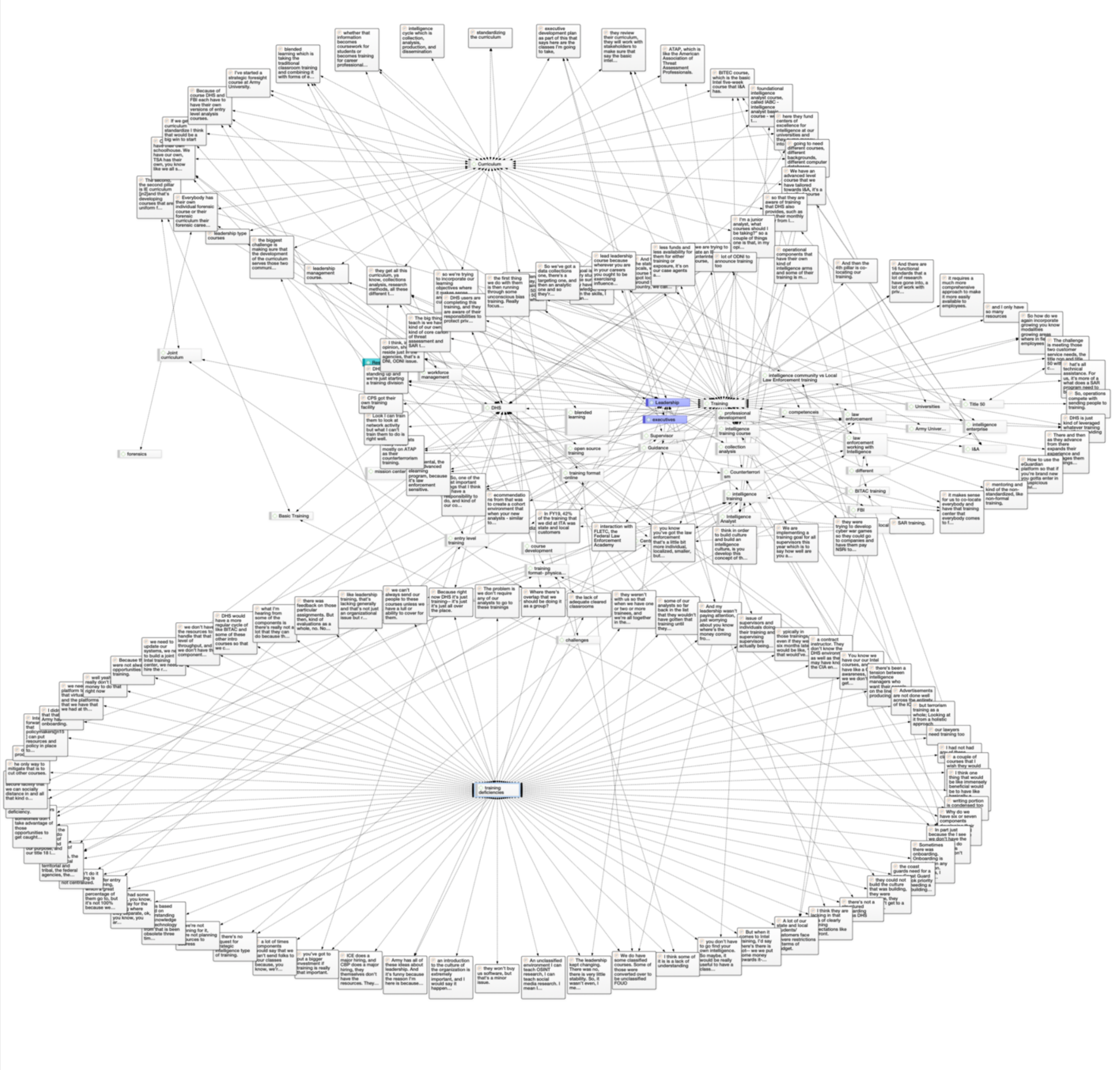
Understanding Training and Curriculum within DHS

The first part of the analysis was meant to provide a better understanding of the overall intelligence analyst training and education within the IC. It proceeds as follows:

Step One: The research team utilized *Atlas.ti* to code all interviews and identified three main domains that were of similar semantic relations: Curriculum, Training, and Training Challenges. *Figure 3* is the illustration of that analysis with the associated quotes collected from the interviews. The team then grouped the similar domains help to understand the challenges, current trends, and best practices in the intelligence training and education.

Figure 3

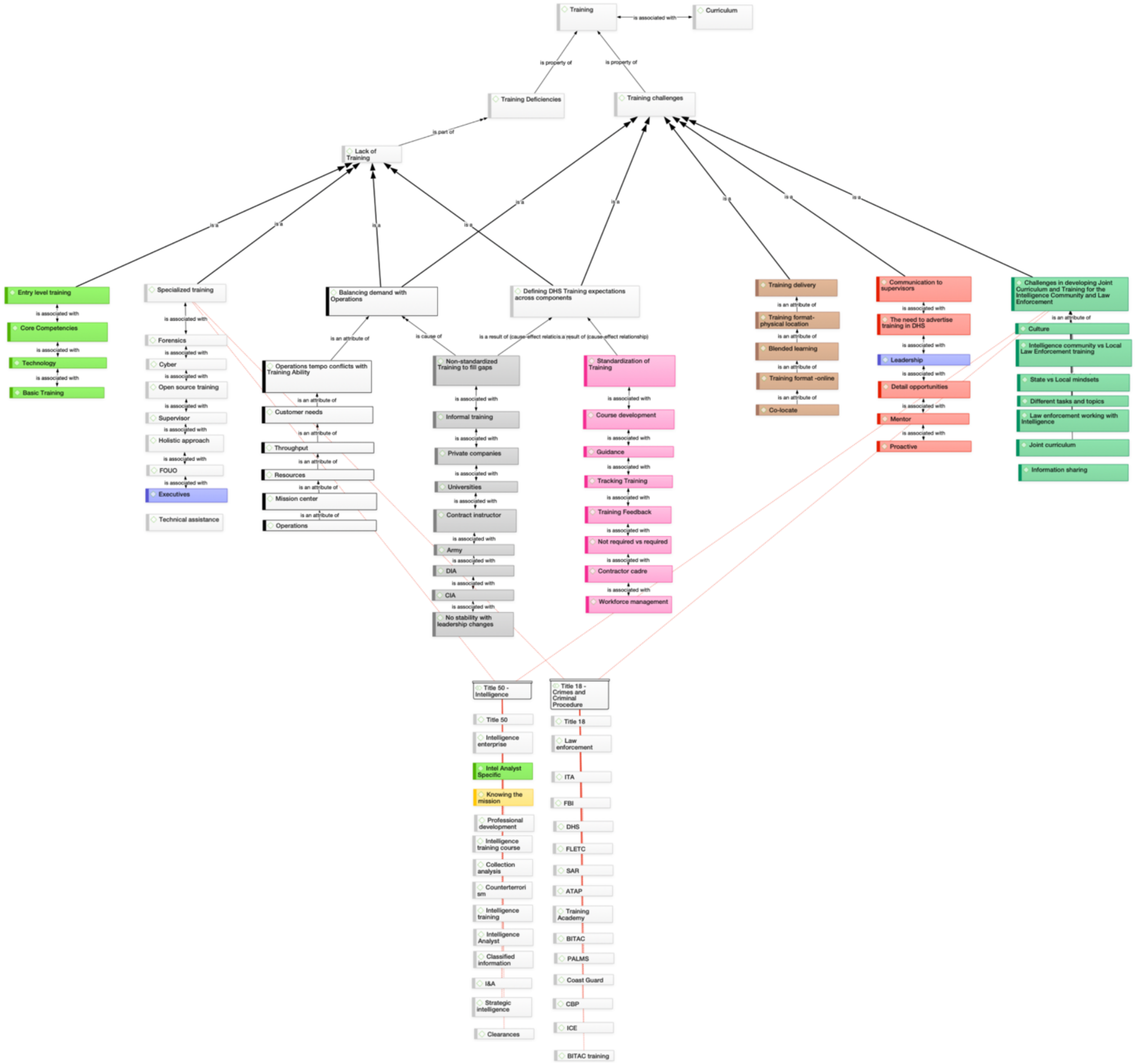
Illustration of Step 1 of Semantic Relation Analysis Using Atlas.ti



Step Two: *Figure 4* below illustrates how the codes from the ethnographic interviews were pulled together in *Atlas.ti* and grouped to the single domain of '**Training.**' There are two semantic relationships that were identified under that domain and they are '**training deficiencies and training challenges**.' These domain categories are not the same and needed to be separated, as '**deficiencies'** identifies training that is not currently present, and '**challenges'** are problems with the existing course offerings. The team then broke down '**training deficiencies'** to a **'lack of training'** – to show the relationship. In addition, *Figure 4* shows how the research team was able to structure and organize the data through multiple domains that were identified from the original set of data. It also breaks down the domains further on the issues that were identified under each: ‘**lack of training**’ (interchangeable with training deficiencies) and ‘**training challenges**’.

Figure 4

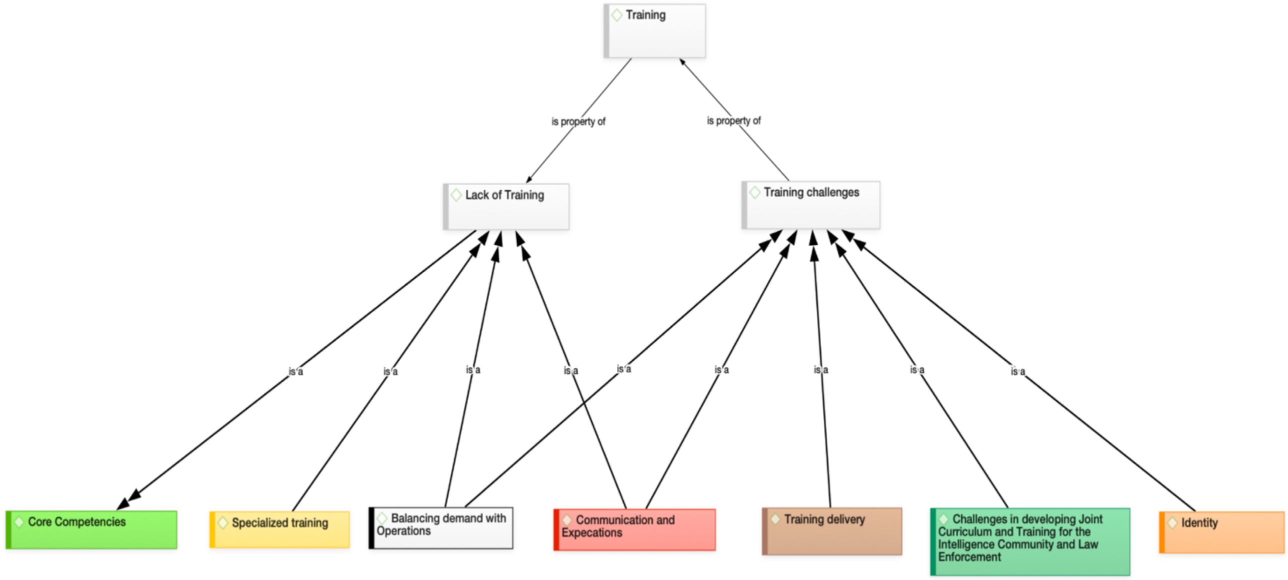
Illustration of Step 2 of Semantic Relation Analysis Using Atlas.ti



<u>Step Three:</u> *Figure 5* demonstrates how the team continued combining similar domains outlined in Step Two, to ensure repeated or alike domains were captured and placed under their associated domain.

Figure 5

Illustration of Step 3 of Semantic Relation Analysis Using Atlas.ti



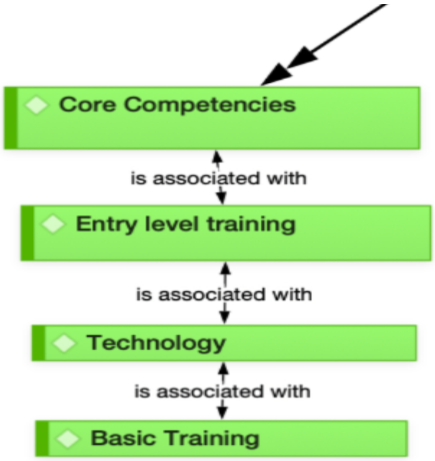
The main domain categories identified here are considered the most important challenges (domains) that face DHS training and education: core competencies, specialized training, balancing demand with operations, communication and expectations, training delivery, challenges in developing joint curriculum and training for the IC and law enforcement, and identity. These challenges were selected because the transcription of the quotes and analysis of all the coded interviews showed the semantic relationship of the categories. While the primary focus of this year's project analysis is on understanding the intelligence analyst core competencies, this reprot will briefly address each of the seven challenges.

Core Competencies

When analyzing **'core competencies'** as the first category of the domain, the team sought to specifically answer the question: What does it mean to be proficient as an analyst? As *Figure 6* illustrates, the first found that this category was part of the overall '**lack of training'** analysis where many interviewees identified it as a significant issue that needs addressing. This initial analysis also demonstrated that participants associate and use **'entry-level training'**, **'technology'**, and **'basic training'** interchangeably with core competencies, and identify all these terms as the same.

Figure 6

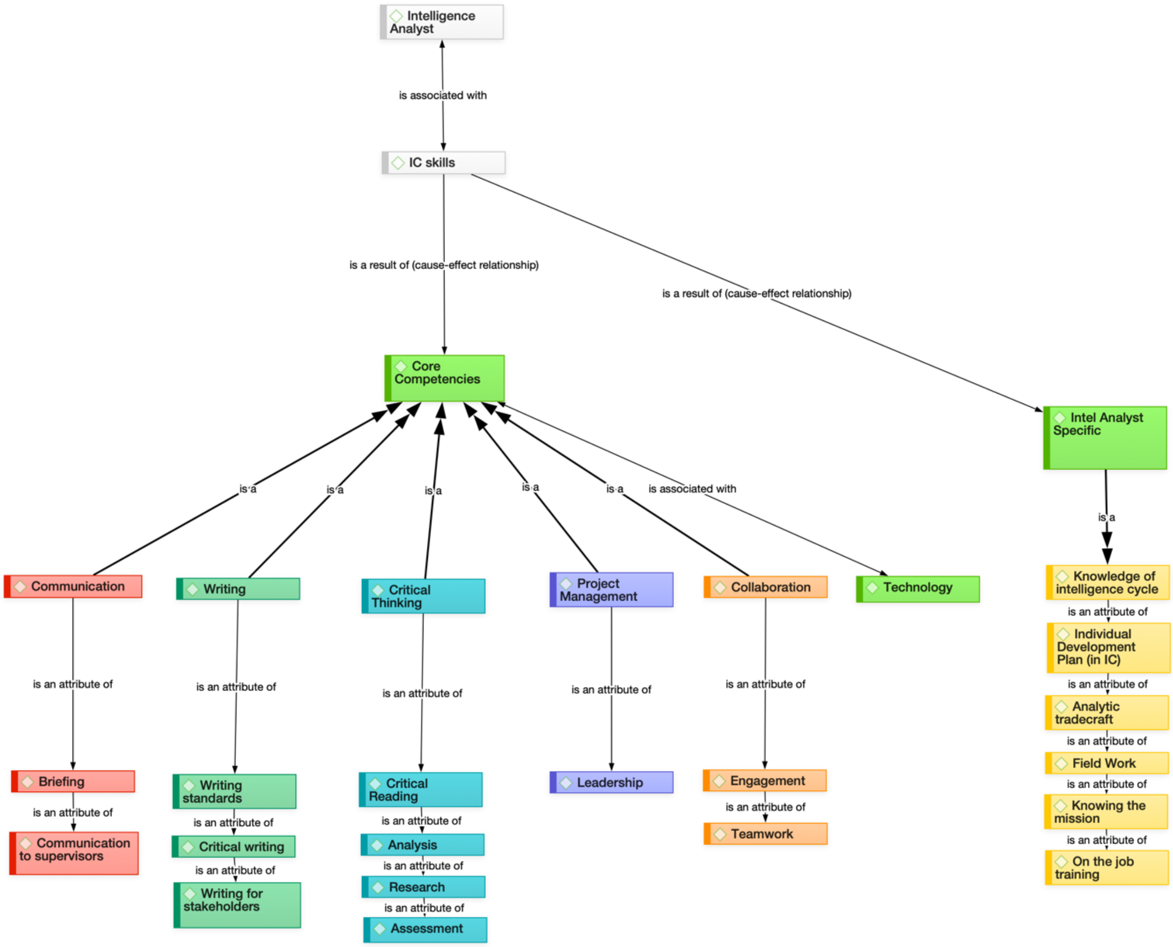
Illustration of Core Competency Deficiencies Using Atlas.ti



The team then broke down **'core competencies'** to understand its attributes and all other possible relationships. *Figure 7* presents the result of that *Atlas.ti* analysis. It is important to emphasize that these attributes are not ranked and are discussed in order they appear on the chart. Therefore, starting from the left side of the chart, many participants associated **'communication,'** or the ability to brief and communicate with supervisors and teammates as one of the main **'core competencies'**. The interviewees highlighted that when they interview or train new analyst, they must be able to communicate effectively. One interviewee explained, *"basically we're looking for the ability to do analysis and then be able to brief it."* Another one highlighted the importance of communication to the job, *"it was our job, as analysts, to filter through and produce these products which could range from just a two-minute briefing to a 30-page assessment for our executives on situational awareness of the threat environment."* Without this competency, the findings suggest, analysts are unable to communicate the results of intelligence analysis products to their supervisors and policymakers.

Figure 7

Illustration Core Competency Components Using Atlas.ti



Next, the participants also identify **'writing'** or **'analytical writing'** as a core competency. Below are a few quotes taken from the interviews that briefly highlight the importance of knowing how to write effectively:

"Look, I can train them to look at network activity, but what I can't train them to do is write well."

"Intelligence & Analysis (DHS) is writing and communication."

"Writing is one of the areas where I've been asked to take more concrete steps to address."

"At a strategic level like mine, you have to be able to write."

"We want you to produce these many reports."

"Writing for stakeholders- I meaning, writing, writing, writing. Report writing."

The team also identified that **'writing standards'**, **'critical writing'**, and **'writing for stakeholders'** are associated with the **'writing domain,'** which means they are used interchangeably. Furthermore, during the interviews, many participants stressed that analyst must come to their jobs already prepared to write at an analytical level, and they should gain those skills in an academic setting or during their previous employment in national security and intelligence. It was explained that someone attending a basic writing course would not have the necessary skills to perform the required tasks an intelligence analyst needs to be effective. The following quote clarifies that further:

"I want to make a distinction between basic writing versus analytic writing. Right, analytic writing adheres to ICD 203 standards for tradecraft. There is a team within I&A that is focused on ensuring analysts adhere to various tradecraft standards, so they themselves provide internal training and consulting to analysts so that they are adhering to quality products."

The research team did interview participants of basic intelligence courses and found that while writing is taught as a skill or competency, not all analysts go through this course prior to starting their position in a DHS organization, component, or local law enforcement. In fact, a common practice within DHS is to hire intelligence analysts and send them straight to their positions rather than have them take a basic intelligence course.

The next core competency identified as essential for an effective intelligence analyst was **'critical thinking.'** Critical thinking takes on many associated terms, such as **'critical reading'**, **'analysis'**, **'research'**, and **'assessment.'** Along with other competencies, participants emphasized that every intelligence analyst must be able and ready to critically engage and think through the problems DHS faces daily:

"You got to be able to think critically, you got to be able to communicate."

"It involves a lot of critical reading and writing skills, so I do a lot of research."

"Critical reading, critical thinking, and critical writing are like the top three. So just being able to, kind of, read in between the lines, take certain facts and think about them and how they might turn into certain outcomes."

"The critical thinking skills are just as important, meaning the synthesis of reporting and the presentation of that synthesized product."

"We're hoping that they have either learned a new analytic skill, so that could be how do you look at a problem and assess it for either a threat or look at it to try and solve the puzzle of question."

"Critical thinking is important."

Discussions on **'critical thinking'** highlighted the difficulty of acquiring this skill after being hired, and many participants argued that it is necessary to hire those candidates who already possess this competency rather than focus on training them afterwards.

"We try to hire people with an analytic mind. So, someone who is interested in looking at information and trying to connect the dots."

Fourth, participants identified **'project management'** as a core competency, along with **'collaboration'** and **'technology.'** However, these three core competencies are not as essential as the first three. That means that while an ideal candidate would possess all six core competencies, communication, analytical writing, and critical thinking are absolutely necessary. The **'project management'** competency is also associated with leadership, but not necessarily with a **'supervisor'**. The participants distinguish between an analyst needing to understand how to lead a project and those in charge of multiple people. Project management in the intelligence field means understanding what needs to be done to fulfill requirements and completing the task.

Similarly, **'collaboration'** was highlighted as an important core competency as analysts are required to work with others outside of their organization or field of expertise. The following interview quotes offer a more in-depth look into that:

"We want you to you know how to collaborate with outside organizations."

"Kind of just as a general rule we do tend to collaborate with other mission centers within I&A and then with other partner agencies."

"Researching, writing, collaborating."

"Collaborating on a product while its being written, I would assume that it would involve more either in-person, when it's not COVID, or, you know, phone calls, team meetings."

"So, there's the core competencies established by OPM and each agency then kind of, you know, implement it, accordingly. So, there are five core competencies that are reflected in each employee's performance plan. So that would be like teamwork, communication, leadership, representing the agency, and in engagement and collaboration, application and the skills behind it."

"I would say a lot of the collaboration happens at the analyst level."

Finally, **'technology'** was briefly discussed in the interviews and is considered the least important competency of the overall six core competencies of an effective intelligence analyst. However, the team found that many participants explained that a basic understanding of technology is required for an analyst to do their job. A few participants expressed that, *"we need a more technical talent pool"* and *"let's get everybody on the same platform across DHS in technology and let's use technology to link us all together."*

Therefore, the team understood that including 'technology' as a core competency would be vital as DHS moves forward in their training and education. It is clear that DHS staff continues to struggle with system functionality and integration of technology into their analysis, and there are deficiencies as there are no identifying, prioritizing and integration of this competency into training and education. Being able to collect, analyze and interpret data from up to 27 distinct DHS information systems and databases is a must for every DHS intelligence analyst.

Furthermore, the team uncovered that many academic intelligence studies programs have already integrated STEM-related courses into their offerings, based on intelligence requirements and ODNI needs assessments. Therefore, adding 'technology' as a core competency was identified as a reasonable contribution to the list of skills an analyst needs to perform their job effective.

Discussion

The six core intelligence analyst competencies listed above are not necessarily new to most members of the IC. Chapter Two has already discussed all of them as part of the review of the existing literature and documents from federal agencies identifying their own 'core learning objectives' that an analyst must have (FBI, 2020). What the team found, however, is that despite the general acceptance of these core competencies by the agencies, they are not fully integrated into the existing intelligence education and training programs due to a number of constraints across the Community, ranging from the lack of resources on all levels of government, confidentiality restrictions and clearances that make it difficult to disperse high-value data to varied and non-complementary combinations of internal and external training programs. Furthermore, in the absence of standardized and mandatory testing, most participants agree that it is difficult for the Intelligence Community to professionalize, evolve as a field, and ultimately, prevent and combat the increasingly decentralized threats.

Moreover, the analysis revealed that there are many agency-specific networks that provide document libraries yet lack application knowledge and collaborative relationship models needed for intelligence sensemaking and discovery (Wu, 2013). In interviews, many participants noted the need for collaborative assessment tools to track training as did some documents we reviewed (ODNI, 2011). For example, when joint networks like Intellipedia, Terrorist Identities Datamart Environment (TIDE), Advanced Global Intelligence Learning Environment (AGILE), and Homeland Security Information Network (HSIN) were implemented, efforts to promote counterterrorism cooperation strengthened each agency's ability to anticipate new threats and increase coordination and crisis response (Department of Defense, 2015; Terrorist Identities Datamart Environment, 2020; U.S. Department of Homeland Security, 2021). Such collaborative data sharing networks create common foundational intelligence training at various levels to identify the evolving demands shared between military and civilian professionals. However, if an analyst does not have basic technological skills to access and understand these databases, such networks become underutilized and data analysis problematic.

Furthermore, one of the most significant findings that relates specifically to DHS is lack of standardized training across the entire organization, including state, local, and tribal agencies. One participant explained that:

> *"right now, everybody does their training in different buildings all dispersed around DC and down in Yorktown in Virginia and some of that is necessary because the Coast Guard does have some specialty training in some areas and their basic courses. But for the courses that overlap across the Intelligence Enterprise, it makes sense for us to co-locate everybody and have that training center that everybody comes to for their intel training."*

In fact, the analysis demonstrated that there are no current standardized intelligence courses that *all* DHS intelligence analysts can attend to obtain core competencies before starting their job. This means that analysts are trained differently with divergent core competencies and skills, which makes transitioning to other components, collaboration among different analysts and teams, and even verbal and written communication with senior leaders challenging and at times inadequate. The following quote captures the dramatic need to address these issues:

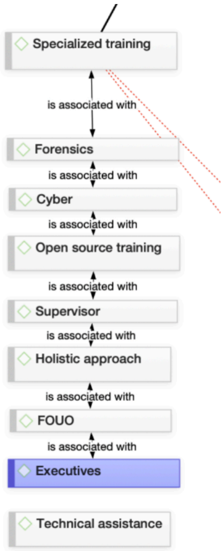
"You got 22 different components doing their own training thing based on their historical training needs and how they did it historically. And historical systems that are 20 years old now or more maybe a few updates here there. It's time for DHS to invest in reorganizing and updating training across the Department."

Finally, although the primary focus of this year's report was to identify specific core competencies an intelligence analyst must possess to be effective across multiple components and organizations of DHS, and recommend their integration into education and training, our team also identified additional issues that negatively impact training and education. In the following section, the research team briefly examines all the domains that presented themselves during the interviews. The recommendations will not cover the issues presented below, rather these will be addressed individually during follow-on years as discussed in Chapter Six.

SPECIALIZED TRAINING: The team discovered that '**specialized training'** domain had the following associated categories: **'forensic'**, **'cyber'**, **'open-source training'**, **'supervisor'**, **'holistic'**, **'FOUO'**, **'executive'**, and **'technical assistance'**. These domains were used interchangeably with **'specialized training'** due to their semantic relationship. This means that when an interviewee commented on attending a **'forensic, or cyber course'** this could also be labeled or could mean a **'specialized training**' that an intelligence analyst needs to be effective at DHS.

Figure 8

Illustration of Specialized Training Components Using Atlas.ti



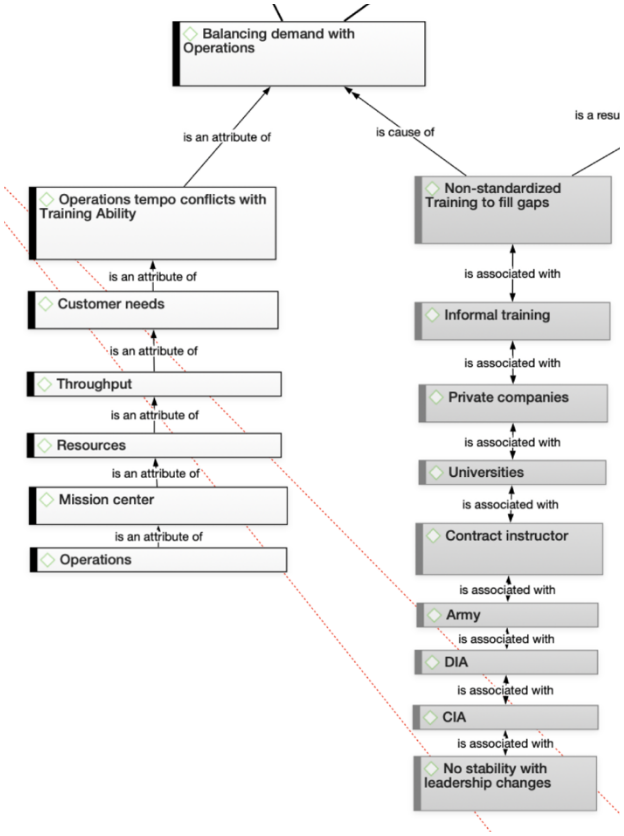
The courses identified during the interviews point to technical or specific skills an analyst will need in certain components or organizations. Many interviewees explained that due to DHS's functions that pool 22 different Federal departments and agencies, each with a different set of responsibilities, specialized training remains highly compartmentalized as DHS did not execute a standardized department-wide course. Instead, each organizations within DHS has its own training. The participants identified this as a major shortfall in receiving specialized training that affects their job preparedness and overall effectiveness. For example, one participant commented that "*everybody has their own individual forensic course or their forensic curriculum and their forensic career path."* There were also specific references to a **'lack of training'** as many interviewees felt that there was not enough specialized, either local or online training to fulfill the demand for more flexibility, cheaper options and less travel.

In addition, the interviewees identified technical, cyber, and forensics (computer) training as lacking within DHS, as well as coursework on both Title 18 and Title 50. Overall, this domain needs further investigation in terms of demand, types of specialized training needed, benefits to the overall DHS mission, and connection to specific mission areas such as counterterrorism. For example, when asked about courses for intelligence analyst that specialize in counterterrorism (CT), participant said "*you know we have our intel courses, and we have like a CT awareness, but we don't really get into the actual CT training."* Others suggest that integrating such training can be difficult to DHS as *"we don't have the resources to do what the IC is doing. We don't have the resources to match what the agencies do on CT and what DoD is doing."* As DHS adjusts its strategic vision to focus on domestic counterterrorism, among others, this analysis demonstrates that there is a need for a more standardized and specialized courses in CT in order to accomplish the mission across the entire department.

BALANCING DEMANDS: The team discovered that **‘balancing dem**ands’ has two distinct cover domains, which are **‘operational tempo conflicts with training availability’** and **‘non-standardized training to fill gaps’**.

Figure 9

Illustration of Balancing Demands with Operations Challenges Using Atlas.ti



There are several issues related to the overall **‘operational tempo conflicts with training ability’** and all show the semantic relationship. This means that they are the same domain, just phrased differently. For example, it has semantic relationships with topics that are connected to **‘throughput’**, which for many intelligence analysts means having the opportunity to train constrained by the need to meet their day-to-day job tasks and requirements. It is simply not possible for them to leave their jobs in order to gain more training. Additional constraints associated with **‘operations tempo conflicts’** include having to meet **‘customer needs’** as well as **‘operational’** and **‘mission center’** needs, and the overall lack of **‘resources’**. Therefore, when highlighting the lack of training due to the difficulties of **‘balancing the demand of operations’**, we must think in terms of all of these different issues identified by the participants. For example, one interviewee explained that *“operations compete with sending people to training, that's definitely the bottom line.”* This competition between training and operations is not necessarily big news for anyone working within government organizations, but this particular domain emphasizes that DHS struggles to find the balance between the time it demands analysts spend on supporting the mission and time it allocates to the same analysts to train and learn about the ways they can effectively support that mission. The following two quotes illustrate the problem:

"We offer up our new analyst training to all the components. So, they're welcome to come. Yes, we do have some challenges with wait lists now, but we will put them on a wait list and get them in. But that does compete with operations, and that's always been an ongoing challenge."

"We offer three courses, they'll get their people through, but they can't get them through as quick enough only because, going back to the point, they can't enroll their people all at once. We've, over the last couple years, we've struggled with the throughput and so we've put a big effort and this year is going to be extremely important to getting all that training back up to speed, and sort of building that you know systematic approach to how we're getting people through all the entry level training.

As highlighted in *Figure 9*, the second domain associated with **'balancing of the demand with operations**' is the **'non-standardization training to fill those gaps.'** The sematic relationships with other domains associated are **'informal training'**, **'private companies'**, **'university training offerings'**, **'contract instructors'**, **'Army courses'**, **'DIA/CIA courses'**, and **'the lack of stability with leadership changes.'** The analysis of these domains showed that because many are not able to attend DHS Basic Intelligence and Threat Analysis Course due to the constraints identified under the **'operational tempo conflict'**, they resort to other types of **'non standardized training'** programs to fill the intelligence analyst core competency gap. Simply put, DHS and its components have had to find alternative courses and instructors to ensure their analysts are trained to fulfill their role and perform the mission essential tasks. When it comes to **'informal training'**, the team found that often it is obtained through private companies, universities, contractor instructor, or other agencies. While this meets some of the immediate training needs, it does not address the need for standardization of the core competencies or specialized training and can create additional issues.

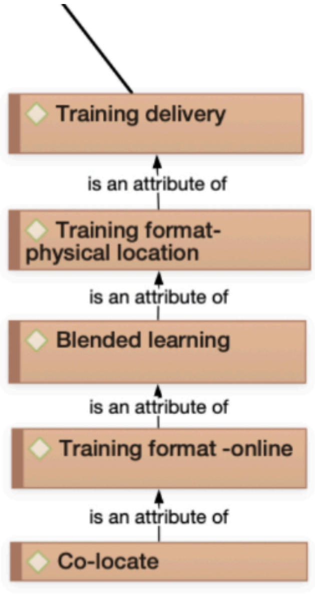
"So, we utilize contract support to help fill those gaps, you know, but the challenge with contractors is they are experts in their areas. For example, say they taught in the Intelligence Community, and then they come to teach with us as a contract instructor. They do not know the DHS environment, as well as they may have known the CIA environment, or the DIA environment. So, there is a learning curve when you utilize contractors. And the problem is, unlike a federal employee, as soon as you get them up to speed, the contract is over, and they go."

This analysis also demonstrated that many intelligence organizations besides DHS also utilize informal or non-standardized training to fill their training and education gaps when experiencing increased operational tempo. However, most participants agreed that this is not a good long term solution specifically for DHS because along with **'no stability with leadership changes'** can exacerbate and cause more training and education problems.

TRAINING DELIVERY: The next challenge to the overall DHS intelligence analyst training and education identified in this analysis is **'training delivery'**, particularly as it relates to its work with local, state, and tribal entities. The following domains were found to be associated with this challenge *(Figure 10)* : **'training format physical location'**, **'blended learning'**, **'training format – online'**, and **'co-locate.'**

Figure 10

Illustration of Training Delivery Challenges Using Atlas.ti



These domains demonstrate that there are a variety of ways in which DHS delivers training for all components and organizations (either specialized training, standardized or non-standardized). The team has also discovered complications associated with training state and local law enforcement across the country. Obtaining funding to travel to DHS training facilities is difficult because many agencies and organizations have rather limited or few resources to provide. Therefore, completing standardized training or meeting training requirements becomes complicated from the moment the new intelligence analyst is hired.

"So, there were some state and locals who couldn't even come here to take our classes because they couldn't afford to attend."

"A lot of our state and local students/customers face severe restrictions in terms of budget."

The resources issues are not limited to the state, local, and tribal intelligence analysts, but also impact the entire spectrum of training delivery for DHS.

"The biggest challenges now are waitlists and delivering the training fast enough. It's a six-week course, we can only deliver so many of those per year. And so, additional resources would help with hiring additional instructors, even if they're doing it virtually, to deliver more of the courses. This is a challenge. And one of the things that typically happens - in hiring in government, is it kind of goes in waves."

“We don't have enough instructors.”

“The Coast Guard needs a new Coast Guard cutter, that took priority over us needing a training building.”

“These surges of training that's needed, but you still have the same resources and same instructors that you can't surge that capability.

“ICE does major hiring, and CBP does major hiring, they don't have the resources. They have a challenge getting their folks through. Even Coast Guard sends their intel folks to us because their program can't get everyone through.”

As this research was conducted during COVID-19, the team quickly learned that there was a significant impact in training delivery due to the pandemic. Due to the training facilities shutdown and individual state, local and tribal government shutdowns, DHS was forced to transform and adjust immediately. Many of the interviewees reflected this as one of the positive impacts out of COVID-19 as it increased the accessibility of training to local and state employees through online or remote training programs.

“COVID forced the positive effects of blended learning in a way that we would have had a harder time doing, but the positive outcome of that is increased student participation from across the country.

Instructors recognized that they were able to train more analysts and deliver content quicker via online platforms. More analysts were able to access it without needing to obtain travel funds and spending too much time away from their jobs. All agree that there is a need to continue offering these remote or online courses even when most COVID-19 restrictions are lifted across the country. Some interviewees discussed the issues related to the virtual environment content delivery that should also be addressed:

“We need a platform to deliver that virtual training and the platforms that we have that we had at the time at the beginning of COVID were inadequate.”

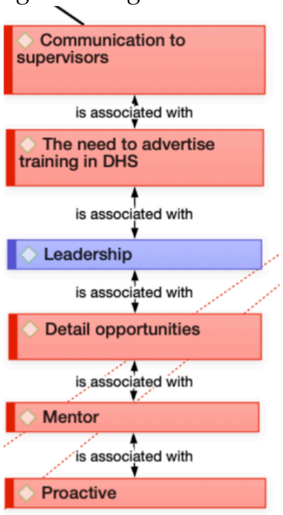
“Now with the virtual environment everybody, wants to take them, and so now we have the challenge of getting more resources in order to deliver more courses, or more iterations of the same course, because the virtual learning has just skyrocketed.”

Finally, the team found there was also acknowledgement that not all courses can or should be offered virtually, especially those containing classified or sensitive materials. These courses must be conducted in person and within secure areas. This research team acknowledges that **‘training delivered in-person and online’** deserves a lot of additional research, specifically on how to organize and sustain such delivery across all operational needs of the DHS enterprise. Due to the unique culture and organization of DHS, exploring this question further could significantly improve some of issues presented above.

COMMUNICATION AND EXPECTATIONS: The research team found that receiving communications and clear expectations from leadership and department on training and education opportunities posed a challenge for intelligence analysts. It was expressed by participants that supervisors would rarely identify intelligence training and professional development course offerings and their schedules course. *"Supervisors and individuals sometimes don't take advantage of those opportunities to get caught up on their training."* The team also found this domain had semantic relationships with the associated domains of, **'the need to advertise training in DHS'**, **'leadership'** communication, **'detail opportunities'**, need for **'mentorship'**, and being **'proactive.'**

Figure 11

Illustration of Communication Challenges Using Atlas.ti



Throughout the interviews, participants explained that DHS is a very large department with various training programs and organizations that supply their own courses and curriculum. Occasionally, course offering is not communicated or advertised to organizations, and the supervisors that manage analysts. This challenge is not necessarily a DHS problem, but as the team has found during the review of guidance documents, it is an issue that affects the entire IC. According to a report by the Inspector Generals of the Intelligence Community, the Department of Homeland Security, and the Department of Justice, the IC lacks balance in information dissemination and interagency communication (2017). This communication gap is caused by physical location limitations, competing agency mentality, poor execution, and management of already developed Joint Intelligence Training competencies, outdated training methodology and source materials, as well as "federal agency vs. military operations" differences (Builta and Heller, 2011; Department of Defense Office of Inspector General, 2014). Lack of sharing information is the most cited inefficiency in mission success within the IC (Builta and Heller, 2011). However, to promote more collaboration, DHS has made domestic and international collaboration a guiding principle in their 2019 Strategic Framework for Countering Terrorism and Targeted Violence to address, "threats with interagency collaboration, including effective intelligence and information sharing, as well as capacity building" (2019, p. 12).

The challenge that DHS faces here was best captured by one interviewee who pointed out: *"Why do we have six or seven components developing their own basic Intel training* *course?"* This makes the career path of an intelligence analyst unclear and problematic, especially for those who would like to advance further within DHS and move across components. While the lack of standardization between components confused some participants, others explained that requiring standardized training across the organizations would be insufficient and prove difficult. "*The main reason is that most of the components have their own internal training anyway. They must get their analysts up and running to do their mission and their support."*

Next, it is crucial to understand that **'communication'** and **'expectations'** domains were combined due to the similar semantic relationship to both **'lack of training'** and **'training challenges'**. For example, the team found that standardization of training includes other domains, such as the need for: **'course development'**, **'guidance'**, **'tracking training'**, **'training feedback'**, understanding what is **'not required and require'**, **'contractor cadre'**, and **'workforce management'** expectations. These also overlap with communication challenges.

Figure 12

Illustration of Expectations Challenges Using Atlas.ti

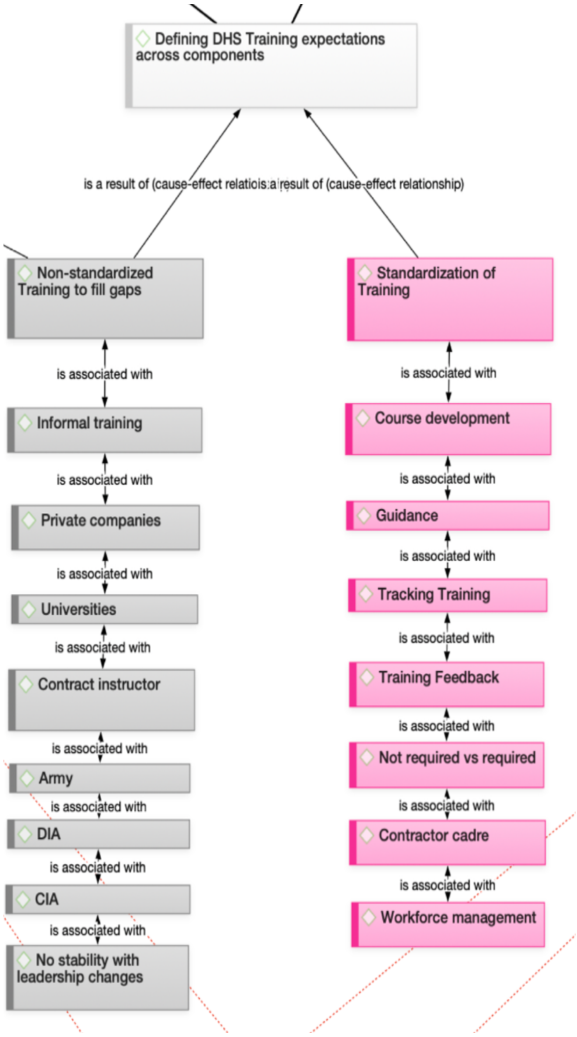


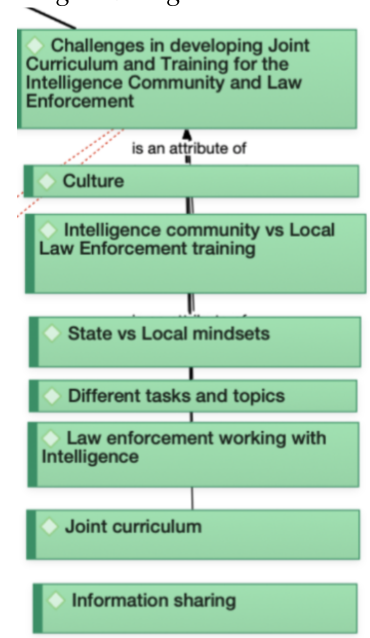
Figure 12 confirms what was already understood during the interviews: while there is an attempt to standardize training and education across the components, there is also a need for the components to have their own training. The research team is not suggesting that non-standardization is better than standardization. Rather, the empirical analysis revealed that there are two contradicting perspectives regarding the intelligence training and education within DHS. While the interviews provided a valuable insight on the lack of defined expectations, the contributing domains identified above require further investigation to clearly understand how DHS training is communicated and what is expected for the intelligence analysts.

JOINT CURRICULUM: Within the **'challenges in developing joint curriculum and training for the Intelligence Community and Law Enforcement'** domain, there were many associated domains: **'culture'**, **'intelligence community versus local law enforcement**

training’, ‘**state versus local mindsets**’, ‘**different tasks and topics**’, ‘**law enforcement working with intelligence**’, ‘**joint curriculum**’, and ‘**information sharing issues.**’

Figure 13

Illustration Joint Curriculum Challenges Using Atlas.ti


Challenges in developing Joint Curriculum and Training for the Intelligence Community and Law Enforcement
is an attribute of
Culture
Intelligence community vs Local Law Enforcement training
State vs Local mindsets
Different tasks and topics
Law enforcement working with Intelligence
Joint curriculum
Information sharing

These domains have many complex associations with deep inherent challenges in developing joint curriculum for all organizations underneath DHS (Figure 13). DHS has a different organizational culture than other federal intelligence agencies, which in turn, also means a different training culture. The biggest difference is that DHS must develop intelligence analyst training for both local law enforcement and the intelligence community. The analysis showed that DHS is struggling to establish the intelligence analyst curriculum requirements that could adequately address the training and education needs of these two completely different target audiences (this will also be discussed during the ‘identity section’). This already poses a challenge for external academic programs set to serve DHS. Internally, this joint training and curriculum requirement causes problems due to the potential issues in regulations and policy.

“Challenges, I guess you'd say, is we're teaching to different authorities. Most federal customers are dealing with strategic intelligence, which is looking out, you know, strategically based on information what the future picture might look like. Then there's tactical intelligence, which is what a lot of local police and even our federal partners, like CBP, and TSA, Secret Service - they might be doing more tactical intel. So, that difference in intel when you're teaching a basic intelligence class, you of course must introduce all the different types of intelligence, because if you talk about one and not the other, now you’ve just alienated half your class. So, it's a very difficult balance of making sure that you cover the different types of intelligence products.

Designing a single curriculum for all DHS intelligence analysts can be difficult as it would have to address two different audiences operating under two different legal statutes: Title 18 or Title 50. These two statutes help explain why when it comes to training, DHS seems to suffer from an identity crisis.

"'One department' is nice, but honestly, we all have a different focus. We have different mission statements; we have different statutes that we are responsible for. And everyone at ICE needs to know certain things about ICE's mission, and that's not the same as CBP. So they're going to need different courses, different backgrounds, different computer databases, and understandings."

As discussed in Chapter Two, there have been studies and efforts to bring certain trainings that overlap together. A participant commented:

"Where there's overlap, shouldn't we be doing it as a group? We haven't made that startup investment for training for Intel training across the Department. We're being asked to unify this, but it's a taboo of training to ask for resources. Everybody thinks that training has enough resources to do what we need to do, but they keep on asking for us to do more with the same resources."

DHS Office of I&A has been working on this challenge, and *"trying to do joint curriculum, joint deliveries, and even facility."* Participants acknowledged that even though there are current efforts in this area, total cohesion is still difficult due to the dueling identities faced by DHS. However, they also recognize that collaboration and teaming up on courses would help increase resources and provide more opportunities for intelligence analysts.

"Just something that's comprehensive for both DHS and FBI would be immensely how helpful."

"We're not just building it for I&A we're building it with the end goal of unifying the intelligence enterprise training."

Recent efforts in creating working groups have resulted in positive outcomes for the joint training and education and address some collaboration challenges that face the DHS enterprise. Some suggest *"a joint career path working group, a joint curriculum working group, a joint instructor working group and joint facilities working group."* While more research is required on this particular issue, given that **'joint curriculum'** domain is closely related to the **'core competency'** domain, the team concludes there is need for the DHS enterprise to establish a cohesive training identity, share resources, fulfill training requirements, and produce effective intelligence analyst.

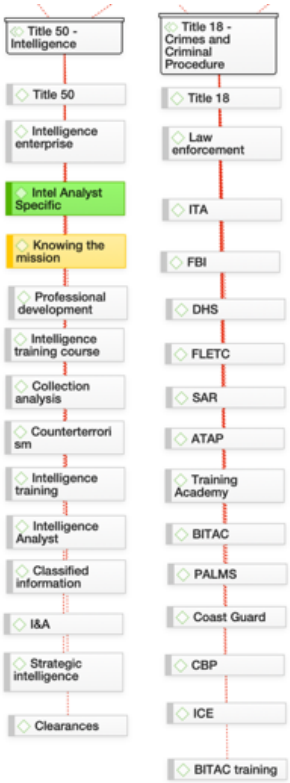
IDENTITY: As the previous section demonstrates, DHS training and education issues are closely related to the absence of a collective identity that stems from having two different legal statutes: Title 50 and Title 18.

Title 50 outlines the role of War and National Defense in the United States Code, and directs the Director of National Intelligence as the head of the IC with the responsibility to keep

Congress informed on all intelligence activities except covert action (Congressional Research Service, 2019). Title 50 organizations and associated DHS employees have a different function and access to a larger intelligence budget. Furthermore, intelligence requirements, training and education are also governed under Title 50. Therefore, Title 50 DHS employees are charged with national security or intelligence missions which are inherently different than Title 18. During our investigation, the research team noticed that Title 50 also related to specific relationships and domains, including **‘intelligence enterprise’**, **‘intel analyst specifics’**, **‘knowing the mission’**, **‘professional development’**, **‘intelligence training courses’**, **‘collection analysis’**, **‘counterterrorism’**, **‘intelligence training’**, **‘intelligence analyst’**, **‘classified information’**, **‘I&A’**, **‘strategic intelligence’**, and **‘clearances’**. The Title 50 relationship directly connects many of the courses, training, and curriculum along with the intelligence community regulations, which impacts how training is conducted and delivered.

Figure 14

Illustration of Title 50 and Title 18 Challenges Using Atlas.ti



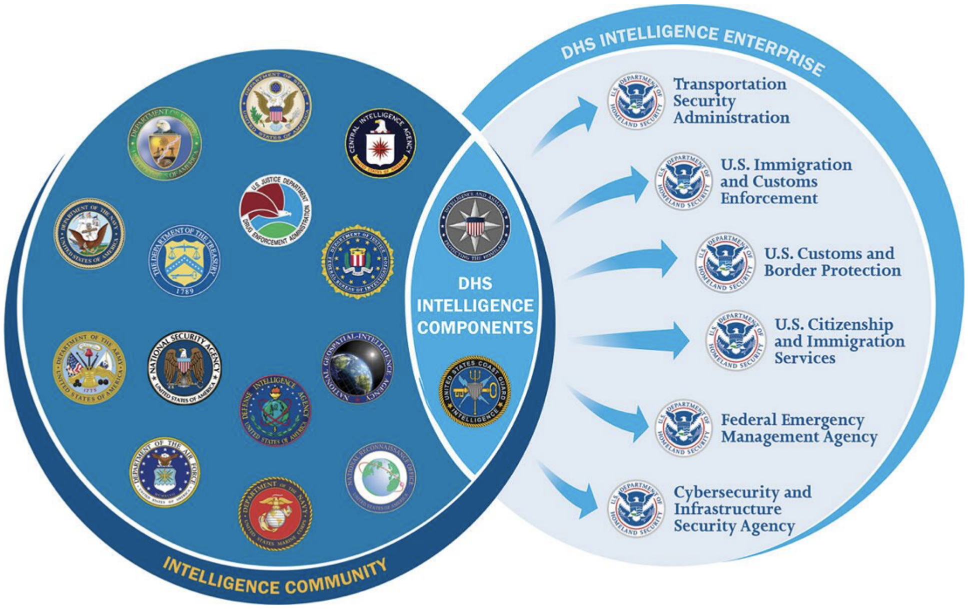
Title 18 refers to federal crimes and criminal procedures including the definition of crimes, the criminal procedure, prisoners, corrections of youthful offenders, and immunity of witnesses. DHS employees operating under the Title 18 policy are subject to different training jurisdictions and budgets, but still provide intelligence analyst-like functions. These organizations have generally smaller budgets than Title 50 organizations despite overlap between missions. In addition, Title 18 is related to **‘law enforcement’** domain and a long list of agencies and training programs and courses: ITA, FBI, DHS (sections), FLETC, SAR, ATAP, Training Academy, BITAC, PALMS, Coast Guard, CBP, and ICE.

Throughout the interviews, the research team has heard that Title 50 and Title 18 differences continually drive a wedge between the intelligence analyst and their training and education requirements and programs across the DHS enterprise, causing many of the employees to have an identity crisis.

"DHS morale is low, and the morale is low for multiple reasons. They're floundering on what they own, and they're too large in some ways. People aren't excited. When I meet people from CIA or FBI, they're typically like-yeah-they're proud of where they work. DHS does not have that same identity. That's got to come from the senior management. They got to establish some programs that people are excited about when they come to DHS. They understand where they fit when they come to DHS. It's not about being an intel analyst, it's about understanding DHS first. What's the mission? What's the vision? What's the goal of DHS? What's the reason for DHS? Why are they getting up every day and doing this work?"

Figure 15

DHS Intelligence Enterprise


DHS INTELLIGENCE ENTERPRISE
INTELLIGENCE COMMUNITY
DHS INTELLIGENCE COMPONENTS
Transportation Security Administration
U.S. Immigration and Customs Enforcement
U.S. Customs and Border Protection
U.S. Citizenship and Immigration Services
Federal Emergency Management Agency
Cybersecurity and Infrastructure Security Agency

Note. Data from https://www.dhs.gov/intelligence-enterprise.

It is clear that having to operate under two legal codes can confuse the organizations or component when identifying who responsible for which mission (*see Figure 15)*. For example, the FBI is the primary federal agency that is responsible for handling counterterrorism cases, yet such investigation may fall into overlapping jurisdictions between agencies. In 2013, the Boston JTTP, CBP, TSA and USCIS were all contributors to the 2013 Boston Marathon bombing investigation (Office of the Inspector Generals of the Intelligence Community, Department of Homeland Security, and Department of Justice, 2017). Due to the multifaceted investigation, there were issues on the interpretation of interagency information sharing MOUs which in turn undermined their ability collaborate on this case (Office of the Inspector Generals of the

Intelligence Community, Department of Homeland Security, and Department of Justice, 2017). Furthermore, the *Review of Domestic Sharing of Counterterrorism Information* found that the quality of relationships between DHS components and the FBI is highly variable and can create additional collaboration and information sharing issues. FBI's lack of collaboration with ICE and HIS, for example, has been attributed to the FBI not understanding the missions of ICE and HSI. On the other hand, FBI and CBP have a healthy working relationship that has been attributed to CBP's distinct authorities and unique access to information on foreign travelers (Office of the Inspector Generals of the Intelligence Community, Department of Homeland Security, and Department of Justice, 2017).

The 2016 review of the DHS Intelligence Enterprise stated that, "The DHS IE does not have a consolidated intelligence doctrine and the CINT does not have full awareness of all terrorism-related intelligence sharing agreements into which the various DHS components have entered. As a result, personal, rather than institutional, relationships play a major role in determining the effectiveness or ineffectiveness of intelligence sharing within and between federal and non-federal entities." An additional recommendation from the 2016 review of the DHS Intelligence Enterprise includes re-issuing the directive defining the DHS IE to explicitly identify which components are part of it (Department of Homeland Security Committee, 2016, p. 4).

Despite efforts by DHS to have a unified counterterrorism mission, the 2017 *Review of Domestic Sharing of Counterterrorism Information,* found that the DHS Intelligence Enterprise was fragmented due to, "elements operating independently" and lack of repercussions or incentives to coordinate cooperation outside of "actual events." I&A is subject to IC directives and standards but not component intelligence programs, except when IC directives have been institutionalized into DHS guidance (2017, p. 15). Differing procedures and expectations for components of DHS contribute to both the lack of a unified DHS identity and challenges to cooperation among the DHS components, their individual missions, and the overarching DHS mission of national security.

This lack of identity could be the cause of the high turnover rate at DHS. The 2020-2024 Strategic Plan emphasizes the need for a human capital pipeline to fulfill the demand for highly skilled workers and leaders in the intelligence community (Department of Homeland Security, 2019). To combat the high turnover in the intelligence community, DHS has implemented rotational assignments to employees. Rotational assignments are meant to increase professional development and advancement, as well as unify the DHS components under a common mission (Stone, 2021). One study found that despite such diversification efforts by DHS, unclear missions and poor implementation of such programs remain part of the overall cultural identity problem.

"I think in order to build culture and build an intelligence culture, you [must] develop this concept of the cohort."

"An introduction to the culture of the organization is extremely important, and I would say it happened 50 percent of the time."

The research team suggests that a further investigation on the **'identity'** domain would also assist in intelligence training and education for DHS as it negatively impacts intelligence analysts' training and education, and their retention.

In sum, while the analysis identified the six core intelligence analyst competencies, it also recognizes that is difficult to study them without consideration of a number of other issues that are affecting intelligence training and education. However, due to the nature of this year's research task, the following chapter provides only recommendations as they relate to the core competencies.

Chapter Five

Initial Recommendations and Implementation Plan

This chapter is intended to provide an initial roadmap for development of a conceptual framework for intelligence analyst core competencies. The analysis presented in Chapter 4 sought to identify specific core competencies that an intelligence analyst must possess to be effective across multiple components and organizations of DHS. It found that:

1) the intelligence analyst working within DHS and its components should have the *basic six Core Intelligence Analysis Competencies*: Analytical Writing, Communication, Critical Thinking and Reasoning Methods, Collaboration, Project Management, and Basic Technology.

These core competencies represent the minimum knowledge, skill, and abilities required of entry-level analysts regardless of their placement within IC elements or DHS components. Vacancy announcements and recruitment efforts may use the competencies to more accurately describe what is important to perform intelligence analysis. Similarly, the lack of competencies might generate calls for future educational and development programs and requirements.

2) in addition to the Core Intelligence Analysis Core Competencies, it is desirable for the intelligence analyst to have *Intelligence Fundamentals Skills* – this includes familiarity with national intelligence structures and policy, intelligence cycle, and intelligence writing and analytic tools.

3) despite recommendations provided in both the 2010 Common Competencies for State, Local, and Tribal Intelligence Analysts document by SLT Working Group and the 2015 Analyst Professional Development Road Map, there is no still no baseline standard of competencies that define the role and function of all entry-level intelligence analysts within DHS and its components. To this day, it remains fragmented and siloed, with each component providing only in-house specialized training that is relevant to their unique mission. Echoing the calls to action by both the academic works the research team reviewed and intelligence enterprise practitioners the team interviewed, our analysis demonstrates that being able to standardize this set of competencies is critical to the DHS's ability to provide and integrate timely intelligence and information, and not merely just a question of hiring and promoting potential job candidates.

In the following paragraphs, this project offers recommendations that reflect these findings, the existing guidance documents, current "best practices" by other IC elements as well as the scientific literature. They aim to provide an answer to the final question: How can these core competencies and findings be integrated into education and training effectively? It is important to highlight that these recommendations are meant to organize and standardize the existing efforts, establish streamlined competency taxonomies and measurable and meaningful competency-based performance factors against which all employees will be hired, promoted, and trained – all without calling for additional resources or organizational changes.

Recommendation 1: Develop a standardized Core Intelligence Analyst Competencies Matrix

There is an urgent need to understand what competencies are valued within DHS and its components, so that they can be further strengthened, sustained and drive all elements down the road to analytical success. If every intelligence analyst in the employment code has these basic competencies, components can focus on more specialized training in the future. The research team recommends that the Core Intelligence Analyst Competencies Matrix should:

- be developed based on the common analytical competencies already identified in the 2015 Road Map that set the minimum recommended qualifications and experience for each analytic proficiency (basic, intermediate and advanced) level.

- update the Road Map to explicitly include the six Core Intelligence competencies as well as the specific Intelligence Foundational Knowledge Skills defined in the analysis.

- include Standardized Learning Objectives. While competencies define the skills and knowledge necessary for every potential intelligence analyst to perform their job, learning objectives spell out what this project wants them to know. (See Appendix B)

- ensure the separation between the Core Intelligence Analyst Competency educational programs from the more specialized in-house training programs providing skills that are unique to individual components or government levels.

- be created, approved, and adopted by DHS, its leadership and training directorates/stakeholders, the Operational and Support components and other state, local and tribal agencies. Senior leadership should seek to tie the core competencies to the DHS overall intelligence analysis mission, communicate their commitment to individual components, and demonstrate support for the innovative thinking required for its success.

- serve as a standard scoring checklist for evaluating the proficiency of all candidates in a uniform manner, designing recruitment pipelines and interviewing guides, mapping career paths, and updating Learning Management educational programs.

- provide foundation for writing job descriptions and establish clear and predetermined criteria before job candidates' application materials are reviewed.

Outcome: Implementation of this recommendation demonstrates commitment to the overall standardization of the Core Intelligence Analyst Competencies but grows awareness of those competencies, and nurtures workforce talent – across DHS and its components. By demonstrating commitment and institutionalizing the minimum recommended analytic core competencies and proficiency levels internally, DHS can model the best practices and promote wider implementation across all levels of government. This in turn will create an environment favorable to the implementation and a more efficient and innovative intelligence analysis.

Metrics: Provide an annual report on the creation and dissemination of the Matrix, integration of the Matrix into hiring practices, educational and training programs and activities, and completion rates. Collect data based on position and associated Core Competency proficiency standards. Collect and analyze scorecards regarding how effectively entry-level Intelligence Analysts meet different Core Competency requirements and proficiency levels.

Recommendation 2: Integrate Core Intelligence Analyst Competencies Matrix into the DHS Performance and Learning Management System

The Core Intelligence Analyst Competencies Matrix should be integrated into the existing DHS Performance and Learning Management System in a way that would provide current employees and managers with an ability to:

- identify the courses and modules that impart Core Intelligence Analyst Competencies education;

- move from a lower level of proficiency to a higher one by enhancing their competencies;

- track their career progression and maintain a repository of transcripts;

- develop routine monitoring, receive performance feedback and incentives for analysts to maintain and enhance their Core Competencies.

- gain access to flexible, open, and distance-learning opportunities without having to leave their post.

Outcome: The intelligence analysis requires a progressive set of educational requirements through which individual analysts should move in a phased manner to both maintain and enhance their competencies. By integrating the Core Intelligence Analyst Competencies Matrix into the existing educational programs, the DHS should be able to match each Competency to a set of courses and modules, and approach career advancement in a more concerted manner. If a component has established curriculum that meets the Core Intelligence Analyst Competency Learning Objectives within their basic intelligence course, intelligence analysts would not need to travel to the main DHS Basic Intelligence and Threat Analysis Course (formerly BITAC) to become Intelligence Analyst Core Competency-Qualified (IACC-Q). Most importantly, this integration would allow DHS to identify and analyze competency gaps and deliver a mapping of internal resources and initiatives that can be used to address each gap and permit individual components and agencies to consider the specific competency proficiency needs of their organizations and tailor accordingly.

Metrics: Collect data on courses and modules that match individual Core Intelligence Analyst Competencies. Maintain transcripts, and track enrollments and rates of completion. Collect and analyze the intelligence analyst career lifecycle data, including but not limited to user records, enrollment and completion histories, individual development plans, course catalogs, and Competency requirements.

Recommendation 3: Engage with Intelligence Community Centers for Academic Excellence (IC CAE) programs and Department of Homeland Security Centers of Academic Excellence to meet both the hiring and educational needs.

By more actively engaging with the IC CAE and DHS CAE programs, DHS can create, attract, and support a professionally competitive and knowledgeable talent pool in multi-disciplinary areas. In order to achieve that, it is necessary to:

- identify the IC CAE programs that offer a more comprehensive curriculum that imparts core competencies and understanding of the IC mission and goals. The research team has compiled a detailed list of the existing programs that can be used to facilitate that process (See Appendix C).

- increase networking and engagement opportunities with both IC CAE and DHS CAE faculty directing and supervising research and teaching activities to provide feedback, guidance, offer advice and suggestions on how to modify coursework; spread awareness of the Core Intelligence Analyst Competencies, as well as the mission and workforce needs.

- organize academic fellowships/professional development for the IC CAE and DHS CAE faculty, provide internships for students, design speaker series and exclusive hiring and recruitment events for IC CAE Scholars.

- develop DHS intelligence analyst hiring pipeline and encourage the IC CAE and DHS CAE programs to refer their top candidates who have already acquired the necessary core competencies, and demonstrated academic, professional, and/or research strengths.

- utilize the Appendix B to recommend additional coursework, certification programs and degrees to those interested in pursuing intelligence analyst careers.

- utilize the Appendix B to supplement the courses offered in the Learning Management System and those offered in the onboarding process.

Outcome: By following this recommendation, DHS can build a talent pipeline and develop a proactive, procedural approach to identifying, qualifying, and nurturing potential candidates toward an eventual hire. Moreover, DHS can ensure that these candidates have mastered the core competencies prior to their hiring date, and that there are easily identifiable educational opportunities for the existing employees who need additional professional development and certification programs to acquire them. Finally, actively engaging with the faculty members of these Centers of Excellence would both stimulate and guide their teaching and research activities and provide opportunities to continually tailor and adjust the curriculum to meet the critical analytical needs.

Metrics: Provide an annual report that includes data on the number of hired IC CAE and DHS CAE Scholars; collect data on networking, speaking and other engagement events, completed internships, hiring and recruitment events.

Recommendation 4: Provide a mandatory Core Intelligence Analyst Competencies online course during the onboarding process.

This recommendation is not as rigorous nor does it guarantee that the newly hired intelligence analyst will reach mastery in any of the competencies, but it will give them all an opportunity to receive at least a basic introduction in a shorter amount of time before entering the DHS workforce as part of the onboarding process. The key to any hiring process is the effective onboarding process that ensures integration of the new intelligence analysts into their new organizations and roles in a standardized manner. This process should:

- focus on updating, expanding and integrating the curriculum offered by DHS Intelligence Academy, DHS Basic Intelligence and Threats Analysis Course (BITAC) and Foundations of Intelligence Analysis (FIAT) to include the online Core Intelligence Analyst Competencies training.

- start as soon as the candidate has accepted the position and should continue into their first 60-90 days of employment.

- include follow-up activities, continuous learning and competency development opportunities.

- be used to match and assign mentor to the newly hired intelligence analysts

- bridge the divide between federal, state, local, and tribal authorities, as well as among different components, as it sets the tone for greater standardization.

Outcome: By building a detailed and uniform onboarding online course, DHS can ensure that all newly hired intelligence analysts are provided the same information. This process would also allow the hiring managers to receive reports on their intelligence analysts' general preparation, proficiency levels, and accomplishments in relation to the onboarding, saving them time and making the onboarding process more flexible.

Metrics: Electronically document performance scorecards and transcripts and run reports after the online course completion has been recorded. Maintain employee online course records for five years.

Recommendation 5: Improve retention and merit-based advancements through educational opportunities.

Conducting innovative intelligence analysis can only be accomplished by empowering, developing, and engaging talent and by maintaining strong succession and promotion plans. To improve retention and merit-based advancement of intelligence analysts through education, there is a need to:

- create and facilitate career mentoring and coaching programs that allow intelligence analysts to move up the proficiency ladder, meet their professional goals and move into supervisory positions.
- provide access to and share advertising of additional educational opportunities for professional development, career advancement and self-nomination opportunities in ways that reach more employees across all DHS components.
- review the structure of career advancement programs to ensure recognition of those who successfully complete Core Competency educational programs.
- recognize accomplishments that are less visible or incentivize specific Core Competency educational opportunities that improve the overall analysis at DHS and its components.
- conduct climate assessment interviews and focus groups to uncover the behaviors and cultural norms within DHS that help and hinder educational efforts to retain and advance intelligence analysts who can innovate and lead change.

Outcome: Through the implementation of mentoring and information sharing programs, DHS ensures the visibility of the Core Intelligence Analyst Competencies Matrix internally and externally. In addition, by integrating the Core Intelligence Analyst Competencies Matrix into career advancement structures, it will promote standardization of knowledge and understanding of the cultural and organizational context for all intelligence analysts to operate effectively.

Metrics: Collect and maintain data about DHS intelligence analysts as they relate to their participation in mentoring and coaching programs. Collect and analyze career advancement programs structures data to ensure they integrate Core Competencies.

Chapter Six

Conclusion and Follow-on Research

The scope of this report was limited to developing an overview of the current trends and challenges in intelligence analysis education and trading, identifying, and analyzing existing gaps, particularly as they pertain to DHS, and mapping out core competencies necessary to operate efficiently and effectively in a complex and unpredictable security environment.

In order to accomplish that, Chapter Two reviewed the calls from the scholarly and practitioner communities to develop a conceptual framework on intelligence education and training and standardize the way ahead for the next generation of intelligence analysts. It also identified and examined the existing training programs within the IC, as well as a number of internal plans and strategies to improve them. This chapter highlighted that unlike academic programs where there has been a much greater standardization of intelligence programs and courses, despite the calls and guidance documents, there are serious gaps in the way different IC elements prioritize and think of core competencies. More broadly, it demonstrates that there is an urgent need to ensure standardization across the IC with core competencies. Without this standardization, intelligence analysts are without a common set of skills, creating challenges and difficulties in doing their job, collaboration, and delivery of intelligence products.

Chapter Three discusses the steps that were taken to identify and measure critical core competencies intelligence analysts should possess to be effective across multiple components and organizations of DHS. More specifically, it describes the multi-method approach the research team adopted to collect and analyze data, and provides a rationale for the use of ethnographic interviews and domain analysis to ensure the overall validity and reliability of the findings. In addition, it discusses some of the limitations associated with the timing of this study during the 2020 COVID-19 pandemic and new administration transfer of power, as well as the constraints of availability and willingness to participate by the IC professionals.

In Chapter Four, the research team found that there were a variety of training challenges with DHS training and education efforts that match Chapter Two findings. Overall, there were seven challenges found during the interviewing and domain analysis: core competencies, specialized training, balancing demand with operations, communication and expectations, training delivery, challenges in developing joint curriculum and training for the intelligence community and law enforcement, and identity. The team briefly reviews each challenge by presenting the Atlas.ti visual mapping and domain association but specifically focuses on the core competency code trees to understand whether the members of IC share the same understanding of analytic, writing, and critical thinking skills, collaboration, and project management. Moreover, this chapter was able to identify how the interviewees prioritize and identify specific challenges within DHS, including training constrained by work duties, and technology and accessibility concerns,

Chapter Five summarizes our findings and offers five specific recommendations that should be considered by the leadership within the DHS, its components, regional Fusion Centers and law enforcement when introducing initiatives to improve and standardize intelligence analysis education and training. It posits that the only way to develop a more talented, trained, and tailored workforce can be achieved by creating a Core Intelligence Analyst Competency Matrix that includes the basic six competencies - Analytical Writing, Communication, Critical

Thinking and Reasoning Methods, Collaboration, Project Management, and Basic Technology – along with Intelligence Fundamentals Skills and minimum proficiency levels. This also requires determining desired standard learning outcomes for each of those competencies. Having a shared understanding of the competencies needed for prospective intelligence analysts will also strengthen the ability to directly engage and collaborate with the IC CAE and DHS CAE programs across the country to create a steady workforce pipeline. Next, by offering more flexible, standardized, and comprehensive online course to all intelligence analysts, the DHS leadership can more effectively standardize the onboarding process and close the gap between federal, state, local, and tribal authorities. Lastly, it recommends establishing a competency-based recruitment strategy, linking the specific minimum core competencies and proficiency levels to intelligence analyst vacancy announcements, and using the same to measure and assess professional development, and track individual development plans and career path.

Year Two Research

In the effort to provide consistent and rigorous standards for DHS intelligence training and education, this study also notes considerations for future research. One of the principal strategic priorities discussed in this report were gaps in intelligence analysis as it pertains to the DHS's counterterrorism workforce. In order for that workforce to remain innovative and flexible, our analysis demonstrated that it ought to be capable of rapidly adopting innovative technologies wherever they may arise. In fact, employing cyber and analytic networks for counterterrorism detection, protection, and surveillance was identified as crucial to maximizing operational efficiency for DHS. There is no doubt that the emerging technologies are increasingly challenging our policymaking, democratic systems of political responsibility and accountability, and uprooting traditional ways we analyze intelligence, prevent attacks, and protect the homeland and its interests. That is why the follow-up report will seek to study the impact of technology across the IC, including strategies, methods, and sources utilized for mission success, and examine the following questions:

- How can the U.S. Intelligence Community receive consistent, updated, and relevant technology training to prevent terrorism?
- What are the best technologies for developing the workforce in counterterrorism and targeted violence?
- What technologies in the commercial sector could assist and contribute toward DHS workforce and professional development?

In addition to continuing to expand upon the previous year's research, these directly relate to Counterterrorism and Targeted Violence Workforce Development questions:

- What are the most up-to-date technologies that DHS can provide to its counterterrorism workforce?
- What counterterrorism training is needed for Federal and SLTT law enforcement partners to ensure HSE has the most up-to-date training on terrorism and targeted violence?

Therefore, this project will explore concrete focus on collecting, analyzing, assessing, and implementing technological training and education standards for the intelligence community charged with protecting the homeland against terrorist threats and operations. It will proceed in a phased manner and seek to achieve the following steps:
1. Collect data on current training and educational requirements across not only the IC but also tech-savvy companies within the private sector in order to identify, compare, and contrast the key technologies required to enhance the U.S. homeland security posture.
2. Analyze the levels of technological proficiency and skills related to new and emerging technologies needed to be highly trained in security infrastructure, information systems, and counterterrorism cybersecurity.
3. Analyze and assess current DHS technology training and educational requirements, and resources to provide that training and develop a strong STEM workforce.
4. Provide recommendations that will lead to the development of an effective and efficient workforce in intelligence for defending the homeland against terrorism.

The ultimate purpose of the follow-on research is to provide an accurate assessment of the workforce's current training and education to utilize technology, operate in the cyber domain, and to protect critical services and infrastructure from potentially disastrous cyber events perpetrated by terrorists. This project would align with the DHS Office of Intelligence and Analysis, Mission Centers (CT, Cyber, and Counterintelligence), and the Fusion Centers as they seek to understand what is missing from current workforce development, identify the requirements and gaps, and build an implementation plan to ensure efficient and practical training for the current and next-generation analyst.

Further research for DHS Workforce Development, Training and Education – Theme Four

Finally, this research report provided a baseline of findings on the current status of the intelligence field in terms of training and education for the workforce. The research team recommends that additional research should be done to enhance the intelligence field, especially with DHS and its training challenges. Specifically, research addressing the challenges outlined in Chapter Four would significantly assist DHS and their workforce development efforts. Below are proposed research topics that could assist in addressing current challenges and building a more efficient and effective intelligence workforce.

Proposed Follow-on Research for Training and Education	
Future research on Challenge areas	**Suggested Questions and Topics**
SPECIALIZED TRAINING	1. Identify specialized training needs for an analyst in vital mission areas across the enterprise (such as forensics and counterterrorism) and identify their learning objectives. 2. Identify some constraints in attendance and creating in-house training versus outsourced training. 3. Identify whether some courses could be consolidated or used to count towards the same course in another component/organization.

BALANCING DEMANDS	1. Identify priorities across the DHS enterprise and their method of selecting analysts for training. 2. Identify constraints in resources and the shortfall needed to fulfill training requirements. 3. Identify organizational best practices to balance training and operational demands (do certain components and organizations have a system already in place that seems to work?)
TRAINING DELIVERY	1. Identify the entire DHS catalog of training and its delivery methods to all components and organizations of DHS, including state, local, and tribal law enforcement. 2. Identify the benefits and constraints of using in-person, online, or blended learning courses for analysts. 3. Identify the impact of training since COVID-19 and its impact to DHS mission sets.
COMMUNICATION AND EXPECTATIONS	1. Identify how DHS communicates and advertises all training, core and specialized, across the DHS enterprise. 2. Identify how expectations and skill requirements are set for each agency. 3. Identify issues between agencies on working together regarding communicating these courses.
JOINT CURRICULUM	1. Identify the specific challenges in developing joint curriculum and training for the intelligence community and law enforcement. 2. How agencies and organizations currently translate different courses between Title 50 vs Title 18 3. Identify the specific challenges in information sharing between Title 50 vs Title 18
IDENTITY	1. Further investigate the challenge of DHS's collective identity due to Title 50 and Title 18 training requirements. 2. Research and understand the differences between State vs Local mindset – across the U.S. 3. Identify which state and local law enforcement agencies hire intelligence analysts and understand if that has improved their policing methods for DHS mission areas (counterterrorism).

Appendix A
Intelligence Community Competencies

Core Intelligence Analyst Competencies

Agency:	Core Competencies	Definitions
Customs and Border Patrol (CBP)	Collaboration	Improved collaboration throughout CBP and with our stakeholders provides shared sense of purpose.
	Innovation	CBP must remain vigilant through innovative initiatives to continually advance and transform the agency into an agile and adaptable organization.
	Integration	CBP must lead development of a seamless global network to integrate border enforcement capabilities and meet the demands of a constantly evolving landscape.
	Resource Management	This strategic resource management framework ensures the Commissioner's vision, goals, and objectives are clearly articulated; programs and activities are aligned to the goals and objectives; resources are appropriately allocated to achieve the desired goals and objectives; and a performance measurement and program evaluation capability enables the assessment of progress made in executing the DHS and CBP mission and operational priorities.
	Risk Management	Anticipate and proactive reaction to strategic risks that impact mission accomplishment
Defense Intelligence Agency (DIA)	Critical Thinking	Uses logic, analysis, synthesis, creativity, judgement, and systemic approaches to gather, evaluate, and use multiple sources of information to inform decisions and outcomes
	Communication	Effectively comprehends and conveys information with and from others in writing, reading, listening, and verbal

		and non-verbal action. Uses a variety of media in communication and making presentations appropriate to the audience
	Accountability for results	Takes responsibility for one's work, sets and/or meets priorities, organizes and utilizes resources efficiently and effectively to achieve desired results, consistent with organizational goals and objectives.
	Engagement and Collaboration	Recognizes, values, builds, and leverages collaborative and constructive networks of diverse coworkers, peers, customers, stakeholders, and teams within an organization and/or access the IC to share knowledge and achieve results
	Personal Leadership and Integrity	Demonstrates personal initiative, honesty, openness, and respect in their dealings with coworkers, peers, customers, stakeholders, teams, and collaborative networks across the IC
Defense Intelligence Agency: Specialty Competencies	GMA Regional Analysis	Research, review, evaluate, interpret, and analyze all source intelligence data on a specific region, country and the immediate environment or transnational topic in order to assess and identify vulnerabilities, opportunities, threats and targets and to develop warning.
	GMA Functional Analysis	Research, review, evaluate, interpret, and analyze all source intelligence data on specific processes and technology for a country, region, or worldwide topic in order to assess and identify vulnerabilities opportunities, threats and targets and to develop warning
	SEA—S&TI Analysis	Applies scientific or engineering skills as well as intelligence analysis skills to research, review, evaluate, interpret, and analyze all source intelligence data on a specific region, country and the immediate environment or

		transnational topic in order to assess and identify vulnerabilities, opportunities, threats, and to develop warning.
Department of Homeland Security (DHS)	Achieving Results (Performance Goals)	
	Technical Proficiency	
	Customer Service (Exceptions for positions (1811 and 1896)	
	Teamwork/Cooperation	
	Communications	
	Representing the Agency	
	Assigning, monitoring, and evaluating work (Supervisors and Managers)	
	Leadership (Supervisors and Managers)	
Department of Defense (DoD)	Interpersonal skills	Develops and maintains effective working relationships, especially in difficult situations. Engages and inspires others. Treats others with courtesy, sensitivity, and respect. Considers and responds appropriately to the needs and feelings of different audiences, situations, and/or cultures. Actively solicits feedback. Exemplifies professionalism, tact, and empathy. Builds trust and commitment.
	Integrity/honesty	Nurtures ethically minded organizations through personal discipline, values, self-control, and policies that reinforce ethical behavior. Demonstrates selflessness of action by doing the right thing regardless of personal and professional consequences. Behaves in an honest,

		fair, and ethical manner without regard to pressure from other authorities. Shows consistency in words and actions. Instills trust and confidence; models high standards of ethics.
	Written communication	Writes to convey information in a clear, concise, organized, and convincing manner for the intended audience using correct English grammar, punctuation, and spelling. Expresses thoughts persuasively and uses effective modes to reinforce message retention.
	- Oral communication	Demonstrates ability to clearly and effectively articulate, present, and promote varied ideas and issues (to include sensitive or controversial topics) before a wide range of audiences. Makes clear and convincing oral presentations. Listens effectively; clarifies information as needed.
	Continual learning	Assesses and recognizes own strengths and weaknesses; pursues self-development. Uses challenges as opportunities to improve and become more effective. Pursues chances to stretch skills to further professional growth. Seeks ways to improve the capacity of others and the organization through knowledge sharing, mentoring, and coaching.
	Public service motivation	Shows a commitment to serve the public. Ensures that actions meet public needs; aligns organizational objectives and practices with public interests.
Federal Bureau of Investigation (FBI)	Collaboration	Establish contacts and interact effectively with external agencies, government officials, the community and internal Bureau contacts; display professionalism while working with others to achieve common goals; and to proactively share information with others when appropriate.

	Communication	Express thoughts and ideas clearly, concisely, persuasively and effectively both orally and in writing; interpret and understand verbal or written communications; tailor the communication to the experience, exposure or expertise of the recipient; and proactively share information with others when appropriate.
	Flexibility and Adaptability	Change is inevitable. To succeed in an unpredictable law enforcement environment, you must be able to adapt to rapidly changing circumstances and quickly respond to urgent needs. Cultivating the quality of adaptability can make you more effective and help mitigate stress.
	Initiative	Willingness to begin projects/work or to address issues; be proactive and creatively respond to problems/issues/tasks.
	Interpersonal Ability	Ability to deal effectively with others; establish and maintain rapport with management, colleagues and subordinates; recognize and show sensitivity to differences in the needs and concerns of others; and mediate concerns between individuals and groups, as well as settle disputes.
	Leadership	Motivate and inspire others; develop and mentor others; gain the respect, confidence and loyalty of others; and articulate a vision, give guidance and direct others in accomplishing goals.
	Organizing and Planning	Establish priorities, timetables and goals/objectives; structure a plan of action for self and others; and develop both strategic and tactical plans.
	Problem solving and Judgement.	Critically evaluate conditions, events and alternatives; identify problems, causes and relationships; base decisions or recommendations on data or sound

		reasoning; and formulate objective opinions.

Note. The data for CBP is from *Customs and Border Patrol Vision and Strategy 2020* (pp. 32-42), by Customs and Border Patrol, 2015, (https://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf). The data for DIA and DIA: Specialty Training are from *DIA Analyst training requirements and Competencies* (pg. 7-8)., by Defense Intelligence Agency, 2008, (http://scripts.cac.psu.edu/users/t/s/tsb4/GEOINT/DIA_Analyst_Competencies.pdf). The data for DHS is from *Performance Management MD #3181 (*pg. 11), by Department of Homeland Security, 2006, (https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_3181__performance_management.pdf). The data from DoD is from *Growing Civilian Leaders*, (pg. 24), by Department of Defense, 2009, (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/143016p.pdf).

Core Competencies Identified in Guidance Documents

Document	**Core Competencies**	**Definition**
Intelligence Community Directive (ICD) 203 [Analytic Standards]	Properly describes quality and credibility of underlying sources, data, and methodologies	Analytic products should identity underlying sources and methodologies upon which judgments are based, and use source descriptors in accordance with lCD 206, Sourcing Requirements/or Disseminated Analytic Products, to describe factors affecting source quality and credibility. Such factors can include accuracy and completeness, possible denial and deception, age and continued currency of information, and technical elements of collection as well as source access, validation, motivation, possible bias, or expertise. Source summary 2 lCD 203 statements, described in lCD 206, are strongly encouraged and should be used to provide a holistic assessment of the strengths or weaknesses in the source base and explain which sources are most important to key analytic judgments.
	Properly expresses and explains uncertainties associated with major analytic judgments	Analytic products should indicate and explain the basis for the uncertainties associated with major analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a full spectrum from

		remote to nearly certain. Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic. Analytic products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). As appropriate, products should identify indicators that would alter the levels of uncertainty for major analytic judgments. Consistency in the terms used and the supporting information and logic advanced is critical to success in expressing uncertainty, regardless of whether likelihood or confidence expressions are used.
	Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments	Analytic products should clearly distinguish statements that convey underlying intelligence information used in analysis from statements that convey assumptions or judgments. Assumptions are defined as suppositions used to frame or support an argument; assumptions affect analytic interpretation of underlying intelligence information. Judgments are defined as conclusions based on underlying intelligence information, analysis, and assumptions. Products should state assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps. Products should explain the implications for judgments if assumptions prove to be incorrect. Products also should, as appropriate, identify indicators that, if detected, would alter judgments.
	Incorporates analysis of alternatives	Analysis of alternatives is the systematic evaluation of differing hypotheses to explain events or phenomena, explore near-term outcomes, and imagine possible futures to mitigate surprise and risk. Analytic products should identify and assess plausible

		alternative hypotheses. This is particularly important when major judgments must contend with significant uncertainties, or complexity (e.g., forecasting future trends), or when low probability events could produce high-impact results. In discussing alternatives, products should address factors such as associated assumptions, likelihood, or implications related to U.S. interests. Products also should identity indicators that, if detected, would affect the likelihood of identified alternatives.
	Demonstrates customer relevance and addresses implications	Analytic products should provide information and insight on issues relevant to the customers of U.S. intelligence and address the implications of the information and analysis they provide. Products should add value by addressing prospects, context, threats, or factors affecting opportunities for action.
	Uses clear and logical argumentation	Analytic products should present a clear main analytic message up front. Products containing multiple judgments should have a main analytic message that is drawn collectively from those judgments. All analytic judgments should be effectively supported by relevant intelligence information and coherent reasoning. Language and syntax should convey meaning unambiguously. Products should be internally consistent and acknowledge significant supporting and contrary information affecting judgments.
	Explains change to or consistency of analytic judgments	Analytic products should state how their major judgments on a topic are consistent with or represent a change from those in previously published analysis or represent initial coverage of a topic. Products need not be lengthy or detailed in explaining change or consistency. They should avoid using boilerplate language, however, and should make clear how new information or different reasoning led to the judgments expressed in them. Recurrent products such as daily crisis reports should note any changes in judgments;

		absent changes, recurrent products need not confirm consistency with previous editions. Significant differences in analytic judgment, such as between two IC analytic elements, should be fully considered and brought to the attention of customers.
	Makes accurate judgments and assessments	Analytic products should apply expertise and logic to make the most accurate judgments and assessments possible, based on the information available and known information gaps. In doing so, analytic products should present all judgments that would be useful to customers, and should not avoid difficult judgments in order to minimize the risk of being wrong. Inherent to the concept of accuracy is that the analytic message a customer receives should be the one the analyst intended to send. Therefore, analytic products should express judgments as clearly and precisely as possible, reducing ambiguity by addressing the likelihood, timing, and nature of the outcome or development. Clarity of meaning permits assessment for accuracy when all necessary information is available.
	Incorporates effective visual information where appropriate	Analytic products should incorporate visual information to clarify an analytic message and to complement or enhance the presentation of data and analysis. In particular, visual presentations should be used when information or concepts (e.g., spatial or temporal relationships) can be conveyed better in graphic form (e.g., tables, flow charts, images) than in written text. Visual inforn1ation may range from plain presentation of intelligence information to interactive displays for complex information and analytic concepts. All of the content in an analytic product may be presented visually. Visual information should always be clear and pertinent to the product's subject. Analytic content in visual information should also adhere to other analytic tradecraft standards.

Intelligence Community Directive (ICD) 610-3 and 610-4 [Supervisory/Non-supervisory and Managerial IC Employees at GS-15 and Below]	Engagement and Collaboration	IC employees are expected to use logic, analysis, synthesis, creativity, judgment, and systematic approaches to gather, evaluate, and use multiple sources of information to effectively inform decisions and outcomes. In addition, IC supervisors are expected to establish a work environment where employees feel free to engage in open, candid exchanges of information and diverse points of view.
	Critical Thinking	IC employees are expected to use logic, analysis, synthesis, creativity, judgment, and systematic approaches to gather, evaluate, and use multiple sources of information to effectively inform decisions and outcomes. In addition, IC supervisors are expected to establish a work environment where employees feel free to engage in open, candid exchanges of information and diverse points of view.
	Leadership and Integrity	IC supervisors and managers are expected to exhibit the same individual · personal leadership behaviors as all IC employees. ln their supervisory or managerial role, they also are expected to achieve organizational goals and objectives by creating shared vision and mission within their organization; establishing a work environment that promotes equal opportunity, diversity (of both persons and points of view), critical thinking, collaboration, and information sharing; mobilizing employees, stakeholders, and networks in support of their objectives; and recognizing and rewarding individual and team excellence, enterprise focus, innovation, and collaboration.
	Accountability for Results	IC employees are expected to take responsibility for their work, setting and/or meeting priorities, and organizing and utilizing time and resources efficiently and effectively to achieve the desired results, consistent with their organization's goals and objectives. In addition, IC Supervisors are

		expected to use these same skills to accept responsibility for and achieve results through the actions and contributions of their subordinates and their organization as a whole.
	Management Proficiency	IC supervisors and managers are expected to possess the technical proficiency in their mission area appropriate to their role as supervisor or manager. They are also expected to leverage that proficiency to plan for, acquire, organize, integrate, develop, and prioritize human, financial, material, information, and other resources to accomplish their organization's mission and objectives. In so doing, all supervisors and managers are also expected to focus on the development and Productivity of their subordinates by setting clear performance expectations, providing ongoing coaching and feedback, evaluating the contributions of individual employees to organizational results, and linking performance ratings and rewards to the accomplishment of those results.
	Communication	IC employees are expected to effectively comprehend and convey information with and from others in writing, reading, listening, and verbal and non-verbal action. Employees are also expected to use a variety of media in communication and making presentations appropriate to the audience. In addition, IC supervisors are expected to use effective communication skills to build cohesive work teams, develop individual skills, and improve performance.
	Technical expertise	IC employees are expected to acquire and apply knowledge, subject matter expertise, tradecraft, and/or technical competency necessary to achieve results.
	Personal Leadership and Integrity	IC employees are expected to demonstrate personal initiative and innovation, as well as integrity, honesty, openness, and respect for diversity in their dealings with coworkers, peers, customers, stakeholders, teams, and

		collaborative networks across the IC. IC employees are also expected to demonstrate core organizational and IC values, including selfless service, a commitment to excellence, the courage and conviction to express their professional views and constructively address or seek assistance to properly address concerns related to the protection of classified information in accordance with EO 13526, Classified National Security Information.
Intelligence Community Directive (ICD) 656 [Performance Management System Requirements for Intelligence Community Senior Civilian Officers]	Collaboration and Integration	IC senior officers are expected to responsibly and proactively provide, discover, and request information and knowledge to achieve results, and are expected to build effective networks and alliances with key peers and stakeholders across the IC, and with other US Government (USG), state, local, tribal and foreign officials, as appropriate. They should actively engage these peers and stakeholders, involve them in key decisions, and effectively leverage networks and alliances to achieve significant results. In addition, senior officers are expected to create an environment that promotes employee engagement, collaboration, integration, responsible information and knowledge sharing, and the candid, open exchange of diverse points of view. This includes ensuring compliance with EO 13526 regarding the proper handling of classified information.
	Enterprise Focus	IC senior officers are expected to demonstrate a deep understanding of how the missions, structures, leaders, and cultures of the various IC components interact and connect. They should synthesize resources, information, and other inputs to effectively integrate and align component, IC, and USG interests and activities to achieve IC-wide, national, or international priorities. In addition, senior officers are expected to encourage and support joint duty assignments and developmental experiences that develop and reinforce an enterprise focus among their subordinates.

	Values-Centered Leadership	IC senior officers are expected to personally embody, advance and reinforce IC core values which include: a Commitment to selfless service and excellence in support of the IC's mission, as well as to preserving, protecting, and defending the Nation's laws and liberties; the integrity and Courage (moral, intellectual, and physical) to seek and speak the truth, to innovate, and to change things for the better, regardless of personal or professional risk; and to encourage Collaboration as members of a single IC-wide team, respecting and leveraging the diversity of all members of the IC, their background, their sources and methods, and their points of view. In addition, senior civilian officers are also expected to demonstrate and promote departmental and component core values, which may be incorporated in writing, as applicable.
	Domain Knowledge	IC senior officers are expected to acquire and maintain a deep knowledge and understanding of their leadership and management "domain," that is, the institutional, organizational, functional, and technical context in which they operate, or demonstrate the capacity to quickly acquire such knowledge. They are also expected to strategically and systematically leverage that knowledge and understanding to plan, develop, direct, and integrate employees and programs in order to achieve organizational results.
	Executive Leadership	IC senior officers are expected to articulate and achieve organizational vision, demonstrate adaptability and flexibility in leading organizational change, and to engage and motivate employees, peers and stakeholders. They must exhibit political savvy and create a workplace that promotes and reflects diversity (of both persons and points of view) and equal opportunity; encourage innovation and critical thinking; and maintain organizational and personal focus, intensity, and persistence, even under

		adversity. Those IC senior officers with duties that are primarily technical in nature (for example, ST or DISL employees) are expected to adapt and apply these same competencies in dealing with professional colleagues and peers in their technical field or professional discipline, as well as organizational customers or clients.
	Management Tradecraft	IC senior officers are expected to acquire, plan, organize, develop, integrate and prioritize the human, financial, material, and information (including classified) resources to effectively accomplish their organization's mission, strategic goals, and performance objectives. Senior officers are also expected to make sound and timely decisions, set clear employee performance expectations, give employees constructive coaching and feedback, and provide appropriate developmental opportunities. They must make meaningful distinctions between the performance of subordinates, and rigorously and realistically evaluate the contributions of individual employees to organizational results. Those IC senior officers with duties that are primarily technical in nature (for example, ST or DISL employees) are expected to adapt and apply these same competencies to the oversight, coordination, and technical management of research, programs, or projects in their particular technical field or professional discipline.
National Prevention Framework	Intelligence and information sharing	Identify, develop, and provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber-threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, and

		Federal governments and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate
	Screening, search, and detection	Identify, discover, or locate terrorist threats through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, biosurveillance, sensor technologies, or physical investigation and intelligence
	Interdiction and disruption	Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards
	Forensics and attribution	Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source(s), to include forensic analysis as well as attribution for an attack and for the preparation for an attack in an effort to prevent initial or follow-on acts and/or swiftly develop counter-options
	Planning	Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives
	Public information and warning	Deliver coordinated, prompt, reliable, and actionable terrorism-related information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat and the actions being taken and the assistance being made available, as appropriate
	Operational coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities

Note. The data from ICD 203 is from *Intelligence Community Directive Number 203: Analytic Standards,* (pg. 2-4), by the Office of the Director of National Intelligence, (2015), (https://fas.org/irp/dni/icd/icd-203.pdf). The data from ICD 610-3 is from *Core competencies for* *non-supervisory intelligence community employees at GS-15 and below,* (pg. 2-5), by the Office of the Director of National Intelligence, (2010), (https://fas.org/irp/dni/icd/ics-610-3.pdf). The data for ICD 610-4 is from *Intelligence community standard number 610-4: Core competencies for supervisory and managerial intelligence community employees at GS-15 and below,* (pg. 2-4), by the Office of the Director of National Intelligence, (2010), (https://fas.org/irp/dni/icd/ics-610-4.pdf). The data from ICD 656 is from *Intelligence community directive number 656: Performance management system requirements for intelligence community senior civilian officers,* (pg. 8-9), by the Office of the Director of National Intelligence, (2012), (https://www.dni.gov/files/documents/ICD/ICD_656.pdf). The data from the National Prevention Framework is from *National Prevention Framework,* (pg. 10-17), by the Department of Homeland Security, (2016), (https://www.hsdl.org/?abstract&did=793534).

Appendix B

Proposed Core Intelligence Analyst Competencies Matrix

Standardized Learning Objectives

Analytical Writing

1. Write correctly and with proper sentence structure
2. Address the "why", "how" and "so what" questions.
3. Tailor one's written message for different audiences/intelligence consumers
4. Able to utilize various analytic techniques within the analytic process
5. Effectively integrate multiple sources while constructing well-supported arguments and sustaining a focused and coherent discussion.
6. Convey in writing the connection/relationship of ideas to other strains of social, economic and political thought

Critical Thinking and Reasoning Methods

1. Process abstract and complex ideas, and analyze issues from many different perspectives and within their historical, socio-economic and political context
2. Able to generate and test hypothesis and conduct research utilizing a variety of sources.
3. Recognize and mitigate their own biases to make sound conclusions based on carefully gathered evidence.
4. Focus analysis efforts to meet the intelligence consumer's decision-making needs.
5. Understand underlying assumptions, connect ideas to one another and evaluate ideas and their merits.
6. Make judgments based on research, analysis of data and empirical evidence.
7. Accurately identify and evaluate records of past events, ideas, and facts, and integrate interdisciplinary and inter-cultural perspectives.

Communication

1. Deliver information and ideas orally in a variety of activities, from informal discussion to formal briefings.
2. Ability to communicate constructive challenges/new ideas, and condense and present complex information accurately, concisely, clearly and quickly to all levels in the organization.
3. Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.

Collaboration

1. Ability to collaborate and effectively engage with team members across the components and government levels to complement and support the analysis.
2. Ability to encourage and enable people to work together as a team to accomplish the project.
3. Provide and receive feedback from managers and team members in order to perform the task.
4. Foster engagement by listening and acknowledging the work, opinions, ideas and concerns of others.
5. Ability to assist others in solving intelligence problems and share information among internal and external partners.
6. Must display a high degree of integrity, commitment to the mission and professional judgment.

Project Management

1. Ability to provide direction and manage analytic projects.
2. Ability to make timely decisions, manage teams and delegate responsibilities to the team members.
3. Ability to prioritize and handle multiple projects simultaneously in an organized manner.
4. Ability to maintain composure under pressure and in face of discouraging developments while keeping the project moving toward successful completion.
5. Ability to mentor new analysts on the analytic process and agency policies and procedures

Technology

1. Ability to use computerized data visualization and intelligence analysis tools.
2. Able to use a personal computer and its applications.
3. Ability to use assistive software to interpret data, draw meaning from qualitative and quantitative data.
4. Ability to think critically about the use and integration of AI and machine learning into the processes and methods of scientific inquiry involving experimentation, observation, and quantitative analysis.

Appendix C
ICCAE and COE Program Competencies

School	Program	Undergraduate	Graduate	Credit Hours	Core Competencies
University of Arizona	ICCAE	Intelligence and Information Operations Curriculum includes three tracks: Operational Intelligence Information Warfare Law Enforcement Intelligence	N/A	120 Credits	Analytical Thinking
Florida International University	ICCAE	Certificate In National Security Studies	N/A	18 Credits	Analytic Writing Communications
Rutgers, the State University of New Jersey	ICCAE	Minor in Critical Intelligence Studies	N/A	18 Credits	Critical Thinking Analytical Writing
University of Alabama (Consortium with Alabama A&M University and Tuskegee University	ICCAE	Critical Technologies ICCAE Scholar Program	Critical Technologies ICCAE Scholar Program	N/A	Writing/Briefing
University of North Carolina in Charlotte (Consortium with Duke University, North Carolina Central University, North Carolina State University, North Carolina Chapel Hill)	ICCAE	Major: Peace, War, and Defenses Concentration: Intelligence and International Security Certificate: Security Studies Certificate: Geospatial Intelligence	Master: of International Studies (optional Intelligence Focus) Certificate: Security Studies Certificate: Geospatial Intelligence	Varies	Writing Critical Thinking
University of New Mexico	ICCAE	National Security Studies Program:	N/A	Bachelor in Integrative Studies: 36	Critical Thinking Writing

		Concentration in Global and National Security Studies Certificate in National Security and Strategic Analysis Critical Technology Studies Program Bachelor in Integrative Studies and Innovation: Global and National Security		credits of residency earned as a BISI major; 45 credits of upper-level coursework	
University of Oklahoma-Norman	ICCAE	Certificate in Intelligence Studies	Certificate in Intelligence Studies	9 Credits	Writing/Briefing Communication Critical Thinking
University of Texas at San Antonio	ICCAE	N/A	MS Data Analytics (Critical Technology Studies) Graduate Certificate in Intelligence Studies	M.S.: 33 Credit Hours Certificate: 12 Hours	Writing/Briefing
Virginia Polytechnic Institute & State University	ICCAE	ICCAE Scholar HUME ICCAE Research Fellowship	ICCAE Scholar HUME ICCAE Research Fellowship	Varies	Critical Thinking Communication
California State University - Fullerton	ICCAE Legacy	ICCAE Scholars	ICCAE Scholars	18 Credits	Writing Critical Thinking
University of Mississippi	ICCAE Legacy	Minor in Intelligence and Security Studies Minor in Global Security Studies	N/A	18 Credits	Critical Thinking Writing/Briefing

University of Nebraska - Lincoln	ICCAE Legacy	National Security Studies Minor IC Scholars Deterrence and Assurance Academic Alliance	N/A	21 Credits	Critical Thinking Writing/Briefing

University of Nebraska at Omaha	ICCAE Legacy and DHS COE (NCITE)	IC Scholars;
		Deterrence and Assurance Academic Alliance;
		CBA Business Analytics
			Political Science - Intelligence and National Security Certificate	15 Credits	Writing
					Communication/Briefing
					Critical Thinking
					Project Management
					Collaboration
					Technology

University of South Florida	ICCAE Legacy	Intelligence Studies Minor BS in Information Science with Intelligence Analysis Concentration	MSIS, Strategic Intelligence MS Intelligence Studies with a Strategic Intelligence Concentration MSIS, Cyber Intelligence MS, Cybersecurity Certificate in Strategic Intelligence Certificate in Cyber Intelligence	B.S., with Intelligence Analysis Concentration is 120 Credits Concentration is 21 credits Intelligence Studies Minor is 12 credits MS is 36 credits	Writing/Briefing
Arizona State University Center for Accelerating Operational Efficiency (CAOE)	DHS COE	B.S. in Aeronautical Management and Technology, Innovation and Society, Public Service and Public Policy Concentration in Emergency Management	M.S. in Robotics and Autonomous Systems, Program Evaluation and Data Analytics, Emergency Management and Homeland Security; Certificate in	B.S. degrees 120 credit hours; M.S. degrees are 32 credit hours; Certificates 15-16 credit hours	Critical Thinking

		and Homeland Security	Homeland Security		
University of Houston Borders, Trade, and Immigration Institute (BTI)	DHS COE	BS Degree in Border Operations Management, Trade, and Transport Security currently in development w/ 3 concentrations: Trade and transport, Migration, and Technology Developing minors in Border Operations Management Cross-Border Trade and Transport Security	MS Degree in Border Management, Trade and Transport Security also in curriculum development stage	B.S. requires 8 core courses and 4 concentration courses for 36 total credit hours; full degree requires 120 credit hours - 5 courses required for the minor for 15 credit hours - Graduate program requires 30 credit hours	Communication Writing Critical Thinking Collaboration
Northeastern University Awareness and Localization of Explosives Related Threats (ALERT)	DHS COE	ALERT and Gordon-CenSSIS Scholars Program	M.S. in Robotics, AI, Applied Machine Intelligence, Security and Resilience Studies, Homeland Security, Gordon Engineering Leadership Program; Graduate Certificates in Strategic Intelligence Studies and Remote Sensing	M.S. programs require 32 credit hours and can be completed in 1-2 years; Certificates take 15-16 credit hours or one year	Writing Communication

George Mason University Criminal Investigations and Network Analysis (CINA)	DHS COE	B.S. in Computational and Data Sciences, Forensic Science, Criminology; Minor in Intelligence Studies	M.S. in Applied Information Technology, Forensic Science/Digital Forensics, Geospatial Intelligence	B.S. programs require 120 hours; Masters programs require 30-36 credit hours	Collaboration Critical Thinking
University of Southern California National Center for Risk and Economic Analysis of Terrorism Events (CREATE)	DHS Emeritus COE	B.A. in Intelligence and Cyber Operations, Minor in Human Security and Geospatial Intelligence	M.P.P specialization in Homeland Security; M.S. in Risk Management, Human Security and Geospatial Intelligence (also a certificate), Certificate in Homeland Security and Public Policy; Certificates in Aviation Safety and Security; CREATE Executive Program in Counterterrorism; ; Law Enforcement Advanced Development (LEAD) Certificate Program; Executive Leadership Program	B.A. in Intelligence requires 128 credits; 51-54 must come from interdisciplinary units within USC Dornsife College of Letters, Arts and Sciences and the USC Viterbi School of Engineering; M.P.P requires 48 credits; M.S. degrees require 34-36 credits; Certificates 15-16 credits, except for Aviation certificates in which courses only last about five days each (five classes required in total); LEAD program is a six-month program using online and classroom courses	Collaboration Communication

Purdue University Visual Analytics for Command, Control, and Interoperability Environments (VACCINE)	DHS Emeritus COE	B.S. in Data Sciences and Visualization, Digital Criminology, Unmanned Aerial Systems, Visual Design and Virtual Product Integration; (SURF) Summer Undergraduate Research Fellowships Program	M.S. in Computer Graphics Technology, Technology Leadership and Innovation, Defense Engineering and Technology; Certificate in Applied Data Analytics (fully online); HS-STEM Career Development Program	B.S. degrees take 120 credits; M.S. 33 credit hours	Communication Collaboration Leadership/Project Management
University of Texas A&M Zoonotic and Animal Disease Defense (ZADD)	DHS COE	B.A. International Studies--w/without International Politics and Diplomacy Track; B.A. Political Science	M.A. Political Science; Ph.D. Political Science	Varies	Critical Thinking

Appendix D
Researcher Biographies

Dr. Michelle Black

Michelle Black, Ph.D. is an Assistant Professor in the Department of Political Science for the University of Nebraska at Omaha (UNO). Dr. Black is the Director of Workforce Development and Education, an Executive Team member, and Lead Researcher for the National Counterterrorism Innovation, Technology and Education (NCITE), which is a Department of Homeland Security Center of Excellence. She is a Research Fellow for the National Strategic Research Institute (NSRI) at the University of Nebraska, and Editor for Space and Defense Journal. Her research has been published in leading political science and security journals, including Dynamics of Asymmetric Conflict: Pathways towards Terrorism and Genocide, Journal of Political Science Education, and Defense and Security Analysis on the topics of insurgency, terrorism, and deterrence. Her current research is supporting the North Atlantic Treaty Organization (NATO) by developing a multi-actor analysis deterrence methodology, which models state and non-state actors' decision-making preferences within a complex threat scenario. She is also leading a research project for Department of Homeland Security through NCITE investigating intelligence training and education trends and challenges across the intelligence community. In addition to her academic career, Dr. Black has over 17 years of professional experience with the Department of Defense. Prior to joining UNO, she was a government civilian for the Department of the Air Force, specializing in deterrence analysis and adversary decision-making for United States Strategic Command (USSTRATCOM) Plans and Policy Directorate at Offutt Air Force Base. During her time at USSTRATCOM, she provided analysis and recommendations to senior leaders about decision-making strategy, deterring state and non-state actors, and regional expertise. Dr. Black has worked in psychological operations as U.S. Army Special Operations NCO (Airborne) for the United States Army Special Operations Command (USASOC) and later as a defense contractor. She deployed to Iraq, Kuwait, and Qatar during Operation Iraqi Freedom and Operation Enduring Freedom working on counterterrorism campaigns for the United States Army.

Dr. Lana Obradovic

Dr. Lana Obradovic is an Associate Professor of Political Science and the Director of the Intelligence Community Center of Academic Excellence at University of Nebraska at Omaha (UNO). She also serves as the Academic Director of the USSTRACOM's Strategic Leadership Fellows Program, Academic Director and the BOLD Leadership Institute, funded by the U.S. Embassy in Sarajevo, Bosnia and Herzegovina. Dr. Obradovic is a certified faculty in the DoD’s National Security Innovation Network “Hacking for Defense” program and serves as “Expert” (formerly, *Defense Civilian Auxiliary Corps*) providing advice on pressing national security issues bimonthly. She has taught international relations and comparative politics courses for the past 18 years at St. John’s University, CUNY, and Mercy College in New York City, and at Yonsei University in South Korea, and has directly supervised student teams that won the General Larry D. Welch Deterrence Writing Award in 2016, 2017, and 2018. Dr. Obradovic’s own book, Gender Integration in NATO Military Forces, won the ERGOMAS 2015 Best Book in Civil-Military Relations award. Her recent publications include “Teaching Deterrence: A 21st Century Update” in *Journal of Political Science Education*, USSTRATCOM’s Women, Peace and Security and Deterrence Report, and research projects on the gray zone conflicts, with a particular focus on the Arctic and the Balkans. She earned her BA degrees in Political Science and International Affairs at the University of Nebraska-Lincoln (1999), a Master of Arts in Government and Politics and a Graduate Certificate in International Law and Diplomacy at St. John’s University (2001), and a Master of Philosophy (2006) and a Ph.D. in Political Science from the Graduate Center of the City University of New York (2009)

Claire Benedix

Claire Benedix is a second-year graduate assistant working towards her M.S. in Political Science with an international affairs concentration. She received her B.A. in Political Science and International Studies with concentrations in foreign and national security affairs and global strategic studies from the University of Nebraska at Omaha. She is currently a graduate researcher for the University of Nebraska at Omaha's National Counterterrorism Innovation, Technology, and Education Center (NCITE), a U.S. Department of Homeland Security Center of Excellence. Her current research with NCITE focuses on training implementation and education standards within the intelligence community workforce. Her research interests include counterterrorism workforce training, intelligence collection and analysis, and reform within the intelligence and defense communities. She hopes to continue her federal service after graduation.

Liz Bender

Liz Bender is a senior majoring in Criminology & Criminal Justice and Spanish with minors in Political Science and Chicano/Latino Studies at the University of Nebraska at Omaha. She is an honors student and student researcher with the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a U.S. Department of Homeland Security Center of Excellence. She has worked with NATO on a multi-actor deterrence methodology, with Dr. Michelle Black and fellow student researcher Josie Nelson, where she researched and wrote strategic profiles for eco-terrorist groups for use in a deterrence scenario. Her other research interests include domestic extremism, domestic terrorism, counterterrorism, and radicalization. In addition to her research with Project 10, she is helping to develop a coding schema to analyze leaders of domestic extremist organizations. She is expected to graduate in May of 2022 and hopes to continue her research and academic career in graduate school upon graduation.

Josie Nelson

Josie Nelson is a recent graduate of the University of Nebraska at Omaha, she graduated magna cum laude with her BA in International Studies with a concentration in global strategic studies and Political Science with a concentration in foreign affairs and national security. Josie is an upcoming graduate student who will work towards her M.S. in Political Science with an international affairs concentration in Fall of 2021. She has worked with NATO on a multi-actor deterrence methodology, with Dr. Michelle Black, where she researched and wrote strategic profiles on Japan and South Korea. Other recent research projects also include her participation in the U.S. Strategic Command Academic Alliance Conference in March of 2021, where she wrote and presented a paper titled, *American Power in the Pacific and the Rise of Minilateralism*. She began her work as a student researcher with the National Counterterrorism Innovation, Technology and Education (NCITE) Center, a U.S. Department of Homeland Security Center of Excellence, as an undergraduate and will continue as a graduate researcher for NCITE. Her research interests include deterrence, counterterrorism, great power competition, intelligence collection and analysis, and international affairs.

Grant Van Robays

Grant Van Robays is a senior and honors student majoring in Political Science with minors in Sociology and Human Rights Studies at the University of Nebraska at Omaha. He currently has an internship with the National Counterterrorism Innovation, Technology and Education (NCITE) Center, which is a Center of Excellence for the Department of Homeland Security (DHS). His research interests include intelligence analysis, counterterrorism, and deterrence. Grant intends to graduate in 2022 and enter the workforce in the intelligence community, national security field, or public service.

References

Bellavita, C. (2008). Changing homeland security: What is homeland security? *Homeland Security Affairs,* 4(2). http://www.hsaj.org/?full article=4.2.1.

Black, M. (2016). Cyber ethnography: A critical tool for the Department of Defense? *Comparative Strategy,* 35(2). 103-113.

Bruce, J.B., and Roger, G. (2015). Professionalizing Intelligence Analysis. *Journal of Strategic Security,* 8(3), 1-23. https://scholarcommons.usf.edu/jss/vol8/iss3/1.

Builta, J. A., & Heller, E. N. (2011). Reflections on 10 years of counterterrorism analysis. *Studies in Intelligence*, 55(3), 1–15.

Burch, J. (2008). The domestic intelligence gap: Progress since 9/11? *Proceedings of the 2008 Center for Homeland Defense and Security Annual Conference*. Homeland Security Affairs. https://www.hsaj.org/articles/129.

Campbell, S.H. (2011). A survey of the US market for intelligence education. *International Journal of Intelligence and Counter Intelligence,* 24 (2), 307-337.

Collier, Michael W. (2005). A pragmatic approach to developing intelligence analysts. *Defense Intelligence Journal,* 14(2), 17-35.

Comiskey, J. (2015). How do college homeland security curricula prepare students for the field? *Journal of Homeland Security Education,* 4(20). https://fisherpub.sjfc.edu/ education_etd/180/.

Congressional Research Service [CRS]. (2019). Covert action and clandestine activities of the intelligence community: Selected congressional notification requirements in brief. https://fas.org/sgp/crs/intel/R45191.pdf.

Cordero, C. (2020). Reforming the Department of Homeland Security through enhanced oversight & accountability. https://www.cnas.org/publications/reports/reforming-the-department-of-homeland-security-through-enhanced-oversight-accountability.

Corvaja, A.S., Brigita J., and Uwe, M.B. (2016). The rise of intelligence studies: A model for Germany? *Connections: The Quarterly Journal,* 15(1), 79-106. DOI:10.11610/Connections.15.1.06.

Coulthart, S, and Crosston, M. (2015). Terra incognita: Mapping American intelligence education curriculum. *Journal of Strategic Security, 8*(3): 46-68. https://www.researchgate.net/publication/282437336_Terra_Incognita_Mapping_American_Intelligence_Education_Curriculum.

Customs and Border Patrol. (2015). Vision and strategy 2020: U.S. Customs and Border Protection strategic plan. https://www.cbp.gov/sites/default/files/documents /CBP-Vision-Strategy-2020.pdf.

Defense Counterintelligence and Security Agency. (2021). National industrial security program (NISP). https://www.dcsa.mil/mc/ctp/nisp/.

Defense Intelligence Agency [DIA] (2008). DIA analyst training requirements and competencies. http://scripts.cac.psu.edu/users/t/s/tsb4/GEOINT/DIA_Analyst_Competencies.pdf.

Department of Defense. (2006). National industrial security program operating manual. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf.

Department of Defense. (2015). DoD general intelligence training and certification. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/330502p.pdf?ver=-M9Eo907_SRPRUd8aBlJug%3D%3D.

Department of Defense Office of Inspector General. (2014). Evaluation of DoD intelligence training and education programs for the fundamental competencies of the DoD intelligence workforce. https://media.defense.gov/2018/Aug/31/ 2001960960 /-1/-1/1/DODIG-2015-015%20(REDACTED).PDF.

Department of Homeland Security [DHS]. (2006). Performance management: Number 3181. https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_3181_performance_management.pdf.

Department of Homeland Security [DHS]. (2016). National prevention framework. https://www.hsdl.org/?view&did=793534.

Department of Homeland Security Committee [DHS Security Committee]. (2016). Reviewing the Department of Homeland Security's intelligence enterprise. https://www.hsdl.org/?view&did=797351.

Department of Homeland Security [DHS]. (2017). DHS lexicon terms and definitions. https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf.

Department of Homeland Security [DHS]. (2019). The DHS strategic plan 2020-2024. https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf.

Department of Homeland Security [DHS]. (2020). Office of Intelligence and Analysis strategic plan: FY 2020-2024. https://www.dhs.gov/publication/office-intelligence-and-analysis-fy-2020-2024-strategic-plan.

Department of Homeland Security. (2021). Homeland security information network (HSIN) 2019 annual report. Homeland Security Information Network. https://www.dhs.gov/sites/default/files/publications/hsin-2019-annual-report_0.pdf.

Dorondo, P.J. (1960). For college course in Intelligence. *Studies in Intelligence,* 4(3), 15-19.

Dorn, D. (2019). Teaching intelligence analysis writing skills: A program evaluation. *Journal of Intelligence and Analysis,* 24(2), 73-94.

Dujmovic, N. (2017). Less is more, and more professional: Reflections on building an 'ideal' intelligence program. *Intelligence and National Security,* 32(7), 935-943. DOI: 10.1080/02684527.2017.1328822.

Federal Bureau of Investigation [FBI]. (2005). The Federal Bureau of Investigation's effort to hire, train, and retain intelligence analysts. https://oig.justice.gov/reports/FBI/a0520/ final.pdf.

Federal Bureau of Investigation [FBI]. (2020). FBI core competencies. https://www.fbijobs.gov/sites/default/files/fbi_core_competencies_definitions.pdf.

Global Advisory Committee. (2015). Analyst professional development road map. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/analyst_professional_development_road_map1.pdf.

Global Justice Information Sharing Initiative. (2010). Common competencies for state, local, and tribal intelligence analysts. https://bja.ojp.gov/sites/g/files/xyckuh186/files /media/document/common_competencies_state_local_and_tribal_intelligence_analysts-2.pdf.

Government Accountability Office. (2021). DoD critical technologies: Plans for communicating, assessing, and overseeing protection efforts should be completed. https://www.gao.gov/assets/gao-21-158.pdf.

Green, P. (2008). An analysis of the requirements and potential opportunities for the future education of law enforcement intelligence analyst. *Naval Postgraduate School Thesis,* Monterey, CA. http://hdl.handle.net/10945/4235.

Hedley, John Hollister. (2005). Twenty years of officers in residence. *Studies in Intelligence,* 49(4): 31-39. https://www.cia.gov/resources/csi/studies-in-intelligence/volume-49-no-4/twenty-years-of-officers-in-residence.

Inspector General of the Intelligence Community, Inspector General of the Department of Homeland Security, and the Inspector General of the Department of Justice. (2017). Review of domestic sharing of counterterrorism information. https://www.dni.gov/files /documents/Newsroom/Domestic_Sharing_Counterterrorism_Information_Report.pdf.

Johnson, Loch K. (2019). Spies and scholars in the United States: Winds of ambivalence in the groves of academe. *Intelligence and National Security,* 34(1), 1–21. https://www.tandfonline.com/doi/epub/10.1080/02684527.2018.1517429?needAccess=true.

Johnson, R. (2005). *Analytic culture in the US intelligence community: An ethnographic study*. Washington, DC: Center for the Study of Intelligence.

Katz, Brian. (2020). The collection edge: Harnessing emerging technologies for intelligence collection. https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.

Landon-Murray, M., and Coulthart, S. (2020). Intelligence studies programs as US public policy: A survey of IC CAE grant recipients. *Intelligence and National Security,* 35 (2), 269-282. https://www.tandfonline.com/doi/epub/10.1080/02684527.2019.1703487?needAccess=true.

Lowenthal, M. M. (2014). The education and training of intelligence analysts. In Roger Z. George & James B. Bruce (Eds.), *Analyzing intelligence: National security practitioners' perspectives.* Washington, DC: Georgetown University Press.

Marrin, S. (2009). Training and educating US intelligence analysts. *International Journal of Intelligence and Counterintelligence*, 22(1), 131-146.

Moore, D.T., Krizan, L., & Moore, E.J. (2005). Evaluating intelligence: A competency-based model. *International Journal of Intelligence and Counterintelligence, 18*(2), 204-220. https://www.tandfonline.com/doi/abs/10.1080/08850600590911945.

Platt, W. (1957) *Strategic intelligence production: basic principles*. FA Praeger.

Office of the Director of National Security. (2010). Intelligence community directive number 610: Competency directories for the intelligence community workforce. https://www.dni.gov/files/documents/ICD/ICD_610.pdf.

Office of the Director of National Security. (2010). Intelligence community standard number 610-3: Core competencies for non-supervisory intelligence community employees at GS-15 and below. https://fas.org/irp/dni/icd/ics-610-3.pdf.

Office of the Director of National Security. (2010). Intelligence community standard number 610-4: Core competencies for supervisory and managerial intelligence community employees at GS-15 and below. https://fas.org/irp/dni/icd/ics-610-4.pdf.

Office of the Director of National Security. (2010). Intelligence community standard number 610-7: Competency directory for analysis and production. https://ni-u.edu/RTE/Policy-ICS_610-7_Competency_Directory_for_Analysis_and_Production.pdf.

Office of the Director of National Intelligence. (2011). Terms & definitions of interest for DoD counterintelligence professionals. https://www.dni.gov/files/NCSC/ documents/ci/CI_Glossary.pdf.

Office of the Director of National Security. (2012). Intelligence community directive number 656: Performance management system requirements for intelligence community senior civilian officers. https://www.dni.gov/files/documents/ICD/ICD_656.pdf.

Office of the Director of National Security. (2014). Intelligence community directive number 651: Performance management for the intelligence community civilian workforce. https://www.dni.gov/files/documents/ICD/ICD_651.pdf.

Office of the Director of National Security. (2015). Intelligence community directive number 203: Analytic standards. https://fas.org/irp/dni/icd/icd-203.pdf.

Office of the Director of National Security. (2020). Intelligence community centers for academic excellence: Strategy 2020-2023. https://www.odni.gov/files/CHCO/ documents/CAE/IC_CAE_Strategy.pdf.

Office of the Director of National Security. (2021). Accountability. https://www.dni.gov/index. php/how-we-work/accountability.

Office of the Director of National Security. (2021). What is intelligence? https://www.dni.gov/ index.php/what-we-do/what-is-intelligence.

Office of Personnel Management [USOPM]. (2020). Agency management report: Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications /dhs-2020-fevs-agency-management-report_3.pdf.

Ortiz, Christopher. (2016). CIA launches signature school program at UNM. https://www.bizjournals.com/albuquerque/news/2016/11/11/cia-launches-signature-school-program-at-unm.html.

Pelfrey, W.V. (2013). Homeland security education: A way forward. *Homeland Security Affairs,* 9(3). http://hdl.handle.net/10945/27490.

Rudner, M. (2009). Intelligence studies in higher education: Capacity-building to meet societal demand. *International Journal of Intelligence and Counter Intelligence,* 22(1), 110-130.

Sherman, K. (1955). The need for an intelligence literature. *Studies in Intelligence, 3*. http://www.odci.gov/csi/books/shermankent/2need.html.

Smith, J. (2013). Amateur hour? experience and faculty qualifications in U.S. intelligence courses. *Journal of Strategic Security,* 6(3), 25-39. DOI: http://dx.doi.org/10.5038/1944-0472.6.3.3.

Spradley, J. P. (1979). The ethnographic interview. Wadsworth: Cengage Learning.

Spracher, W.C. (2009). National security intelligence professional education: A map of US civilian university programs and competencies. PhD diss. The George Washington University.

Spracher, W. C. (2010). Teaching intelligence in the United States, the United Kingdom, and Canada. *Oxford Research Encyclopedia of International Studies*. https://oxfordre.com /view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-308.

Spradley, J. P. (1979). *The ethnographic interview*. Waveland Press Inc.

Stone, M. (2021). If you love them, let them go: A comparative analysis of rotational programs and recommendations for the homeland security enterprise. Master's thesis. Naval Postgraduate School. https://www.hsdl.org/?view&did=854358.

Terrorist Identities Datamart Environment (TIDE). Homeland security digital library. (2020). https://www.hsdl.org/?view&did=826091.

Wu, Y. (2013). Strengthening Intelligence Education with Information-Processing and Knowledge-Organization Competencies. *Journal of Strategic Security, 6*(3), 10-24. https://www.jstor.org/stable/26457765.