Tampere University

Jarkko Oksanen

THE QUEST FOR KNOWLEDGE

Intelligence Community Centers for Academic Excellence Institutions as Educators of Intelligence Analysis in the United States

Faculty of Management and Business
Master's Thesis
October 2022

ABSTRACT

Jarkko Oksanen: The Quest for Knowledge: Intelligence Community Centers for Academic Excellence Institutions as Educators of Intelligence Analysis in the United States
Master's Thesis
Tampere University
Degree Program in Politics
October 2022

This master's thesis examines intelligence education within the Intelligence Community Centers for Academic Excellence (IC CAE) institutions, which are funded by the federal government of the United States. Intelligence within this study is understood as the process in which information important to national security is requested, collected, analyzed, and disseminated, and as the products of that process. Intelligence education in the United States has grown in scope after the terrorist attacks of 2001 and the IC CAE program was established to increase the pool of diverse and proficient workforce for the needs of the United States Intelligence Community. The primary data of this study consists of Office of the Director of National Intelligence (ODNI) and Senate Select Committee on Intelligence (SSCI) documentation and a sample of 22 Intelligence Community Centers for Academic Excellence institutions' curricula and course descriptions. Secondary data includes numerous intelligence studies monographies and journal articles. Although the curricula of various intelligence education programs have been studied before, the formation of their curricula has not been researched through curriculum theory.

The present study incorporates the theoretical components of the globalization of intelligence, the universities-security-intelligence nexus, and the institutional and programmatic curriculum to its theoretical framework. The premise of the theoretical framework holds that at the level of institutional curriculum, national security trends in the United States are reflected in the themes of the expectations towards the Intelligence Community and intelligence analysis. These expectations, then, are assumed to be observable at the programmatic level of intelligence education curricula. To investigate these objectives, the research questions are as follows: 1) What kind of themes arise as expectations for intelligence analysis for the institutional curriculum of intelligence education? and 2) How are the themes of the institutional curriculum present in the procedural knowledge intelligence analysis courses of the Intelligence Community Centers for Academic Excellence institutions' programmatic curriculum?

To answer to these research questions, this study adopts a descriptive research design with content analysis as its research method. Based on the results, it is argued here that two sets of themes are observable in the data. First, the analytic tradecraft of intelligence analysis is expected to be objective, impartial, timely, and to apply scientific practices as reflected in the Intelligence Community Directives (ICD) standards. These themes are connected to a second set of themes regarding strategic all-source intelligence analysis, which is expected to be predictive and multidisciplinary. The themes of the institutional curriculum recurred at the programmatic level and occurred in the IC CAE curricular data. The analysis indicated that introductory courses in intelligence analysis had incorporated various elements derived from the Intelligence Community's analytic tradecraft, including Analytic Standards, Analytic Tradecraft Standards and Structured Analytic Techniques (SATs), as well as intelligence-specific verbal and written communication techniques, and critical thinking. A disconnect between the institutional and programmatic curriculum levels was the relative lack of anticipatory methodologies within the sample curricula, as the strategic intelligence analysis themes highly valued prediction. While the results are preliminary, the present study found that curriculum theory was purposeful in the analysis of intelligence education and could be applied in various studies in the future.

Keywords: Intelligence Education, Intelligence Analysis, Intelligence Community Centers for Academic Excellence (IC CAE), United States Intelligence Community, Intelligence Studies

CONTENTS

ABBREVIATIONS AND ACRONYMS

ACH Analysis of Competing Hypotheses

CIA Central Intelligence Agency

COMINT Communications Intelligence

DCI Director of Central Intelligence

DCIA Director of Central Intelligence Agency

DIA Defense Intelligence Agency

DNI Director of National Intelligence

DoD Department of Defense/Pentagon

FBI Federal Bureau of Investigation

FISA Foreign Intelligence Surveillance Act of 1978

GEOINT Geospatial Intelligence

HPSCI House Permanent Select Committee on Intelligence

HUMINT Human Intelligence

IAFIE International Association for Intelligence Education

IC CAE Intelligence Community Centers for Academic Excellence

ICD Intelligence Community Directives

IIO Information Influence Operations

IJIC International Journal of Intelligence and CounterIntelligence (Journal)

IMINT Imagery Intelligence

INS Intelligence and National Security (Journal)

IR International Relations

IRTPA Intelligence Reform and Terrorism Prevention Act of 2004

IS Intelligence Studies

MASINT Measurement and Signature Intelligence

MIP Military Intelligence Program

NATO North Atlantic Treaty Organization

NGA National Geospatial-Intelligence Agency

NIC National Intelligence Council

NIE National Intelligence Estimate

NIP National Intelligence Program

NIS National Intelligence Strategy

NRO National Reconnaissance Office

NSA National Security Agency

NSC National Security Council

NSS National Security Strategy

ODNI Office of the Director of National Intelligence

OE Outside Expert

OSINT Open Source Intelligence

PDB President's Daily Brief

PDDNI Principal Deputy Director of National Intelligence

SAT Structured Analytic Technique

SEIB Senior Executive Intelligence Brief

SIGINT Signals Intelligence

SSCI Senate Select Committee on Intelligence

TS/SCI Top Secret/Sensitive Compartmentalized Information

UKUSA The United Kingdom – United States of America Agreement

US United States of America

USA PATRIOT Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

US IC United States Intelligence Community

WMD Weapons of Mass Destruction

FIGURES AND TABLES

1. INTRODUCTION: THE UNENDING NEED FOR INTELLIGENCE

"Knowledge crowns those who seek her" – Slogan of Syracuse University

Intelligence consists of the process in which information important to national security is requested, collected, analyzed, and disseminated. Intelligence is also the product of that process, as well as the safeguarding of those processes by means of counterintelligence. In addition, intelligence is operations carried out by intelligence actors. (Lowenthal 2015, 10; McDowell 2009, 11; Gill 2009; 214–217.) The duality of intelligence process and product is inherently predictive, as political, military and other decision-makers, being the prime customers of intelligence, expect forewarning of future events (Marrin 2011, 11; Agrell & Treverton 2015, 3–4). Since intelligence is used to navigate an international system of various state and non-state actors, it is also global in scope. Intelligence is not only utilized to maintain power relative to competitors, but also to outmaneuver them with decision advantage. (Svendsen 2012a; Stout & Warner 2018.) The inability of the United States Intelligence Community (US IC) to predict the terrorist attacks of 2001 was largely perceived as an intelligence failure. Faulty intelligence analysis was blamed, and various legislative and organizational reforms were introduced to prevent anything similar from ever happening again. This has also resulted in intelligence analysis facing considerable public scrutiny. The intelligence community has, in turn, made great efforts to implement more standardized and professional analytic tradecraft. (Treverton 2009; Fingar 2011; Durbin 2017.)

The global and diffused perception of threats and risks has contributed to the United States Intelligence Community needing an increasing number of educated and proficient personnel in its ranks (Treverton 2009; Campbell 2011; Landon-Murray 2011). As a result of this demand for a capable workforce, intelligence has become an educational field within universities and other institutions of higher education. The recent phenomenon of intelligence education has grown in the past two decades and spread globally. (Svendsen 2012a; Dujmovic 2017; Gearon 2020). In the United States, a specific funding program, the Intelligence Community Centers for Academic Excellence (IC CAE), was established in 2005 and is now overseen by the Office of the Director of National Intelligence (ODNI). The

program seeks to “meet the nation’s demand for a diverse cadre of professionals to carry out national security priorities and obligations”. That is, educating a pool of proficient talent for potential intelligence work. (ODNI 2020). Some studies have examined the IC CAE program and the curricular content of participating institutions (Landon-Murray & Coulthart 2020), but few if any have been interested in the formation of these curricula. There is, after all, a range of expectations towards intelligence community workforce at the level of the Executive branch of government (the President), Congress (especially the two parliamentary intelligence oversight committees), and the intelligence community itself (the ODNI, but each agency with their specific needs as well) (Fingar 2011; Gearon 2020).

The premise of this study is that these expectations are manifest in the *institutional curriculum*, a theoretical construct of the policy between schooling, culture, and society. Curriculum-making at the level of the institutional curriculum typifies “what is desirable in social and cultural orders, what is to be valued and sought after by members of a society or nation”. (Deng 2009, 589.) It is investigated in this study what themes constitute the institutional curriculum and how the institutional curriculum is reflected at the level of program design of the IC CAE institutions. The more empirically accessible level of *programmatic curriculum* rationalizes certain knowledge, skills, and dispositions, and is often defined by former practitioners who have moved to the academia (ibid.; Walsh 2017b). The programmatic curriculum demonstrates the actual, implemented curricula, and is studied here via a sample of intelligence education curricula and course descriptions from the IC CAE institutions. By sampling a selection of documentation from the Intelligence Community, Congress, and the IC CAE institutions, this study examines the formation and interaction of the institutional and programmatic levels of intelligence education curriculum in the United States. To my knowledge, there is no prior research that examines the formation of IC CAE program curricula via curriculum theory, and the study addresses that research gap. To approach this research problem, this study adopts a descriptive research design. Content analysis is utilized as the principal research method.

The research questions of the study are the following:

1. What kind of themes arise as expectations for intelligence analysis for the institutional curriculum of intelligence education?

2. How are the themes of the institutional curriculum present in the procedural knowledge intelligence analysis courses of the Intelligence Community Centers for Academic Excellence institutions' programmatic curriculum?

Based on the results, it is argued here that two sets of themes describe the expectations inherent in the theorized institutional curriculum. First, the theme *Improvement of Analytic Tradecraft and Intelligence Analysis* expects intelligence analysis to be objective, impartial, timely, and to apply scientific practices as reflected in the Intelligence Community Directives (ICD) standards. These themes are closely connected to the second set of themes, *Strategic, Disciplinary, and Scientific Knowledge*. This set of themes regards strategic intelligence analysis as an all-source intelligence effort, that must be predictive and utilize multidisciplinary domains of science and knowledge to achieve its anticipatory objectives and forewarning. The academia is regularly consulted about knowledge areas germane to this set of themes. Within these themes, the academia is seen as a valuable outreach partner to intelligence, which can identify new lines of inquiry relevant to intelligence.

These themes of the institutional curriculum were observed within the programmatic curriculum. The sample program types were mostly scholar programs, certificates and minors, aligning with the trends noted in other studies. The selection of courses, however, was limited compared to previous research. Most of the course descriptions for intelligence related courses were expository, combining many tradecraft elements such as Structured Analytic Techniques (SATs), and intelligence-specific briefing, reporting, and critical thinking techniques. Courses within the sample were almost devoid of anticipatory methodologies, and this fact was the clearest disconnection between the conjectured institutional curriculum, and the implemented programmatic curriculum.

To investigate the research questions, the study proceeds with five chapters. Chapter 2 introduces the methodological framework of the study: research design, theoretical framework, sampling and data, and method of analysis. In support of the theoretical framework, Chapter 3 examines the global nature of American national intelligence policy from the perspective of historical and current expectations that are set upon intelligence, as well as intelligence education as public policy in the contemporary strategic environment. Chapter 4 explores the essential qualities of intelligence analysis that continue to challenge intelligence agencies: its relation to (social) science, the anticipation of futures, and the ways which uncertainty and confidence in analytic judgments are expressed in the intelligence

tradecraft. Chapter 5 presents the analysis of institutional and programmatic curricula of the sampled data. Chapter 6 details the main arguments of the study and proposes avenues for further research.

2. RESEARCH DESIGN AND METHODOLOGICAL FRAMEWORK

2.1. Research Designs for Intelligence Studies

Intelligence Studies (IS) was institutionalized as a sub-discipline of International Relations (IR) in the decades after its initial development during the 1950s (Ben Jaffel et al. 2020, 324). The roots of IS, similarly to IR, extend to other disciplines, such as strategic studies, history, law, and sociology (Svendsen 2009, 705), but its influences have become much more diverse in the last decade. This study is educationally situated within the discipline of IR, although it resembles "pure" Anglo-American Intelligence Studies literature in its overarching interest in the phenomenon of intelligence in the national context of the United States. Additionally, most of the secondary literature featured here is specialized in intelligence and theoretically detached from the larger debates in International Relations. Yet intelligence is an inseparable dimension of international politics and the discipline, even if quite under-theorized (Andrew 2004; Svendsen 2009; Marrin 2018). Intelligence very much occupies itself with international affairs and world politics but is conducted against and for other nations domestically and internationally. The global status of the United States rests on formidable intelligence apparatus that covers all sectors of policy. American connectivity with the intelligence world is influential and consists of complex multilateral and bilateral arrangements and two-directional intelligence liaison. Even the US is, to many extents, dependent on various partners across the world. (Svendsen 2012a, 95.) While research into the United States Intelligence Community is not generalizable to other intelligence systems, the factors above contribute to its significance in possibly informing other national contexts at the global stage of intelligence.

The most up-to-date scholarly discussions in Intelligence Studies take place in the British *Intelligence and National Security* (INS) and American *International Journal of Intelligence and CounterIntelligence* (IJIC) journals, both established in 1986.[1] From the pioneering US work in the 1950s (Sherman Kent among others), intelligence literature has seen gradual expansion in content and diversification in purpose, with the partial disclosures by British

[1] Other prominent, newer journals in the field include *International Journal of Intelligence, Security, and Public Affairs*, the *Journal of Intelligence Analysis*, the *Journal of Intelligence History*, the *Journal of Mediterranean and Balkan Intelligence*, and the *Journal of Policing, Intelligence and CounterTerrorism* (van Puyvelde & Curtis 2016, 1040).

and American Intelligence Communities starting from the 1970s. It is for these reasons that the body of literature is predominantly Anglo-American. Conforming to these perspectives does no favors to the intelligence nations left in the margins of the scholarship (Davies & Gustafson 2013; van Puyvelde & Curtis 2016). The relatively good availability of data and openness of these intelligence systems, however, allows for ease of conducting basic research about intelligence, compared to less transparent intelligence cultures.

Sources of data for intelligence research are as varied as they are for multidisciplinary social sciences in general. Agency historians and at times, outsiders, have access to various proprietary archives, and such research is not different from research in military and diplomatic history (Warner 2006, 21). The Central Intelligence Agency (CIA) has even published its own intelligence research journal *Studies in Intelligence* since 1955 (Kent 1955). Public provisions of the journal include classified articles and unclassified excerpts, available at the CIA website. For US-specific research, physical and electronic archives and databases are available for researchers,[2] in addition to news media sources, interviews, videos, statistics, and social media among others. Essential sources for insightful data are interviews, which are often featured as methods of data collection for journal articles and monographies, although they often tilt towards the anecdotal. Research ethics in IS obviously has to take into account the confidentiality of the identities of those interviewed, especially if they work in the intelligence profession. The leaked intelligence documents available from whistleblower breaches are another conundrum, as the academician must weigh between the leaked information in principle being classified, proprietary, and illegally disseminated, and their own judgment of the questions of self-censorship and academic freedom (Goldman 2018, 354–355). Research into some sensitive intelligence-connected subjects, such as authoritarian information influence operations (IIOs) may risk the researcher becoming a target of coercion (Nato StratCom CoE & Hybrid CoE 2022, 15), which underlines the need for added layers of cyber security while performing data collection.

[2] For instance, a 2019 research on intelligence outsourcing listed such repositories as The Black Vault, CIA Records Search Tool, Cryptome, Declassified Documents Reference System, Digital National Security Archive, Electronic Frontier Foundation, Every CRS Report, Federal Procurement Data System, Federal Register, Federation of American Scientists, Freedom of Information Act, Government Attic, Library of Congress, National Archives and Records Administration, United States National Security Archives (George Washington University) Public Access to Court Electronic Records, US Declassified Documents Online, and Wikileaks; and unclassified records from US government departments as its primary sources (van Puyvelde 2019, 233).

The research design of this study is descriptive. By being descriptive, the study classifies and categorizes empirical facts in categories that can be later used as evidence in theory building or hypothesis testing. Inferences from the data are made to describe the case where multiple social phenomena interact and constitute the case of the study. By making these inferences, the study reduces data to claims and propositions that advance the research objective and further studies. (Toshkov 2016, 31–33.) The study does not test hypotheses or make causal claims (della Porta & Keating 2008, 28–32). Rather, the study engages in exploratory research by investigating a phenomenon for more precise future research questions. In doing so, the study prototypes a theoretical framework that warrants further hypothesis testing and formation of successive inquiries (Rich *et al.* 2018, 69–70; Toshkov 2016, 32–33). The research cycle started with exploratory literature reviews and elaboration on the phenomena of intelligence teaching, from which the research design emerged. Subsequently, the two literature review components of the American intelligence context (including basic elements of the intelligence cycle, relevant American intelligence history, intelligence education, and the tradecraft of intelligence analysis) were conducted. Informed by this literature, the theoretical framework was assembled to describe the phenomena. Then, data was unitized by defining the units of analysis within the data (that is, sampling and coding units (themes)), and sampled, limiting the amount of sampling units to a manageable size. Afterwards, the coding of the data commenced, and as observations and inferences were made, data was reduced to analytic propositions. Finally, the results were narrated in the conclusions of the study. The theoretical components, data and sampling, and method of analysis are described in detail below.

2.2. Theoretical Framework: From Globalization of Intelligence to Curricula

This study draws from intelligence and curricular theories to examine a phenomenon that overlaps different levels of the social world. Top-down, the framework combines the theoretical concepts of globalization of intelligence and the universities-security-intelligence nexus, whose interaction results in the formation institutional and programmatic curricula in intelligence education. The actual, implemented intelligence education curricula as listed in online educational resources are accessible to anyone, of course, but without the application of theoretical lenses, they remain uninterpreted. This study sketches a more explicit

theoretical and empirical rendering of the elements that are likely to influence the real-world curricula.

In terms of system-level theory, Adam Svendsen's theory of intelligence globalization is applied in the study (Svendsen 2012a). Accordingly, it is assumed that the world is undergoing a process of *globalization of intelligence*, which Svendsen defines as:

> … "the greater interconnectedness and interdependence of intelligence and its institutions across the world. This is as well as referring to intelligence cooperation occurring more widely and in greater depth, whether between individuals, organizationally, technologically, and so forth." (Svendsen 2012a, 24.)

This cooperation – intelligence liaison – is understood here as the essential dynamic that regulates the globalization of intelligence. Intelligence liaison refers to national intelligence agencies performing a regular, close contact with governmental or non-governmental counterpart units, occurring either intrastate or interstate. Whereas regional intelligence arrangements contribute to the larger globalization, they are confined to their immediate regional surroundings. The UKUSA Agreement countries (the US, the UK, Canada, Australia and New Zealand) are an example of a group of states liaising regionally but expanding to global reach outside of the parameters of the regional sphere, as intelligence sharing agreements were made with many other European partners. (Svendsen 2012a, 10–15; 92–93.) Consequently, intelligence liaison initiated from the national level to the international level works both ways according to the logic of globalization, as such contact accelerates the wider spread of intelligence products, practices, technologies, personnel, and other artifacts to both national and international spaces. For instance, the increasing private-sector interest in intelligence analysis (especially in Business Intelligence or Competitive Intelligence) signals that competence in the tradecraft-part of such education is sought after not only within the IC itself (Parsons 2020, 278–279.) Some concerns arise along with the effects of the globalization of intelligence. In addition to the critique towards state surveillance policies that the Snowden leaks exacerbated, the proliferation of intelligence may introduce an adversarial logic to many social contexts, as intelligence frequently occupies itself with targets, producing a securitized rendering of the world (Diderichsen 2019, 417–418).

Intelligence liaison is performed at varying depth, ranging from formal agreements to high informality. Common liaison arrangements often include the sharing of information and joint collection efforts, within the domains of law enforcement, military and diplomacy. Its

performers include legal, defense, and military attachés, intelligence officers and even politicians. Intelligence liaison, then, also has relevance in each stage of the intelligence cycle, the fundamental intelligence process (Svendsen 2012a, 10–15.) Intelligence liaison with institutions of higher education is less about collection and sharing of intelligence, and more about outreach efforts. This outreach, pertinent to the IC CAE programs, has been focused on improving intelligence analysis. For instance, already in 2007, the 2006–2009 Director of the Central Intelligence Agency (DCIA) Michael Hayden stressed the importance of "analytic outreach" to stakeholders. (Svendsen 2012b, 21–22.) It is, however, important to note that while theoretically, intelligence liaison includes outreach to external experts, that is not the case with the US IC's guidance and instructions. The Intelligence Community Directive 205 makes a clear distinction between collection and consultation. (ODNI 2013.)

In the realm of overt intelligence liaison, academies are part of transnational knowledge network clusters, which consist of public and private, commercial and non-profit sector, government and non-governmental organizations (NGOs) stakeholders (Svendsen 2012a, 97). Universities and institutions of higher education act as intersections of global information flows, receiving, filtering, evaluating, modifying and channeling knowledge within the academia but to the broader society as well (Ahlbäck 2018). Certain hub cities such as Washington D.C. and London in the UK host a significant number of transnational, knowledge-circulating entities, readily connecting to the academia via what Liam Gearon calls the *universities-security-intelligence nexus*. This interface of universities-security-intelligence nexus comprises four domains:

> "The operational defines the different modus operandi of engagement between universities and security and intelligence agencies; the epistemological treats of knowledge as the critical currency of the universities-security-intelligence nexus; the ethical determines the framework for behavioural and moral judgements called into play, and called into question; the existential domain shows, at least in prospect, a common shared concern (put negatively) of forewarning and protection against threat and (put constructively) survival (of states, societies, even, today, species) as a shared strategic teleology or purpose." (Gearon 2020, 15–16.)

Within these domains operate national governments, national universities, and national security and intelligence agencies, which all have in common the global human concerns that ultimately orient their various quests for knowledge. All these domains manifest readily in the objects of this study. Whereas the operational domain interfaces with practices of intelligence liaison and outreach, the epistemological domain orients the contents of the favored intelligence education curricula. The ethical defies the code of conduct between the academy and intelligence agencies. The existential, on the other hand, unites intelligence

and the academies, although the academic telos is more defined in terms of shared humanity and not national concerns. For the theoretical framework of the study, the universities-security-intelligence nexus is thus considered a fundamental interface of exchange, where national intelligence requirements from Congress, the executive, and intelligence community levels are interacting with academic pursuits of science.

Universities have historically been a site of espionage intrigue and at times extensive human intelligence activity (Crosston 2018, 143; Johnson 2020, Gearon 2020, Lefebvre 2021). In Gearon's view, the operational domain of the universities-security-intelligence nexus is characterized by the modalities of *the covert* (the secret and clandestine collection of intelligence that entails limited accountability and openness), *the overt* (that is democratically accountable, and open), and *the covert-overt* (where secret, clandestine intelligence collection is performed in a political environment of democratic accountability and enhanced openness). The latter modality gives rise to the currently perceived dissonance of intelligence agencies performing overt and transparent student and staff outreach activities at campuses (and collaborating in the IC CAE program), but the odd researcher finding themselves mired in espionage investigations or getting arrested for spying. And as Gearon and Parsons suggest, the relations between intelligence and security apparatus are likely to intensify and diversify in the future, adhering to globalizational logics. (Gearon 2020, 20–21; Gearon & Parsons 2018, 84; 89–90.)

Second, Gearon's conceptualization of the epistemological domain of the universities-security-intelligence nexus combines collective, disciplinary and cross-disciplinary knowledge, and all-source intelligence. This pursuit of knowledge collection is "theoretically without limit". Thus, in the epistemological domain, national and global universities as well as national security and intelligence agencies have the shared commitment of reaching for all and any knowledge that furthers their missions. All-source intelligence refers to the synthesis of intelligence gathered via the five core disciplines of human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT) and open source intelligence (OSINT), which in addition to their epistemological roles have a critical operational dimension. As Gearon elucidates, the modus operandi of "protection from threats" shared by intelligence agencies is a focused objective since the enemies are known. This search for knowledge of undefined or prospective enemies draws the intelligence actors to the academia. Though academic purposes such as serving the public good serve to unite some institutions across the

academia, Gearon notes that no cross-disciplinary, unified definition of purpose exists. All knowledge within the academia, however, is potentially useful as knowledge for protection from security threats – that is, for intelligence analysis (Gearon 2020, 25–27.) *Intelligence analysis*, then, is defined here in Rob Johnston's (2005, 37) terms: "the socio-cognitive process, occurring within a secret domain, by which a collection of methods is used to reduce a complex issue to a set of simpler issues." The American tradition of strategic intelligence analysis was initially conceived as a social scientific endeavor (Kent 1965), but has to synthesize many other domains of scientific disciplines and knowledge to serve its purpose (Marrin 2011; Walsh 2020).

Descending to the realm of curricula, which are the more empirically operationalizable elements of this study, three levels of curriculum have been identified in Educational Studies and Curriculum Studies. First, Walter Doyle's[3] analysis of curriculum-making in the formation of a school subject involves the discourse of *institutional curriculum*. Institutional curriculum forms a vital link to the universities-security-intelligence nexus, as curriculum-making at the institutional level represents "what is desirable in social and cultural orders, what is to be valued and sought after by members of a society and nation". Therefore, the institutional level consists of curricular policy at the intersection between schooling, culture, and society. (Deng 2009, 589.) Applied to the scenario of the IC CAE program, the institutional curriculum-making involves considerations of national security, the resulting curation of IC workforce, and the functions of intelligence outreach (in the American intelligence parlance, this is called Analytic Outreach) that is extended to academic institutions (Gearon 2020; Johnson 2020; Gearon & Parsons 2018; Svendsen 2012b). To investigate the ideas that comprise the institutional curriculum of intelligence teaching in the United States, Chapters 3.1. and 3.2. present a literature review of the historical intelligence developments of the 20th century that have shaped those expectations. Chapter 3.3. and 3.4. focus on the teaching of intelligence. Chapter 4, in turn, concerns intelligence analysis, which connects the institutional and programmatic levels of curriculum with actual educational content. Conjecturally, the population of intelligence-teaching universities at large is also influenced, to some extent, by the level of institutional curriculum, even if they are not institutionally connected to the IC CAE program via funding or other outreach. Universities in the US tap

[3] Doyle's studies were unfortunately available for my research institution, but different papers from Educational Studies have referenced his theoretical framework sufficiently, and in addition, operationalized them in various ways.

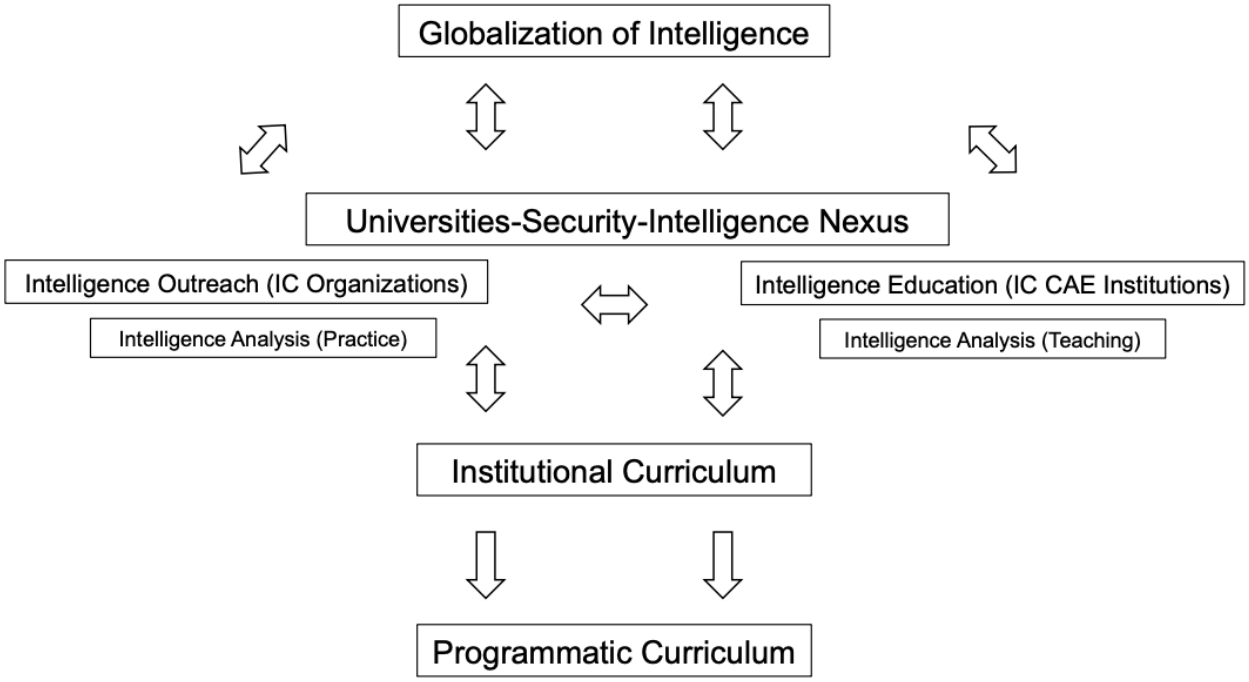
into lucrative industries such as the national security enterprise for revenue, responding to the demand of intelligence teaching (Dujmovic 2017, 939). Thus, the framework adopted here lends itself to wider future research on the intelligence-teaching phenomenon as well.

Curriculum-making at the level of the *programmatic curriculum* "transforms institutional curriculum into school subjects, programmes, or courses of study provided to a school or system of schools". The programmatic curriculum, thus, is contained in curriculum documents and materials for use in schools and classrooms. As a school subject or a course is constructed, a set of arguments is framed to rationalize the selection and arrangement of content (including knowledge, skills, and dispositions), and that content is then transformed for schools and classroom use. (Deng 2009, 589.) The notion of programmatic curriculum has also been elaborated to include the planning of aims, content, activities and sequence (Zhang & Heydon 2016, 549). Accordingly, the level of the programmatic curriculum is set to "embody a 'theory of content'", influenced by the institutional curriculum and manifested in teaching and learning (Deng 2009, 589). There are indications that the intelligence studies educators convey these theories of content via values judgments to intelligence curricula. These values are formed based on the educators' professional history, worldview and understanding of analytical skills, competencies and knowledge. (Walsh 2017b, 1006–1007.) When applied to the curricular expectations of the IC CAE program, important discussion has taken place in the literature on intelligence education (as outlined in Chapter 3.3.): Should the curricular content prepare and train students for prospective intelligence careers complementing their substance fields with intelligence minors or certificates, or should the institutions offer dedicated intelligence studies degrees (Johnson 2020, Walsh 2017b, Dujmovic 2017, Lowenthal 2017)? Currently, the IC CAE programs lean towards the former (Landon-Murray & Coulthart 2020). While building on the higher-level premises of theoretical framework (globalization of intelligence and the universities-security-intelligence nexus), the analytical part of this study is focused on the institutional and programmatic curriculum, as the primary data best corresponds to those level of analysis.[4] Below, the theoretical framework of this study is expressed in visual form. The model is intended to

[4] The framework of this study also informs one final level of curriculum-making: the *classroom curriculum*. The classroom curriculum is "characterized by a cluster of events jointly developed by a teacher and a group of students within a particular classroom". Curriculum-making at this level transforms the programmatic curriculum from its guidance documents and materials into actual instructional events. (Deng 2009, 589.) In a phenomenological sense, this level connects to the most intricate empirical reality of intelligence teaching, as it encompasses the actual experience, interests, and capacities of students (ibid.). Ironically, the classroom curriculum is something this study cannot access due to various research constraints. The category is included in the theoretical framework for future use.

remain parsimonious to accommodate future enhancements and different dimensions of the institutions involved.

Figure 1 Theoretical Framework of the Study.



2.3. Sampling and Organization of Primary and Secondary Data

To study the theoretical levels of globalization of intelligence, universities-security-intelligence nexus and institutional curriculum, the first component of primary data consists of a sample of government documents. They were selected to represent the Intelligence Community after the wider "analytic transformation" of the 2004 reforms had started to be implemented (SSCI 2011, 25–27), but also to include the intelligence developments of the last three administrations. First, representing the congressional discourse, the Senate Select Committee on Intelligence (SSCI) reports covering the years 2009–2011, 2011–2013, 2013–2015, 2015–2017, 2017–2019, and 2019–2021 were included. In these oversight reports, the SSCI reports its activities to the Senate, and to the general public. Second, Office of the Director of National Intelligence (ODNI) documentation includes the National Intelligence Strategies (NIS) of 2014 and 2019, as well as the Intelligence Community Directives (ICD) 203–208, which address the analytic standards of the IC. Moreover, the IC CAE Strategy of 2020 is included in the data. The NISs, ICDs, and the IC CAE Strategy represent the IC influence on curricular discourse, influencing both the

institutional and programmatic levels of curriculum.[5] Ultimately, it is the level of the intelligence community where detailed guidance on intelligence analysis is conceived and enacted.

The second component of primary data, which pertains to the programmatic curricula level, consists of a sample of 22 Intelligence Community Centers for Academic Excellence higher education institutions (ODNI 2022a). [6] In sampling the data, the vetting process excluded any program that did not have information on the IC CAE program requirements, including the associated degree programs, course listings, and course descriptions (the actual curricula). After the vetting of available data, 13 out of 37 grant receiving institutions, and 9 out of 34 legacy institutions were deemed eligible for further analysis (30.9% of the population). After the vetting process, available intelligence education curricula were compiled in a master corpus document for later coding. Only latest course catalog information (fall and winter semesters of 2022) was included. The data on the IC CAE institutions curricula faced a number of limitations. Unlike initially anticipated, no course literature was available for any of the curricula. As Coulthart and Crosston noted (2015, 56), course descriptions do not necessarily reflect the reality of teaching and the perspectives of individual instructors. Some programs had more content available than others, biasing the results towards the more informative programs. (ibid.) Since the classroom level of curriculum is not considered here, the sample was deemed sufficiently descriptive of the programmatic curriculum.

During the data collection phase, simple categorical data of the IC CAE units was recorded for organization. The variables included the eligibility of data for analysis (whether mentions of IC CAE courses and programs were listed at the educational institution's website, and whether curricular data was available), and program type (general IC CAE scholar program not attached to any specific study program; certificate, minor, or concentration; or undergraduate or graduate degree program). Finally, the integration of any mandatory intelligence analysis courses was recorded in the data. While these variables would have

[5] It is acknowledged here that to contextualize the global strategic environment of the "globalization of intelligence" theoretical level, ODNI's Annual Threat Assessments (ATA) of the US IC could have been included as additional sampling units in the primary sources. They were ultimately left out of the data, as they describe the configurations of the strategic environment rather than the analytic expectations that would be reflected in the institutional curriculum. Another set of documents with similar caveats, the National Security Strategies (NSS) were initially considered and coded as well but were deemed insufficiently descriptive of the intelligence analysis expectations to be included here.

[6] The population of the IC CAE institutions listed by the ODNI as of 2022 was 71. The sample and population universities are listed in Appendix, Tables 5 and 6.

allowed for limited statistical information about the sample, this was ultimately deemed unnecessary for the more qualitative nature of the applied thematic content analysis. The relative frequency distribution of each program type within the sample is illustrated in Figure 3 in the final analysis (Chapter 5.2.).[7]

The sampling for both components of the primary data was guided by the research questions and limited by the scope of the study itself. Sampling techniques based on the theory of representation (where all single members of a population have an equal chance of being included in the sample) was not applicable to the IC CAEs due to a lack of data, nor purposeful considering the qualitative nature of the research questions. In contrast, the sampling here represents *snowball sampling*, where an initial sampling of units yields more potential sampling units, and the sample grows until a termination criterion is reached. Underlying snowball sampling techniques is the intertextuality of the sampling units, which is displayed in networks and connectedness of the text units analyzed. (Krippendorff 2019, 116; 121–122.) In the sense of intertextuality, the SSCI reports and the NISs informing the institutional curricula are highly connected to each other by reoccurring references. The high intertextuality also applies to the secondary data, for which two literature reviews were conducted. The secondary data combines dozens of articles and books researching the United States intelligence community's history and functions, intelligence education, and different aspects of intelligence analysis. The literature builds a fundamental understanding of these themes to conceptualize the theoretical notions of globalization of intelligence, the universities-security-intelligence nexus, and the two levels of curricula to the overarching theoretical framework. As the research questions are based on curriculum theory, this research design allows the study to suggest answers to them by building a construct of the phenomena that is assumed to influence them.

2.4. Method of Analysis: Content Analysis

Content analysis is a research method that systematically analyzes the content of communication. Any material conveying a message, such as articles, websites, speeches, interviews, images, videos et cetera, is suitable for content analysis. Content analysis has been widely applied in International Relations starting from the 1940s, with current applications adopting quantitative, qualitative, manual and computer-aided analyses within

[7] A similar number is provided in Figure 4 for the population of the IC CAE institutions in the Appendix, although no program type information was available for roughly a third of the population.

a range of research designs. (Pashakhanlou 2017, 448–449; 459.) The formalization of content analysis is tied to advancements in communications studies and the development social scientific concepts in the 1930s and 1940s. During that time, new concepts were developed to analyze mass media, specifically the interrelationship of communication content and the recipients. Propaganda analysis of the Second World War advanced content analysis by focusing on how to place communication content to its respective context of its production and reception. The 1940s saw further application of content analysis in disciplines such as political science, psychology, education and literary studies. (Schreier 2012, 10–12.)

Contemporary content analysis "is an empirically grounded method, exploratory in process, and predictive or inferential in intent". As described by Krippendorff (2019), content analysis has incorporated various social theoretic developments in its conceptual foundations that contribute to the theoretical framework of this study. These principles, then, act as central assumptions about how intelligence, and intelligence curricula are constructed. First, content analysis acknowledges that global, dynamic and technologically supported interdependencies form *systems* manifest in ubiquitous communication networks. Global systems differ markedly from one-way mass media, since they possess properties of interactivity and simultaneity of parallel communication on a global scale, with potentially universal participation. Second, *computation* has brought about the increasing replacement of communicators by algorithms. Messages are generated by robots and addressed to computers in various technologically defined settings such as automatic teller machines, online shopping, robo-calls and so on. Textual matter is accessible in vast quantities via search engines and online data repositories. Consequently, social life and interaction have been altered in complex ways that require novel theorizing. Finally, the acceptance of *discursive co-construction* (constructivism) implies a life lived together in linguistic structures. Human institutions are co-constituted as interdependent realities through discourse. Discursively co-constructed texts, therefore, contribute to the supporting or challenging social realities – for instance in activities such as collaborative innovation, and scientific research. (Krippendorff 2019, 3.)

Out of the multiple ways of conducting content analysis, Krippendorff's comprehensive system of the method of content analysis is applied in this study. After the sampling of data, as described in Chapter 2.3., unitizing follows. In the *unitizing* phase, observational instances in support of the hypothesis or conclusion are selected. Units are wholes that the

researcher distinguishes and treats as independent elements. *Sampling units* are “units that are distinguished for selective inclusion in an analysis”. For this research, sampling units in the primary data are the various government documents included (NISs, and SSCI reports), as well as the ICDs, and the curricula of the IC CAE sample institutions. (Krippendorff 2019, 102–104; 116.) *Recording/coding units* (hereafter referred to as coding units), on the other hand, are selected for separate description, transcription, recording, or coding. Coding units are compared, analyzed, and summarized to be used as the basis of the inferences of the final analysis. They are contained within sampling units, often coinciding with them. (ibid., 104.) The level of coding unit for this research is that of the *theme*. Themes are particular combinations of words, such as phrases, sentences, or even paragraphs. Using the theme as a unit of analysis introduces some caveats. First, the same theme may be referenced in different ways and with different configurations of words. Further, references at times occur very subtly, or not overtly at all. (Rich et al. 2018, 181–182.) The themes listed below are certainly complex, and contain various subsets of concepts (for instance, “Strategic Intelligence” predicates a set of component functions). The primary sources themselves are by design communications from the intelligence community level to stakeholders and the public (NISs) and from the legislative branch to the general public (SSCI reports). Subsequently, these messages must be unambiguous enough to convey political objectives to these audiences. While the theoretical framework of this study helps operationalize the themes with substantive content, it also illustrates how much intelligence-contextual information hides behind the appearance of concepts and sentences.

The coding categories on level of institutional curriculum were assembled deductively based on recurrent themes in research literature, and inductively based on recurrent themes in primary data. Since the coding scheme had to be built from the ground up, this resembled open coding, in which the researcher breaks down data and builds a list of codes and categories attached to the text. (Rietjens 2014, 133–135). As the institutional curriculum is posited to function as an interface of both the globalization of intelligence and the universities-security-intelligence nexus, the coding units addressed in the analysis were ultimately narrowed down to *Improvement of Analytic Tradecraft and Intelligence Analysis* and *Strategic, Disciplinary, and Scientific Knowledge*, as they bridged more clearly with the contents of the programmatic curriculum as operationalized below. Table 1 lists the final coding units and subsets of themes for the institutional level of curriculum.

National Security Policy Trends Themes	National Intelligence Policy Trends Operational Themes
Improvement of Analytic Tradecraft and Intelligence Analysis[8]	Strategic Intelligence, Anticipatory Intelligence, Uncertainty and Probability Estimates, Cyber Threat Intelligence, Information Evaluation, Standardization of Analytic Tradecraft, Analytic Outreach and Outside Experts (OEs), Intelligence Liaison, Analytic and Technological Innovation, Data Analysis and Quantitative Methods, Transparency of Analysis
Strategic, Disciplinary, and Scientific Knowledge[9]	Social Sciences, Humanities, Science, Technology, Engineering and Mathematics (STEM), Languages, Cyber Security, Data Analysis and Statistics, Futures Studies

Table 1 Coding Units for Institutional Curriculum

For the programmatic level of intelligence curricula, Coulthart & Crosston's (2015) framework is applied. In their study, the authors identified three broader knowledge areas across a sample of US intelligence education curricula (see Chapter 3.4.). Within these knowledge areas, intelligence analysis is contained within the category of *procedural knowledge*, which also includes data management, communication, and operational skills. As all these competencies fundamentally overlap with intelligence analysis, they were all elected as coding unit themes for the curricular analysis. A set of codes was incorporated from Coulthart and Crosston as the subcategories for the procedural knowledge theme of *Analysis*, and its operational theme *Intelligence Analysis (Methodologies and Methods)*. (Coulthart & Crosston 2015, 58–60) Moreover, while Rob Johnston's (2005) definition of intelligence analysis as such is not operationalizable, the contents of procedural knowledge category are. The analysis category corresponds with "the socio-cognitive process", including critical thinking, teamwork, and other academic skills, as well as the "collection of methods" which are addressed in most basic courses of intelligence analysis curricula (for comparison, see Systematic Variables in Johnston 2005, 40). Table 2 lists the coding units and subsets of themes for the programmatic level of curriculum. (Coulthart & Crosston 2015, 58–60).

[8] Sources, e.g., Marrin 2011; Gearon 2020; Walsh 2020; ODNI 2014; ODNI 2015a; ODNI 2019; ODNI 2022b; SSCI (2015, 2017, 2019, 2021).
[9] Sources, e.g., Marrin 2011; Gearon 2020; Walsh 2020; ODNI 2014; ODNI 2019; ODNI 2022b; SSCI (2015, 2017, 2019, 2021)

Procedural Knowledge Themes	Procedural Knowledge Operational Themes	Intelligence Analysis (Methodologies and Methods) Theme Subcategories
Data Management	Data collection, Data manipulation	Anticipatory Methodologies, Comparative Analysis Methods, Criminal Intelligence Analysis, Critical Thinking, Cryptanalysis (SIGINT, EW), Cyber Threat Analysis, Data Analysis, Geoinformatics (GIS), Leadership Analysis and Profiling, Open Source Intelligence (OSINT), Political Analysis, Qualitative Analysis, (Social) Network Analysis, Structured Analytic Techniques (SATs), Systems and Simulation, Threat Analysis
Analysis	Intelligence Analysis (General), Intelligence Analysis (Methodologies and Methods)	
Communication	Written Communications, Verbal Communications	
Operational Skills	Interviewing, Espionage Tradecraft, Deception Techniques, Private and Government Investigations	

Table 2 Coding Units for Programmatic Curriculum

After the coding units had been determined and refined, the recording and coding phase took place. *Recording* refers to content analysts interpreting what they see, read, or find and state their experiences in the formal terms of an analysis. Recording acted as initial "reconnaissance" of the primary and secondary data, and the revision of applicable coding categories. *Coding*, in contrast, adopts "observer-independent" rules for this process, that is, various formalized recording instructions. Natural sciences often prioritize the latter by relying on mechanical measurement, but in social research, human interpretative abilities are even more inherent to the process. (Krippendorff 2019, 129.) Both recording and coding of the primary data of this study were performed utilizing Atlas.ti 22, which is a qualitative analysis software based on coding with user-defined sets of codes. All primary data were compiled in the software, and the coding categories shown in Tables 1 and 2 were used to analyze the data. Initially, a too wide set of codes emerged at the theoretical level of globalization of intelligence, including the two themes of Strategic Environment and Democratic Oversight and Accountability. The themes were especially prevalent in the contextual Chapters 3.1. and 3.2., but their inclusion would have ultimately distracted the content analysis from the intelligence analysis content sought in the curricula. This demonstrates the challenges of a more iterative and inductive conduct of content analysis.

The researchers performing the coding, the coders, benefit from intercoder reliability, which is the interaction and consensus achieved across multiple analysts performing the coding phase (Rich *et al*. 2018, 189). The rigor of intercoder reliability is not achieved in single-coder studies such as this one. The coding instructions here, however, are *replicable* with

more robust data and the analysis is, in principle, reproducible with multiple researchers. Further, another condition for coder reliability in this research design is a sufficient understanding of the American intelligence context. The necessary contextual knowledge to achieve this coder criterion should be, in theory, explicit in the following literature review chapters. However, intelligence scholars with different levels of expertise might draw different inferences from the data and come up with insights and observations that are excluded here. (Krippendorff 2019, 281–283.) Consequently, the most significant weaknesses of the research design applied here concern the coding, which is inherently limited by the coder's contextual knowledge and understanding of the researched phenomenon. Important coding categories may have been overlooked, and reliance on the theoretical framework while working on the analysis may lapse into more subjective interpretations. (Schreier 2012, 31–32.) Further, the qualitative reduction of data into inferential propositions may lose important nuances along the way or be distorted by cognitive biases, just as intelligence analysis does (Whitesmith 2019).

The *validity* of content analysis refers to the quality and truthfulness of the results, regarding the phenomena that are observed. Validity is judged by scrutinizing the inferences drawn from the data against independently available evidence, separate observations, competing theories or interpretations, or of being able to inform successful actions. Out of the three types of validity applied to content analysis, *face validity* refers to the nebulous, but ever-present "common sense" and consensus of judging published results publicly. *Social validity* arises from the research findings contributing to public discussion of important social concerns. Social validity, for instance, is attractive to many organizations that fund research. Finally, *empirical validity* "is the degree to which available evidence and established theory support various stages of a research process", and how specific inferences withstand additional data, or the findings of other research efforts. Empirical validity also includes the "internal validity" of the research process and its logic, which may be challenged and critiqued by outside observations and evidence. Moreover, the empirical validity of content analysis can be measured by different correlation metrics that are not applied here. Empirical validity cannot account for the significance of face validity (intuition) or the social, political, and cultural factors that influence social validity and peer reviews. (Krippendorff 2019, 361–363.) This study rests on these three facets of validity, whose realization is evaluated in the concluding Chapter 6. To complete the content analysis research cycle, Chapter 5 presents the final analysis of the study, reducing the data to main findings and

illustrating the inferential logic used. In Chapter 6, the findings are narrated as the main arguments.

3. THE UNITED STATES AND THE GLOBALIZATION OF INTELLIGENCE

3.1. The Rise of the United States Intelligence Community

In this chapter the historical evolution of American intelligence, mostly in the 20th century, is described. The structure, oversight and tasks of the contemporary intelligence system are examined to provide a picture of the role of intelligence behind the ideas that contextualize and influence the institutional and programmatic curricula of intelligence education. More specifically, the objective of this chapter is to ground the theoretical framework to the globalization of American intelligence, and the resulting global dynamics that influence national security policies. The historical developments guide the research towards the first research question: what kind of themes arise as expectations for intelligence analysis for the institutional curriculum of intelligence education?

The history of the United States Intelligence Community is that of incremental development – capability-wise but also in terms of legislation and statutory role of the respective agencies. Starting from the centralization process of intelligence of the late 1940s, numerous statutes have clarified the role and remit of each agency, and the relationship of the executive and legislative branches of government. These items of legislation have increasingly brought the IC agencies under congressional and intra-agency oversight. As intelligence successes and baseline work are seldom publicized, American intelligence history may appear marked by scandals, controversies and intelligence failures. And since most of the American intelligence community's analysts are located within the Central Intelligence Agency (CIA) (Johnson 2008, 336), so does the agency enjoy prominence in this account.

The usual narrative of American intelligence history begins with the Revolutionary War (1775–1783), during which the Continental Congress frequently utilized intelligence. Intelligence, then, was collected mainly from human sources by George Washington and his generals. These leaders constituted both the analysts and end-users – something of an affront in today's standards. (Tidd 2008, 6.) During the time of Revolutionary War, American military intelligence played an important role in securing victory from British forces in 1781, although the capabilities were rudimentary. Washington had created the Secret Committee and the Committee of Secret Correspondence to surveil British troop movements, perform covert activities, and conduct negotiations with foreign governments. Washington also

employed in his service a team of spies, the Culper Ring, for human intelligence (HUMINT) purposes. In 1776, Congress passed the First Espionage Act, making spying and espionage punishable by death – essentially, to safeguard sensitive information from British eyes. Despite Britain's veritable and pioneering history in intelligence matters, the lacking implementation of battlefield intelligence proved costly in the Revolutionary War, with the defeat of the British. (Jensen et al. 2018, 34–36.)

The role and scope of American intelligence grew again during the times of Civil War, during which both the Union and the Confederacy utilized intelligence diversely. Human intelligence operations included agent networks set up by the South while the North enjoyed counterintelligence successes. Classical reconnaissance was conducted by the cavalry and hot air balloons were also used. The use of signals intelligence (SIGINT) emerged through flag signaling systems and code breaking. (Tidd 2008, 8.) The North prevailed in composing an intelligence organization with the help of Allan Pinkerton's Pinkerton National Detective Agency. While George Washington had extensive military experience and could produce assessments for his organization, Abraham Lincoln lacked such background. Starting from 1861, Lincoln drew from the expertise of General George B. McClellan, a Mexican War veteran, who in turn summoned his old acquaintance, Allan Pinkerton for aid. (Jeffreys-Jones 2003, 24–25.) Thus, the Civil War's first proper intelligence organization was established. Additionally, in 1863, the Bureau of Military Information (BMI) was created by General Joseph Hooker, commander of the Army of the Potomac, to serve as a prototype all-source intelligence unit in contemporary terms (Tidd 2008, 8). Pinkerton's estimates on Confederate troop strength, however, turned out to be often greatly exaggerated, affecting Union's war effort. According to the intelligence historian Rhodri Jeffreys-Jones, Allan Pinkerton, nevertheless, was a formative influence on the American espionage enterprise, with Pinkerton's "definition of the role and character of the undercover operator". (Jeffreys-Jones 2003, 24–25, 43.)

Before World War I commenced, The Office of Naval Intelligence (ONI) was established in 1882 and the Army's Military Information Division (MID) in 1885. Both cumulated information and disseminated intelligence to other government departments and Congress. Whereas during the late 1800s peacetime intelligence was accepted and consolidated, World War I brought with it permanence and specialization. (Tidd 2008, 9–10.) The Federal Bureau of Investigation's (FBI) precursor, Bureau of Information was founded in 1908. An unnamed sibling, the obscure U-1, was established after President Woodrow Wilson saw the need for

the State Department to take a more active role in intelligence matters. Before American entry into the war, the Department of State's new counselor, Frank L. Polk, started coordinating foreign intelligence activities – for instance establishing liaison with the British and French embassies. (Jeffreys-Jones 2003, 60–64.)

In 1914, European radical anarchism had spread to the United States with a series of bombings occurring. This led to the Bureau of Investigation (BOI) commencing the Palmer Raids, culminating in 1919 mass arrests, detainment, and deportations of immigrants. Jensen et al. (2018, 38–39) argue that retrospectively, this precedent influenced later mentalities of xenophobia, nativism, and racism against immigrants – especially regarding the future Red Scare. Although the US understood the need for intelligence capabilities after World War I (and had established a joint cryptanalysis Cipher Bureau between State Department and the military, which was shut down in 1929), intelligence came to be viewed with precarity. Even after the success of World War I, the US refused to establish a peacetime intelligence agency. (Jensen et al. 2018, 40)

The Japanese attack on Pearl Harbor in 1941 took the nation by surprise. President Franklin Roosevelt's disinterest in SIGINT collection has been attributed as one of the reasons for such a strategic surprise. Though war preparations included the organization of intelligence, the intelligence community proved to be in a fragmented state. The Office of Strategic Services (OSS), a vast intelligence agency equipped with 24,000 employees at best, was founded in 1942 to handle foreign intelligence and improve the intelligence capability. FBI, on the other hand, investigated German subversive action such as the Operation Pastorius Ring which had planned on sabotaging American infrastructure targets. Anglo-American intelligence efforts achieved critical success. British cryptanalysts of the Project Ultra led by Alan Turing managed to break the Nazi cipher used in the enigma machines. (Jensen et al. 2018, 42–45.) This liaison laid the groundwork for a significant SIGINT agreement (UKUSA) between the US and the UK that lasted through Cold War (Warner 2014, 143).

As the OSS was disbanded after the war, a new organization for intelligence structure was needed in the forebodings of Cold War. After significant deliberations, draft legislations and presidential impetus, American intelligence apparatus were centralized under the Central Intelligence Agency in 1947, from the agency's prototypical predecessor, the Central Intelligence Group (CIG). The National Security Act was passed July 25th, 1947 and signed into law the next day by President Harry S. Truman. For the first time, a statutory mandate

for centralized US intelligence was created. This meant that for the traditional military and law enforcement agencies, a new coordinating authority under the executive branch and the National Security Council (NSC) was introduced. The priority for CIA became advising the NSC on intelligence matters. (Durbin 2017, 63, 86–87; 89)

The expanding of CIA budget and covert operations at the cost of analysis functions and political accountability described the time of Allen W. Dulles as the CIA Director from 1953 to 1961. During that time, the CIA was perceived as a container of revolutionary threats around Central Europe, Middle East, Africa and Southeast Asia, East Asia, and Latin America. The communist takeover of China, Soviet encroachment on Eastern Europe and the Korean War of 1950–1953 catalyzed more aggressive (covert) foreign policies during the presidency of Dwight D. Eisenhower. In 1953 and 1954 the CIA enjoyed the "success" of overthrowing the regimes of Iran and Guatemala – operations which were publicized only much later. The desire for congressional oversight grew during the late 1950s, as oversight subcommittees of the Armed Services and the Appropriations committee were formally established in the Senate. An intelligence subcommittee was authorized by the Armed Services committee. In the 1950s, CIA ultimately became an independent bureaucracy, with its mostly unchecked resources and policy preferences for conducting secret foreign policy. As Harry Ransom describes, the CIA failed to create a true intelligence community, and the intelligence system became more fragmented. (Ransom 1984, 205–209.) Despite this, during the 1950s, other elements of the intelligence community were strengthened. Importantly, the National Security Agency (NSA) was founded in 1952. The NSA was designed to improve codebreaking, oversee US defense communications security, and reduce competitive duplication between different SIGINT actors. A large network of listening posts with global coverage was organized for the agency. (Jeffreys-Jones 2003, 175.) Eisenhower had learned the significance of SIGINT and IMINT during his experiences of the Second World War, and contributing to the latter, he approved the Lockheed U-2 aerial reconnaissance plane program. The operational use of the U-2 became a success, providing unprecedently detailed intelligence on Soviet infrastructure. (Andrew 1995, 201; 222–224.)

The notoriously botched Bay of Pigs operation started with flawed CIA assessments of Fidel Castro's Cuba being susceptible to political uprisings. In April 1961, some 1450 CIA-trained rebels of Brigade 2506 landed in Cuba but failed to succeed in mobilizing the masses or making military gains. Yet Premier Nikita Khrushchev was convinced that the US would

overthrow Castro with military force and wanted to deter such expeditions. The Soviet Union deployed 50 000 troops and armaments such as anti-aircraft batteries, patrol boats, fighter jets, bombers and missiles fit to carry nuclear warheads at the intermediate and medium range. In October 1962 the US captured concerning IMINT on weapons systems whose range encompassed nearly all the United States. Largely thanks to the Soviet defector Oleg Penkovsky's intelligence, the American administration had room to consider their options more carefully, as he had provided advance information of Soviet Medium (MRBM) and Intermediate-Range Ballistic Missiles (IRBM) before their deployment. The Cuban Missile Crisis ultimately ended in the Soviets withdrawing the missiles from Cuba, and the US removing Jupiter missiles from Turkey, as well as providing security guarantees. Oleg Penkovsky was tried by a Soviet tribunal and executed for treason in May 1963. (Dylan et al. 2020, 112–117.)

The 1970s saw new intelligence controversies, several parliamentary committee inquiries and subsequent intelligence reform especially regarding the CIA. President Richard Nixon resigned in 1974 in the aftermath of the Watergate scandal, as a burglary attempt at the Democratic Headquarters in the Watergate Hotel was found to be linked to the White House. A secret FBI program COINTELPRO (Counterintelligence Program) that ran from 1956 to 1971 was found to have implemented tactics to disrupt and infiltrate factions such the American Communist Party, Ku Klux Klan, the Black Panther Party, the American Nazi Party, the new left, and women’s rights groups. FBI’s activities in the COINTELPRO were publicized in 1972 after several thousand documents were stolen from an FBI office in Pennsylvania. (Jensen et al. 2018, 54.)

Reforms were initiated from the permanent state bureaucracy, the political executive (White House) or Congress. In 1973, the CIA’s analytical responsibilities were fundamentally reorganized, and then restructured as the President’s Foreign Intelligence Advisory Board (PFIAB) felt that CIA analysis underestimated Soviet weapons development threat. In 1974, a New York Times article by Seymour Hersh revealed that the CIA had assisted in the deposing of Chilean President Salvador Allende. The article series exposed an internal CIA document dubbed as the Family Jewels that listed various CIA abuses. President Gerard Ford’s White House set the Rockefeller Commission to investigate these allegations, and the Executive Order 11905 implemented some of the committee’s recommendations. Congress launched the four reforms of Hughes-Ryan Act of 1974 (strengthening congressional and presidential controls on covert actions), Church and Pike Committee

hearings, the establishment of congressional oversight committees (the 1976 Senate Select Committee on Intelligence, SSCI, and the 1977 House Permanent Select Committee on Intelligence, HPSCI), and the Foreign Intelligence Surveillance Act (FISA) that was passed in 1978. (Durbin 2017, 130–131; 135.) Named after the senator Frank Church, the eponymous committee learned that the CIA had involved its officers in domestic spying against students in American campuses, and systematic reading of citizens' mail in the Operation CHAOS. (Johnson 2020, 83.) Moreover, US intelligence was alleged to be involved in recruiting American journalists and media employees as human sources (assets in CIA parlance); and in Nixon's attempts to block the Watergate investigation, as well as experiments with mind control and interrogation methods of the infamous Project MKUltra (Lester & Rogg 2019, 137).

President Ronald Regan was active in military and intelligence affairs and his administration (1981–1989) increased the respective funding. Though some success was met with the covert support of noncommunist insurgencies known as the Reagan Doctrine (such as American military intervention in Grenada's communist-supported takeover), the administration faced criticism in the 1988 Iran-Contra Affair. The White House had secretly sold arms to Iran and funneled the profits to anticommunist "Contra" guerrillas of Nicaragua. (Warner 2014, 235; Meese et al. 2018, 110.) In 1989, George H. W. Bush was elected President to a moment in time where the Soviet Union's eventual demise was cautiously anticipated. Bush himself had served eight years as vice president to Ronald Reagan, as well as the Director of Central Intelligence (DCI) for one year in 1976–1977 (Andrew 1996, 503–504). Bush's administration and penchant for active diplomacy played a part in the 1989 reunification of Germany and membership in NATO (North Atlantic Treaty Association). The Gulf War of 1990–1991 saw the US leading a coalition of 35 countries to repel Saddam Hussein's Iraqi invasion of Kuwait. Already during Bush's tenure, plans of budget cuts to defense were presented to the Senate budget committee. Succeeding President Bill Clinton delivered on promises of a "peace dividend", and intelligence budget received its cuts as well. Although military spending and personnel numbers were greatly reduced, some have later argued that the defense drawdown was successful in prescient military modernization. (Meese et al. 2018, 112–113; 115; Jensen et al. 2018, 64.)

In the 1980s, the United States had already been drawn to fatal incidents with various terrorist organizations. Of course, the origins of American domestic intelligence had lied in countering subversive forces emanating often from outside regions. Capable forces,

however, had been stirring in many countries during the Cold War, often trained and armed by the opposing superpowers. During the Clinton years it became clear that the Scylla of Soviet-sponsored revolutionary Left terrorism gave way to the Charybdis of fundamentalist Islamist terrorism. In 1993, a lone Pakistani man gunned down CIA personnel in front of the agency's headquarters in Virginia. Several weeks later, a team of al-Qaida jihadists in New York detonated a truck bomb under the Tower One of the World Trade Center. Subsequent fire killed six, and a thousand were injured. In 1998 al-Qaida simultaneously attacked US embassies in Nairobi, Kenya and Dar es Salaam in Tanzania, killing 301 and wounding over 5000. And in 2000, a small boat carrying al-Qaida suicide bombers was detonated near the USS Cole destroyer in Aden, Yemen, killing 17 American servicemen. (Warner 2014, 283–283; Jensen et al. 2018, 61; Hoffman 2017, 89.)

The American intelligence history before the terrorist strikes of 2001, then, highlights the President's role as the key customer of intelligence operations, as well as an institution which directed intelligence priorities and the development of intelligence capabilities. Multiple intelligence failures (Pearl Harbor, Bay of Pigs, and others) as well as controversies of the 1970s Family Jewels expositions shaped the public image of intelligence. The domestic spying scandals of the 1970s brought about the statutory intelligence oversight into the American intelligence system, as civil liberties and privacy were violated. The Congress gained much better visibility into the workings of intelligence.

Though terrorism and subversion recurred as themes before and after the World Wars, the focus of the strategic environment was on the bipolar order and its reflections to affiliated and non-affiliated states and proxies until the dissolution of the Soviet Union. As power in the international system was redistributed and ex-Soviet satellites gained their independence, the superimposed polarity gave way to a differently global world. Emerging technologies in the fields of SIGINT and IMINT of the World Wars and the Cold War transformed both intelligence requirements and collection technologies to more complex and sophisticated systems that grew the scope of analysts recruited to the workforce. The diversity of intelligence needs during the Cold War culminated in all-source requirements for intelligence analysis. Foreshadowed during the Cold War and in the 1990s, a new paradigm for intelligence would emerge, adding layers of more complex intelligence analysis requirements in addition to the continuing relevance of traditional military domain.

3.2. The Global War on Terror and the Contemporary Intelligence Community

Osama bin Ladin, a wealthy Saudi, had been active through the 1980s in organizing resources for the Afghan mujahideen resistance to fight the 1979 Soviet invasion of the country. The CIA had been one of the benefactors of the mujahideen, channeling funds and resources via Pakistan's Inter-Services Intelligence (ISI), though the US government and al-Qaida have been adamant the CIA did not help al-Qaida directly at any point. (Warner 2014, 283.) After the Soviets withdrew from the failed invasion of Afghanistan, bin Ladin turned his grievances into a theologically inspired strand of ideology intended to mobilize disgruntled demographics into a mindset of "clashing civilizations". Indeed, eloquently to some, he depicted a global faith of Islam under siege in his 1996 and 1998 *fatwas*, assigning the United States and Israel the role of antagonists. As a political objective, bin Ladin sought to restore the pan-Islamic caliphate that had perished along with the Ottoman Empire in 1924, framing the aim in a fervently fundamentalist rhetoric. (Hoffman 2017, 95–100.) At least since 1999, before al-Qaida commenced September 11 attacks of 2001, the US intelligence community had suspicions of attacks to come on American soil. It was in the President's Daily Brief of August 6th, 2001,[10] that a strategic warning without a target, date or attack method (although plane hijacking was mentioned) was given, but there was nothing to act on for the security agencies. Furthermore, during the 1990s the US had limited the interagency sharing of law enforcement and intelligence information to safeguard individual privacy with rigorous new rules, referred as "the Wall"[11] (Warner 2014, 284–285).

In the morning of September 11th, one of the four planes hijacked by al-Qaida terrorists crashed in the North Tower of the World Trade Center. A little later, another struck the South Tower. Soon after, a third one hit the Pentagon. The fourth flight was supposedly intended to strike U.S. Capitol or White House, but its passengers struggled the hijackers, and the plane crashed in Shanksville, Pennsylvania. The attacks took the lives of 2973 people.

[10] A declassified excerpt of the brief, titled "Bin Ladin Determined to Strike in US", is partly available electronically, for instance, via The George Washington University's National Security Archive project. In hindsight, the PDB indicated New York as a site for attacks, and implied aircraft hijacking as a possible attack method (The National Security Archive 2004.) These observations highlight the difficulty of assessing multiple, idiosyncratic attack plot clues, and also point to the possibility of intentional deception by the terrorist organization.

[11] These 1995 Procedures were adopted by the Department of Justice, and they altered the 1978 FISA interpretation and were subsequently dubbed as "the Wall" between law enforcement and intelligence officials, separating these investigations. This development also extended to the FBI internally. (DoJ 2006.)

(Jensen et al. 2018, 66–67.) Thus, the American security paradigm changed. US forces launched a large military operation ENDURING FREEDOM to root out al-Qaida in Afghanistan, and to topple the al-Qaida-supporting Taliban regime. Military operations to keep the new Afghan government in place tied American resources in Afghanistan (until the hasty withdrawal of 2021, when Taliban took over again). Intelligence enterprise came to enjoy a resurgent status, with CIA's paramilitary operations playing an important part in tracking down al-Qaida terrorists. Moreover, largely justified by the belief of Saddam Hussein's government developing Weapons of Mass Destruction (WMD), a US-led coalition invaded Iraq in 2003. Saddam Hussein was executed in 2006. Alas, the collapse of Iraq's authoritarian political system resulted in disarray and civil war, fueled by al-Qaida and Iran's policies. (Meese et al. 2018, 119–120.)

The attacks of 9/11 brought about congressional investigation, and immediate reform of the national security and intelligence sector. The intelligence committees HPSCI and SSCI conducted a joint inquiry and concluded that the intelligence community had failed to counter the terrorist threat that had emerged in the 1990s. Surveillance authority was strengthened domestically with the introduction of the USA PATRIOT act (Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism), which passed both Congress chambers overwhelmingly in October 2001. One of the most significant alterations to the American national security architecture since the National Security Act of 1947 was the creation of Department of Homeland Security through the Homeland Security Act of 2002. This new, cabinet-level agency was composed of 22 federal agencies or their elements, totaling nearly 170 000 employees. (Durbin 2017, 211–215; 217.)

The 9/11 Commission's acclaimed report recommended the creation of a strong Director of National Intelligence, the formation of a National Counterterrorism Center (NCTC) to bring together law enforcement, military, and intelligence actors, and declassifying the overall intelligence budget (Durbin 2017, 224). The 9/11 Commission's recommendations, the preceding Snowcroft Commissions's work, and President George W. Bush's executive orders resulted in the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), which effectively made counterterrorism as the priority of the IC. The legislation established the DNI as the head of all IC, and the Office of the Director of National Intelligence (ODNI) as the DNI's support organization. And the compilation of CIA's two prime products – the President's Daily Brief (PDB), and the National Intelligence Estimates (NIEs) – were transferred to the DNI. (Lester & Rogg 2019, 141–145).

The first DNI, John Negroponte, who was appointed in February 2005, quickly realized the limitations the IRTPA legislation had set. ODNI's initial steps were reminiscent of CIA's sluggish start. Negroponte's first six months, however, saw the creation of the first National Intelligence Strategy (NIS), which was connected to the administration's National Security Strategy (NSS). Another initiative was the improvement of the IC's workforce by establishing the National Intelligence University system. Congressional critique towards the ODNI continued throughout its first years, and after Negroponte stepped down as DNI, subsequent DNIs until James Clapper (2010–2017) served for short periods (Michael McConnell 2007–2009) and Dennis Blair (2009–2010). As a response to criticism, President Bush attempted to enhance ODNI's authority with an executive order in 2008. The ODNI's bureaucratic struggles were soon eclipsed by Edward Snowden's revelations, revolving around the National Security Agency (NSA). (Durbin 2017, 239–243.)

Revelations matching the scandal of the 1974 Family Jewels reports saw the light of day in June 2013, as the NSA contractor Edward Snowden's leaks were publicized by The Guardian and Washington Post. Approximately 1,5–1,7 million highly classified American and British signals intelligence and communications intelligence (COMINT) documents comprised the data, detailing intelligence capabilities, methods and partnerships. A prelude to Snowden's leaks had been the 2010 leaks of Bradley (now Chelsea) Manning's 500 000 classified documents distributed via the WikiLeaks platform. Edward Snowden's revelations brought significant public doubt on the intelligence community's ability to safeguard its classified data from "insider threats",[12] but also energized the discourses on civil liberties, privacy and their protection as well. (Durbin 2018, 243–244; Gioe & Hatfield 2021, 704–705; 707.)[13] Snowden's leaks revealed the extent to which the intelligence community had gone in interpreting the USA PATRIOT act, an example being the PRISM bulk collection program. According to a Top Secret (TS) document referred to by The Guardian, the NSA had under the PRISM program collected data from such providers as Microsoft, Google, Yahoo!,

[12] Damage factors of such intelligence breaches may include lost lives, compromised sources and methods, the costs of replacing lost collection capabilities, economic or reputational damage done to relevant institutions of corporations, stunted employee morale, redirected personnel resources for damage assessments, and various geostrategic disadvantages (Gioe & Hatfield 2021, 729).

[13] These debates have popularized the association of intelligence collection with mass surveillance. The discourses have also animated the nascent Surveillance Studies subdiscipline of sociology and various other social sciences that conceptualize 'surveillance' as a far more essential and ubiquitous, intersubjective phenomenon that underlies any society (see e.g., Haggerty et al. 2012).

Facebook, PalTalk, YouTube, Skype, AOL, and Apple – many of which denied having had knowledge of such collection (Greenwald & MacAskill 2013).

The then-DNI, James Clapper, was tasked by President Barack Obama to counter the narrative of an all-powerful mass surveillance state with a trove of declassified documents that were later organized on the website *IC on the Record*. According to Timothy H. Edgar's account,[14] the administration sought a "Big Transparency" approach in declassifying intelligence records and not only relying on exhausting current FOIA (Freedom of Information Act) cases. (Edgar 2017, 81–82.) Whereas the Pentagon called the Snowden leaks the biggest theft of US secrets in history (Strohm & Wilber 2014), and the damage to the collection systems was certainly unprecedented, Edgar argued that the Snowden revelations made the NSA more transparent, accountable, (ironically) more protective of privacy, and ultimately, more effective (2017, 5). In the end, NSA's and FBI's transgressions were brought under controls with the USA Freedom Act of 2015, which limited the types of data the NSA could collect about Americans (Durbin 2017, 244).

President Donald Trump's (2017–2021) relationship with the intelligence community was fraught with mistrust, culminating in the 2022 Mar-a-Lago affair. Indeed, the relationship has been called "consistently uncomfortable and fractious" (McLaughlin 2021, 788). Trump's denial of Russian interference in the 2016 presidential election and references to "deep state" enemies were not an invitation to cordial relations with the IC. Already in 2017, he had endangered Israeli sources by revealing intelligence to Russian officials. The CIA also had to pull an agent placed in Kremlin due to fears of Trump's White House risking the operation. Moreover, in 2019, Trump insisted on posting a classified satellite photo of an Iranian space launch facility on Twitter on the grounds of presidential declassification privilege. Thus, Trump in the White House was increasingly seen as a security risk to US secrets. (Mazzetti 2022.) During August 2022, the FBI made an additional search at Trump's Mar-a-Lago resort in Florida, seeking documents that contain classified information. Earlier in 2022, Trump had returned some dozen boxes, according to the affidavit, that contained 25 documents marked Top Secret, 92 Secret, and 67 Confidential. Some of the documents were designated HCS

[14] Edgar had worked within the IC for seven years in a team of internal privacy watchdogs. In 2009 was chosen in Obama's national security staff as director of privacy and civil liberties. He had left the government just before Snowden's revelations became public. (Edgar 2017, 3).

(HUMINT Control Systems) and NOFORN (No Foreign Nationals), underlining their sensitivity. (Lowell 2022.)

Joe Biden was inaugurated under the shadow of the insurrection of Capitol Hill on January 6th, 2021, where law enforcement intelligence was blamed for intelligence failures. Later that year, the hasty withdrawal of US forces from Afghanistan drew criticism not only towards the administration, but to intelligence performance as well. According to several CIA, DIA, ODNI, and DoS reports seen by The Wall Street Journal, the IC had optimistically anticipated the Afghan government and Kabul to fall only later that year. The DCIA William Burns, though, responded to the criticisms that the agency did convey the severity of the situation in its reports, if not the precise hour when President Ashraf Ghani fled his office. (Salama & Strobel 2021, McEvoy 2021.)

The Russian invasion on Ukraine starting in February 2022 has seen surge of intelligence liaison and public dissemination of intelligence as international policy. Moreover, the conflict has so far showcased the might of the American intelligence prowess in a conventional military conflict. Indeed, for the Americans and Ukrainians as well, the strategic warning of US intelligence was precise and actionable. What is remarkable about the intelligence dimension in the Russo-Ukrainian war is the scope of 'intelligence-led communications' that are calculated, accessible, and sanitized releases of information, such as the UK Defence Intelligence "intelligence updates" that describe daily developments in the Ukrainian theater. Actual raw and finished intelligence has been disclosed as well, especially in the imagery intelligence and signals intelligence domains. The various bodies disseminating intelligence to the public dimension in the war from confidential briefings to social media updates rely on the power and authority of intelligence to, for instance, expose Russian false-flag operations. (Dylan & Maguire 2022, 34–37.)

Moreover, the conflict has again mobilized the cadres of OSINT (open source intelligence) analysts, investigative journalists and intelligence pundits to produce original analysis for public audiences and the media. Although careless reporting of Ukrainian activities in the conflict zone may reveal troop movements and jeopardize Operational Security (OPSEC), OSINT investigators have developed respective codes of conduct for their analysis. These informal ethical guidelines and verification techniques have advanced since the OSINT surge of Russian annexation of Crimea in 2014 and the start of the Syrian civil war in 2011. (Perrigo 2022.)

The US Intelligence Community now consists of eighteen organizations, categorized in three groups by the ODNI. The late Jeffrey T. Richelson aptly described the scope of the US IC's activities in his encyclopedic work on the community:

> "Its activities include the collection of information using reconnaissance satellites, aircraft, ships, ground stations, emplaced sensors, computer network exploitation, and undersea surveillance, along with traditional overt and clandestine human sources. It also acquires and exploits open sources, foreign materiel, as well as videos and documents. In addition, its personnel process and analyze the information collected using the most advanced computers and a variety of specially developed techniques for extracting a maximum of information from the data." (Richelson 2016.)

Two organizations are independent agencies (the ODNI and the CIA), and nine are Department of Defense (DoD) elements (including the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial-Intelligence Agency (NGA), and the National Reconnaissance Office (NRO))[15]. Seven are elements of other departments and agencies, including the Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Agency's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis). (ODNI 2021.)

The highest government authority at the executive level directing US intelligence efforts is the National Security Council (NSC). The NSC and the president work on the national security strategy and national foreign intelligence objectives and priorities, producing guidance for the intelligence community. The intelligence community is headed by the Director of National Intelligence (DNI), a role established in the Intelligence Reform and Terrorism Prevention Act of 2004. The DNI is situated in the Office of the Director of National Intelligence (ODNI), as is the National Intelligence Council (NIC), established in 1979. The director is the principal advisor to the president and the NSC in matters of national security intelligence. (Meese et al. 2018, 260–261.) There are two intelligence programs that define the US IC's efforts. The National Intelligence Program (NIP) financially supports the activities of the CIA and is controlled by the ODNI. The Military Intelligence Program (MIP) is controlled by the DoD and funds the military entities involved in national security intelligence

[15] The rest of the organizations are the intelligence elements of the five DoD services: the Army, Navy, Marine Corps, Air Force and Space Force – the last being the latest addition to the family (ODNI 2021).

activities. Moreover, the NSA, the DIA and the NGA operate under both programs. (Lemieux 2019, 56.) According to the ODNI, the bulk of the requested US IC budget for 2022 (as confirmed in Intelligence Authorization Act for each fiscal year) belongs to the NIP ($62.3 billion) and the rest to the MIP ($23.3 billion). The 9/11 Commission recommended the IC to declassify its budget, and the community has done so since 2011 for the NIP and 2012 for the MIP. (ODNI 2022b.)

In the case of the United States, Lester and Rogg (2019) note how intelligence oversight is constrained by structure on the one, and ideology on the other hand. As permanent intelligence institutions are a relatively new creation, the role of intelligence is still evolving. The Executive branch of government retains the ultimate control over intelligence, and Congress has oversight authority. At the ideological level, American liberal tradition conceptualizes individual liberty, freedom of thought, and public participation in government free from manipulation and coercion. These values are often at odds with the fundamentally secretive and intrusive methods of intelligence. Subsequently, the necessary need of trust in Federal government to legitimately withhold information from the public is an enduring cause of tensions between the public, Congress and the Executive branch. (ibid., 135–136.) Covert action has often been in the center of controversies. As a third way between military action and diplomacy, conducted operations can be 'plausibly denied'. It was only in the 1970s when the Hughes-Ryan amendment to the Foreign Assistance Act of 1961 required the President to sign a memorandum of covert action (a 'Finding') and send it to Congress whenever such action was considered (Lester & Rogg 2019, 137).

The current oversight system for the US IC, as said, was institutionalized in the 1970s at the level of Congress. Several other entities have been established since. The House Permanent Select Committee on Intelligence (HPSCI) is now composed of 13 members of the governing majority of the House of Representatives and 9 members of the governing minority. The HPSCI regularly holds hearings with all intelligence community agency members, and its subcommittees[16] address intelligence policies, programs, activities, and budgets. The Senate Select Committee on Intelligence (SSCI) includes eight members of the governing majority of the Senate, as well as seven members of the governing minority.

[16] The subcommittees are the Strategic Technologies and Advanced Research (STAR) Subcommittee, the Counterterrorism, Counterintelligence, and Counterproliferation (C3) Subcommittee, the Intelligence Modernization and Readiness (INMAR) Subcommittee, and the Defense Intelligence and Warfighter Support (DIWS) Subcommittee (HPSCI 2022).

The SSCI oversees and studies intelligence activities and programs. Its activities include mostly closed session hearings, annual legislation to authorize the IC funding, among other oversight tasks. (Lemieux 2019, 56–60.) The Privacy and Civil Liberties Oversight Board is an independent entity in operation since 2007 and includes five bipartisan members nominated by the President and confirmed by the Senate. Its focus is on the protection privacy and civil liberties regarding counterterrorism legislation, activities and policies. The Office of the Inspector General of the USIC (IG-IC) was established in 2010 through the Intelligence Authorization Act. Its tasks include audits on the whole IC, investigations on different risks, vulnerabilities and deficiencies that affect the IC. The IG-IC reports to the Congress on intelligence effectiveness, fraud and abuse of intelligence. It also operates a hotline for whistleblowers and offers legal protection to IC employees and contractors. (Lemieux 2019, 60.)

From the overview above, several key national security policy trends arise that illustrate the expectations towards the institutional curriculum. The terrorist strikes of 9/11 reformed the IC and scrutinized intelligence analysis unprecedentedly. It was perceived as an intelligence failure and the resulting reform was profound. The strikes established a new paradigm for intelligence which had to take into account a qualitatively different threat (Treverton 2009). Intelligence powers were strengthened, and controversial collection programs were established. The recruitment of new workforce was also accelerated with government initiatives, as is discussed below in Chapter 3.3. The Snowden revelations of 2013 energized the global discourse on intelligence oversight, privacy and civil liberties and commenced a new wave of transparency policies to the conduct of the IC. The disclosures also revealed the depth of global intelligence liaison. Along with the related reforms, the US intelligence system has evolved into its current iteration.

While this subchapter has described national security and intelligence in contemporary terms, and the problematics of the overt and covert modes of action, it has so far overlooked the “universities” and “nexus” of the universities-security-intelligence nexus component of the theoretical framework. As said, the universities-security-intelligence is the interface where intelligence requirements and expectations meet academic pursuits. While these paths have often converged, the clearest divergence is the purpose of knowledge. Intelligence looks for knowledge useful for protection against threats against national security, whereas the consideration of science, in for instance climate and sustainability

studies, is to map the scenarios that affect all of humanity. Below, the domains of the universities-security-intelligence nexus are sketched.

3.3. Intelligence Education in the United States

As intelligence and its many aspects are increasingly globalizing, courses and programs in intelligence and intelligence analysis are now commonly featured in many higher education programs across the world. The United States is a fitting laboratory for such development, as the government-funded IC CAE program and other initiatives support intelligence education efforts generously. The phenomenon of increased intelligence teaching in higher education itself is a relatively recent development in the United States. Prior to the events of 9/11, only two civilian[17] universities offered programs in intelligence, although between 1985–1999, the number of non-government higher education courses on intelligence had increased from 54 to between 200 and 300. In 2009 that number had risen to at least 845. (Landon-Murray & Coulthart 2020, 270; Campbell 2011, 308). The number of actual degree programs that integrate intelligence studies has been estimated to range over 100 as of 2022, including 73 IC CAE-funded institutions (Ramsay & Macpherson 2022, 5). Institutions of higher education acclimate themselves to geopolitical changes to supply relevant programs and courses. Whereas 9/11 has been a watershed moment for the expansion of Security Studies research (Buzan & Hansen 2009, 227), and intelligence education in general, earlier examples include the growth of Russian studies programs during the Cold War, the proliferation of science and engineering majors (encouraged by the government) following the Soviet launch of the Sputnik satellite in 1957, and the increase in Arabic language programs after 9/11 (Dujmovic 2017, 939.)

According to Loch K. Johnson's overview on CIA-academia relations, most members of the academia tolerate at least open and voluntary relationships between intelligence officers and scholars, secret relationships between university staff and government agencies are considered inappropriate. (Johnson 2020, 81–84.) In the research setting, however, it is nevertheless reasonable to keep sensitive information secure for contractual and

[17] In addition to civilian paths to intelligence analysis education, the National Intelligence University (NIU) provides degrees for employees of U.S. Armed Forces or the federal government. Other criteria include being a US citizen, and that of holding an active TS/SCI (Top Secret/Sensitive Compartmentalized Information) clearance. (NIU 2022.) Students within the NIU have the advantage of studying in a classified environment. Such a setting will allow the students to get used to similar systems they would use as an analyst within the IC (Parsons 2020, 279–280).

counterespionage reasons.[18] There is also a clear difference between voluntarily counseling and advising intelligence agencies out of the sense of friendship, patriotism, ideology, status etc. and engaging in a hidden *and* paid relationship. As to university campuses acting as recruiting grounds for potential workforce, Johnson says that some universities allow CIA recruiter presence if done openly in "Career Day" settings. Some universities, on the other hand, have outright banned intelligence operations from being carried out in campus grounds (for all the good such a ban does) – to keep university atmosphere free and open and devoid of intelligence presence. While sometimes CIA has attempted to recruit faculty members to gather intelligence abroad and contribute to overt propaganda writing against foreign adversaries, Johnson argues that government meddling with scientific publication risks the staining of credibility and the very notion of academic independence, a practice not in place in democratic societies. (Johnson 2020, 84.) Regarding the presence of CIA and other 'spooks' around US institutions of higher education, Johnson concludes that statutory guidance – that is, legislation – could in theory be put in place to properly define the relationship of academics and intelligence officers in such sensitive environments (Johnson 2020, 91–92).

A set of studies has examined the intelligence education programs in the US in the past decade. Campbell (2011) identified a common inventory of intelligence education textbooks (many of them occurring on the pages of this study as well). He noted that the previous decade had already seen significant progress, and anticipated growth in the trends of intelligence-specific study programs, web-based distance courses, and the increasing standardization of intelligence tradecraft as recommended by the 9/11 and WMD Commissions. (Campbell 2011, 310–311; 330.) Landon-Murray (2011) studied a sample of security and intelligence studies program curricula and found their incorporation of advanced theory and modeling and methods light at the graduate level. He also noted that it would be important to understand how responsive academic programs are to the needs of the intelligence community, to not transmit some "pathological" tendencies to the academia. (Landon Murray 2011, 511–512.) In another article Landon-Murray (2013) called attention to shifting the unit of analysis from intelligence education programs to systems and sets of programs that "funnel graduates into the IC". He recommended that academic

[18] In the academy (as well as business and government sectors), China is increasingly implicated in various espionage activities. The British MI5 and FBI heads Director General Ken McCallum and Chris Wray issued a joint address in July 2022, warning of Chinese covert theft, technology transfer, and exploitation of research (MI5 2022, FBI 2022).

programs and professional development of intelligence analysts be harmonized, as the IC had no uniform training and education program across organizations. He also drew attention to the inclusion of human capital officers' and analytic managers' perspectives in the intelligence education literature. (Landon-Murray 2013, 769–771.) Landon-Murray and Coulthart (2016) compiled a sample of prominent civilian intelligence teachers' perspectives on the role of tradecraft and training aspects in their teaching programs. The interviewees argued that by including some facets of intelligence training and tradecraft, academic programs could provide venues for future practitioners to get sensitized to limits and gaps in tradecraft. Social scientific foundations could then be better connected to professional practice to counter the deficits of IC training. (Landon-Murray & Coulthart 2016, 16.)

Walsh (2017b) discusses how intelligence curricula are designed in the United States and across the Five Eyes (FVEY) partner countries (Australia, Canada, New Zealand, United Kingdom, and the US). He argues that the education component in the intelligence discipline has no evaluation research agenda in place and proposes a normative framework for such endeavors. Walsh utilizes five broad themes of training and education: curriculum, accreditation, continuing professional development, teaching and learning and finally, content and assessment (2017b, 1006). As to intelligence education curricula, Walsh points out that educators often design curricula based on their own values judgments, as opposed to clear evidence from research. This kind of normativity appears to derive from the educators' professional experience, worldview and contextual understanding of analytical skills, competencies, and knowledge – leaving certain content-related judgments hidden. Likewise, other variables than the educator's values judgments influence curriculum development, including what the current political leadership perceives as important, how the security environment has changed, and the role of technology. Finally, curriculum design itself cannot cater for the needs of every national intelligence community agency, let alone across such international communities such as the Five Eyes. (Walsh 2017b, 1006–1007.)

More recently, Johnson has agreed that two scholarly discussed main orientations in American intelligence education still exist. The 'theoretical' approach would seek to understand intelligence in the context it operates: foreign affairs and national security policy, and how intelligence informs government. Without going too deep into analysis practices themselves, this approach would rather educate students on such dynamics as politics, successes and failures, oversight, the history of collection and analysis, counterintelligence, and covert action. The practice-oriented approach would, on the other hand, teach students

to write intelligence products, and to utilize intelligence gathering and analysis methods. Often former intelligence officers act as instructors at these centers. Johnson points out that connecting the abstract and clinical sensitivities of these approaches may prove to be a challenge in the US, as the teaching of detailed intelligence tradecraft would require more former intelligence officers in the universities' payroll. He does, however, remark that a third model in the form of an intelligence studies bachelor's degree has been developed in the Norwegian Defence Intelligence School (NORDIS) – although only professionals are allowed to enroll in the program. (Johnson 2020, 87–89.) An instructor based in the same program has illuminated in a written piece on how the NORDIS model has utilized a combination of Structured Analytic Techniques (SATs), creativity, critical thinking, and sensemaking to create a distinct methodology for intelligence analysis (Borg 2017, 2; 11).

Johnson also references to the 'ideal intelligence program' ideated and assembled by the retired CIA officer Nicholas Dujmovic in the Catholic University of America, where intelligence would not comprise a full degree program (2020, 89–90). In a 2017 article, Dujmovic writes that he based the curriculum creation process on the prospects of employment for the graduates and not just the academic staff and thus, "what the intelligence agencies actually need and want". Dujmovic's two main CIA interviewees said they preferred graduates in substantive fields instead of undergraduate majors in intelligence, but they also wished that new analysts should have sufficient background knowledge about the historical side of intelligence. He emphasizes how interviewees from the US IC at large also favored graduates from other fields than intelligence. Candidates with degrees from specific intelligence analysis programs also supposedly do not stand out from their contemporaries, as intelligence agencies would prefer to teach analysis in-house. Dujmovic argues that ultimately, any academic student's major subject should provide the essential qualities of critical thinking, argumentation and analysis also sought by intelligence employers. To understand intelligence, he maintains, the topics of collection, analysis, counterintelligence, covert action, and accountability – as included within his program – should suffice. (Dujmovic 2017, 937–940.) Long-term analyst, researcher, and instructor of intelligence Mark M. Lowenthal has also presented a similar view that intelligence studies themselves do not comprise a major subject if one wishes to get employed as an analyst, but intelligence nevertheless serves as a normal function of government, shared by all political systems across the globe (Lowenthal 2017, 986–987).

Dujmovic's and Lowenthal's arguments are sound from the perspective of those who strictly want to get employed as intelligence officers for US government agencies. The discussion, however, seems to overlook the fundamentally *academic* pursuits of teaching and researching intelligence. Ben Jaffel *et al*. point out that Intelligence Studies (IS) has rather engaged in theorizing for the needs of intelligence services than *of* intelligence as a social phenomenon, with IS remaining a "prisoner of its state-professional lineage" (Ben Jaffel et al. 2020, 325). This bias on research (which is rather apparent judging from the literature featured in this study as well) is likely connected to the fact that many of the prominent authors on IS are themselves former practitioners of intelligence or have been closely affiliated with insider-like environments. In addition to delving into the ontological and epistemological fabrics that envelop intelligence and intelligence-making, scholars have many other academic motivations to research the subject. As for any societal subject, it is necessary for the academia to research intelligence to expand public understanding and accountability of a more elusive, and unnecessarily mystified, subject. Declassified data on, for instance, intelligence history, also helps to place the significance of intelligence to a historical context (Andrew & Dilks 1984). Current and aspiring intelligence analysts, and intelligence scholars notwithstanding, Riehle observes that other possible audiences for intelligence studies programs simply include anyone who wishes to improve critical thinking and analytical skills. And the skills entailed in such programs are also applicable, he continues, in banking, law enforcement, and business risk analysis amongst other careers. (Riehle 2021, 75.)

This subchapter has displayed some dynamics of the operational, epistemological, and ethical domains of the universities-security-intelligence nexus. As for the operational and ethical domains, the dynamics of overt and covert collection on campuses has been described vis-à-vis the historical background already addressed in Chapter 3.1., where CIA's operation CHAOS was described as a historical source of suspicion, among other concerning instances. The transparency and openness of the academic environment are at odds with the covert conduct of intelligence, and it seems (workforce-related) recruiting presence is relatively tolerated, if conducted in a professional sense. And of course, academics conduct classified research and consult national security agencies willingly. As for the epistemological domain, the discussion about the "ideal" intelligence program indicates that substantive, disciplinary knowledge has many proponents in the IC, especially CIA. Interestingly, the academia is also interested in intelligence as a cultural, political, and

social phenomenon – a notion that seems overlooked in many of the scholarly discussions. The following subchapter 3.4. takes a closer look at the IC CAE program's modus operandi.

3.4. The Intelligence Community Centers for Academic Excellence Program

The Intelligence Community Centers for Academic Excellence (IC CAE) program was established in 2005 to meet the national demand for professionals in national security. The intent of the program is "to increase the pool of competitive, diverse, applicants, and to increase awareness of the IC mission and culture throughout ethnically and geographically diverse communities". Its planning and implementation adhere to the guidance set forth in the National Security Act of 1949, the Intelligence Authorization Act of 2004, and the 2019 National Intelligence Strategy. In practice, the program seeks to foster a community of scholars and IC professionals by awarding them grants to create integrated programs through partnerships with the IC. (ODNI 2020.) A 2019 figure from fiscal year 2005 and projected to fiscal year 2021 totaled approximately $69 million dollars of funding for the IC CAE program. The ODNI served as the IC CAE program manager from 2005 through 2011, until the DIA took over in 2011 by appointing the program executive, whereas the budgetary oversight of the program was left to ODNI. The management of the program transitioned back to ODNI in the fiscal year of 2020. (GAO 2019, 1; 40–42.) The IC CAE universities can be divided to two groups, the Grant Receiving Institutions and Legacy Institutions. Legacy institutions are defined as "any IC CAE Program that continues to meet criteria as defined in the Funding Opportunity Announcement on institutional diversity, program management, event management, faculty development, and curriculum after it has completed its grant period of performance; with the strategic intent to create a diverse, skilled, and knowledgeable scholar ready for hire in the Intelligence Community." (ODNI 2022a.) The IC CAE grant applicant institutions can apply as lead/independent institutions, a lead institution in a consortium, or a partner institution. (Landon-Murray & Coulthart 2020, 273).

The IC CAE program was first piloted at Trinity Washington University in Washington, D.C., as per the Intelligence Authorization Act for Fiscal Year 2004, which directed the DCI to "develop a pilot project to test and evaluate alternative innovative methods to promote equality of employment opportunities in the IC for women, minorities, and individuals with diverse ethnic and cultural backgrounds, skills, language proficiency, and expertise." (GAO 2019, 5.) The efficacy of the program has had a mixed congressional response. The Senate

Select Committee on Intelligence oversight reports that also contain the public provisions of the Intelligence Authorization Acts for each fiscal year shed some light on the success of the program in eyes of the Committee. The SSCI said in its 2011 oversight report (2009–2011) that it spent "considerable time examining the progress and status of a wide range of educational, training, and scholarship programs within and associated with the Intelligence Community" (SSCI 2011). In the 2013 (2011–2013) oversight report, the Committee said it had met with Program Directors and managers of IC CAE and other IC-supported "on at least annual basis" (SSCI 2013).

On a more critical note, the Committee's additional 2019 report remarked that the IC had "apparently ceased" to collect and analyze demographic, educational, employment and other data about involvement in the IC CAE program after 2009. The Committee also reported that the ODNI and DIA had informed the HPSCI that the "IC currently cannot provide statistical evidence as to whether the IC CAE program is fulfilling its objectives." The Committee directed the ODNI to resume such data collection and requested the Government Accountability Office (GAO) to conduct a review on the program. (SSCI 2019b.) The GAO audit, published in August 2019 and conducted between August 2018 and May 2019, contains not only essential historical data on the IC CAE program, but assesses the management of the program in years 2011–2019. The GAO concluded that:

> "…the current program manager, DIA, has not sufficiently planned and overseen the program and the IC is unable to determine whether the program has been successful in meeting its goal to create an increased pool of culturally and ethnically diverse job applicants for the IC. Specifically, DIA has not developed results-oriented goals or documented an overall strategy for the program, evaluated external factors that could significantly affect the program's success, defined and collected comprehensive metrics, or conducted an assessment of the program's performance." (GAO 2019, 37.)

The GAO provided seven recommendations for the DNI to address the programmatic deficiencies of the IC CAE, most of which were related to the setting and documentation of results-oriented goals, evaluation, and IC element participation. (GAO 2019, 37–38.) The workforce diversity goals of US IC are included as core values in its *Principles of Professional Ethics for the Intelligence Community*. Workforce diversity is argued to help the IC "combat emergent global, and increasingly complex national security threats" (ODNI 2022c). Certainly, historical sensitivities in racial, gender, and sexual discrimination are so deeply embedded in the United States diversity discourses that they escape the scope of this study. Jeffreys-Jones presents three arguments as to why the beginning of the 21st century marked an incremental change in the demographic make-up of the American

intelligence agencies. First, white male domination was questionably operationally as, for instance, a white man with a Harvard accent seemed out of place in the context of decolonized countries and indeed, continents such as Africa. Second, recruitment of just a narrow segment of the population translated to a less talented pool of workforce. Finally, as an all-inclusive society was becoming an idea accepted by liberals and conservatives alike, exclusionary recruiting outside of minorities (that made up the majority of the American population) was undemocratic. (Jeffreys-Jones 2003, 278–279.)

Gender equality and discrimination against sexual minorities were increasingly addressed during President Clinton's tenure. Clinton's executive order in 1995 banned discrimination against homosexuals in security clearance procedures, allowing openly gay persons to work in the IC. During history, homosexual double agents were allegedly recruited by blackmailing, though Jeffreys-Jones notes that most publicized traitors such as Aldrich Aimes had been overwhelmingly heterosexual. (Jeffreys-Jones 2003, 279–280.) More recently, while sexual minority identities within the IC remain largely obscured, it seems post-9/11 recruits in the IC at large possess a more progressive view on various social identities, perhaps partly independently of the more consciously diverse hiring policies as well. It appears minority representation continues to suffer from a partisan polarization in the political discourse, even if it has progressed remarkable in recent decades. (Nolan 2022, 722–724.) This is evident from John A. Gentry's critical examination of diversity hiring policies in the US IC. According to Gentry, the claim that domestically defined demographic diversity improves the functional performance of intelligence work is unsubstantiated. He remarks that especially during Obama and Biden years, diverse hiring was argued on the grounds of ultimately partisan values but not performance metrics. He concurs with the GAO reports that found the IC's reporting on diversity goals lacking. According to Gentry, some of his IC contacts interviewed for his article said that CIA's experience with the IC CAE program had been unfavorable. (Gentry 2021, 19–20.)

Few academic studies have examined the IC CAE institutions and their outputs. Even fewer have considered the network they form as an instrument of US public policy. For instance, a Scopus query for terms "IC CAE" produced 167 results, most in engineering. With the search terms "Intelligence Community Centers for Academic Excellence", 7 results were found.[19] Landon-Murray and Coulthart's 2020 piece surveyed former IC CAE scholar

[19] This query was performed October 3rd, 2022.

students with a limited sample of 19 respondents, out of whom 36% had gotten employed in intelligence and approximately 13% entered the IC after their time as IC CAE Scholars. Moreover, the authors found certain emerging trends within the program design. First, a significant majority of the programs were established at the undergraduate level (33 out of 49), and even more so were identified minors of certificates (38 out of 49), signaling a possible tendency in the IC to favor minors and certificates over "proper" intelligence studies degrees – being in line with some of the argumentation in the intelligence curricula design debate. Second, a variety of distinct programs focusing on cyber security and other technologically specialized orientations have, for instance, emerged. (Landon-Murray & Coulthart 2020, 270–274.)

Stephen Coulthart and Matthew Crosston's 2015 study on American intelligence programs from 1992 to 2012 identified 17 intelligence programs across the US, most of which were founded after 2005, coinciding with commencing of the IC CAE funding program. The authors established a threefold typology of knowledge areas that defined the course content of these programs: procedural knowledge, core knowledge and domain knowledge. First, *procedural knowledge* would include the likes of data management, analysis, communication, and operational skills. For instance, data management includes the collection and manipulation of data, and the authors did notice an increased emphasis on open source intelligence (OSINT). Analysis, the specific interest to this research, comprises of the general intelligence analysis or alternatively, "research methods in intelligence" and the like, but also skills in critical thinking. The other type of analysis courses includes particular methodologies, such as Geographic Information Systems (GIS) and warning and forecasting methodologies. Communication as part of procedural knowledge addresses the communication of finished intelligence products to customers, as well as written and verbal communications. Operational skills include practical and non-analytical skills in intelligence, such as interviewing and espionage tradecraft, although these techniques usually face limits in civilian educational institutions. (Coulthart & Crosston 2015, 58–61.)

The second pillar, *core knowledge*, would introduce the students to intelligence organizations and processes, historical study of intelligence and ethical and legal issues. According to the authors' categorization, the five main intelligence collection disciplines of HUMINT, OSINT, SIGINT, IMINT (or GEOINT) and MASINT were introduced to students, as well as other intelligence functions such as covert operations and counterintelligence. Moreover, the historical study of Intelligence Studies was included in this category. The third

pillar, *domain knowledge*, consists of the areas of national security, criminal activity, and business, as they are the central domains where intelligence is used and applied. Issues in the domain knowledge category include terrorism, insurgency, civil wars, and cyber security. Regional studies covering almost all areas of the world were also featured in the course content, the Middle East being the most popular. (Coulthart & Crosston 2015, 61–63.)

Another timely study including the IC CAE institutions in its data among others examined the dual question of intelligence education programs living up to professional educational standards, and to which extent intelligence education programs have integrated quantitative analysis courses in their curricula. Ramsay and Macpherson's sample identified 33 graduate programs based on an IPEDS (Integrated Postsecondary Data System) query and 87 current IC CAE grant recipients and legacy institutions, likely representing most of the publicly available graduate-level national security intelligence programs in the US. Out of the programs included in the sample, only 28 met the International Association for Intelligence Education (IAFIE)[20] core areas criteria, and with the addition on covert action, only seven met all the educational categories. Moreover, the authors found, that only 8 IC CAE programs met the criteria of the study, signaling a lack of maturity in educational content. Finally, only 6 out of 28 programs displayed evidence of the inclusion of a statistical methods class, an advanced methods course and additional statistical methods. (Ramsay & Macpherson 2022, 8–11; 13–14.)

Based on the overview of the IC CAE program above it is clear there exists a research gap in studying the curricula of the IC CAE institutions. If the SSCI and GAO found so little evidence of the program's efficacy in increasing diversity, that puts the program's democratic legitimacy at risk. Whereas this study does not examine the diversity aims of the program, they have been noted as an integral part of the argument for workforce policy. While the programmatic course content of the IC CAE universities has been touched upon in general research on intelligence education curricula, and the program types have been mapped, there remains plenty of gaps in the understanding of the programmatic content.

[20] The International Association for Intelligence Education (IAFIE), which was founded in 2004, is a pioneering institution in setting professional standards for intelligence education. The academic association comprises of members from various domains of intelligence, such as national security, law enforcement and competitive intelligence. The IAFIE helps educational institutions create intelligence studies programs and provides them with shared experiences, methods, sources and teaching materials. (IAFIE 2022a; 2022b.) Whereas the IAFIE standards provide an excellent benchmark for comparing intelligence studies curricula (as shown by Ramsay & Macpherson (2022), they do not reflect the needs of this study.

To conclude Chapter 3, the themes arising from expectations towards intelligence and intelligence analysis at the institutional level have been illuminated for the purposes of this research. Though not included in the coding unit themes of the study, the significance of such variables as the strategic environment, democratic oversight and accountability, state and non-state actors, global power structures, intelligence failures (and successes), terrorism, emerging technologies, privacy, civil liberties and transparency, return of investment (ROI), and diversity of inclusion of workforce are acknowledged as important shapers of expectations towards intelligence analysis.

Moreover, the context for the second research question regarding the presence of procedural knowledge within the IC CAE programmatic curricula has been established. The procedural knowledge categories have been operationalized under the themes *Data Management, Analysis, Communication, and Operational Skills*, and the respective operational themes (Table 2 in Chapter 2.4.). While some programmatic themes from Chapter 3.4. will resurface in the final analysis, the following Chapter 4 will argue for the main elements included in the coding unit themes *Improvement of Analytic Tradecraft and Intelligence Analysis*, and *Strategic, Disciplinary, and Scientific Knowledge*.

4. INTELLIGENCE ANALYSIS AS A MODE OF KNOWLEDGE PRODUCTION

4.1. The Process of Intelligence: The Cycle, Collection Disciplines, and Products

As the operating environment of the United States Intelligence Community has now been established, a closer examination of the processes and principles of intelligence analysis follows. The aim of this chapter is to zoom into the components, goals and methods of intelligence analysis, introducing the reader to more perennial questions as well as central themes in current research. In this literature review, several orientations of scholarship on intelligence analysis as a mode of knowledge production are reviewed. First, the intelligence cycle introduces the process of intelligence, encompassing the essential functions from collection to dissemination. Second, the relationship between intelligence and science in general, and the dialogue between intelligence analysis and social sciences is examined. Then, the anticipation of futures and the inherent uncertainty in intelligence analysis are addressed. Essential to the research objective, the coding unit themes of *Improvement of Analytic Tradecraft and Intelligence Analysis*, and *Strategic, Disciplinary, and Scientific Knowledge* are contextualized.

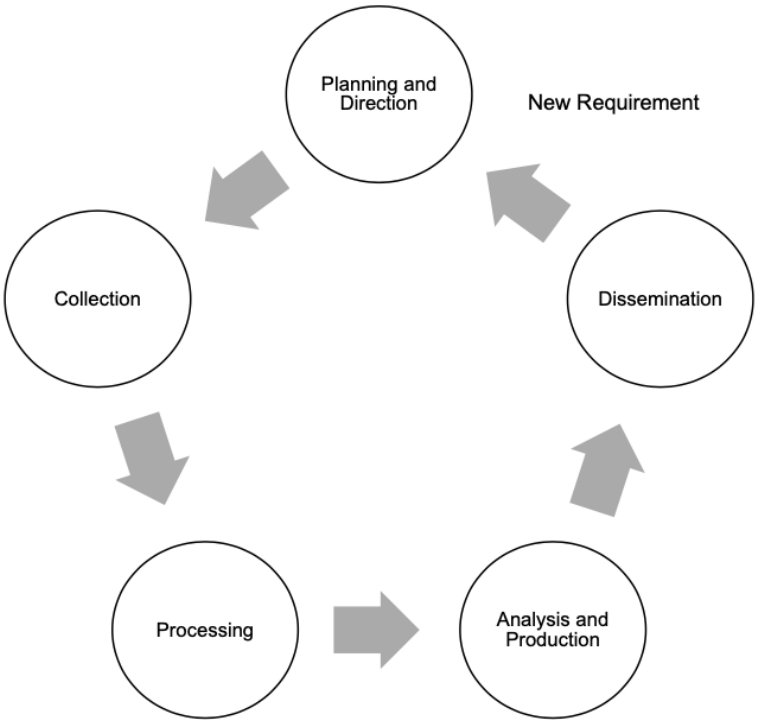
To begin, the disciplines of intelligence collection (the INTs) are now reviewed in more detail, with the focus on human intelligence (HUMINT) and open source intelligence (OSINT). The collection disciplines introduced here are the foundational processes that direct the intelligence community's efforts in their pursuit for all-source intelligence at different levels. The introduction of nomenclature such as OSINT into university curricula is an example of the interchange between the institutional and programmatic levels of curricula in the theoretical framework of the study.

Intelligence is generally considered to operate on three different levels: strategic, operational, and tactical. Yet the division is not clear-cut, and intelligence of all levels may overlap. For instance, *tactical intelligence* in the traditional military domain has to do with the practical application of intelligence to identifying and dealing with target individuals and organizations. When activities involve operations against multiple targets and require coordination, *operational intelligence* is produced to support those efforts. (McDowell 2009, 13–15.) For national decision-maker customers, strategic intelligence informs the creation

of national policy, monitoring of the international situation, and supporting policies such as trade or national industries. In militaries, strategic intelligence is usually reserved for senior leadership, addressing such considerations as contingency plans, developing of weapons systems, and defining force structures. (Clark 2019, 23.) Strategic intelligence enjoys prominence in the US National Intelligence Strategy (NIS) of 2019, being the first of the foundational mission objectives set in the strategy (ODNI 2019).

The processual nature of intelligence is usually illustrated – to a pedagogical if not complexity-describing degree – through the *intelligence cycle* (see Agrell & Treverton 2015, 4, for the earliest use in the U.S. Army in 1948). The intelligence cycle includes the definitional process and activity of intelligence, as well as the final product. The verisimilitude of the intelligence cycle has been debated for decades now, yet it seems to retain relevance as a heuristic description, and it could be applied to the acquisition of intelligence at any of the three levels (strategic, operational, and tactical). (Johnson 2010, 12–15.) Here it suffices to introduce the classical model (illustrated below in Figure 2), with a descriptive emphasis on the collection phase, and analysis later in Chapter 4.

Figure 2 The Intelligence Cycle (Johnson 2012, 12).



First, as the administration identifies new requirements or intelligence priorities, *planning and direction* are commenced. At this crucial stage of the cycle, intelligence officers must

establish the intelligence needs of policymakers, a task at times hindered by the lack of communication. The *intelligence collection* phase employs the vast networks of the various intelligence collection disciplines (the INTs), be it more technical in nature (as in reconnaissance, aircraft, satellite or ground-based listening posts) or human-sourced. (Johnson 2010, 12–15) The respective "five disciplines" of intelligence collection that form the American core taxonomy of sources, are as follows:

- Open Source Intelligence (OSINT); information available to the general public that is of potential intelligence value,
- Human Intelligence (HUMINT): intelligence derived from information collected from and provided by human sources,
- Measurements and Signature Intelligence (MASINT): scientific and technical intelligence obtained from quantitative and qualitative analysis of data (metric, angular, spatial, wavelength, time dependence, modulation, and hydromagnetic) derived from specific technical sensors,
- Signals Intelligence (SIGINT): intelligence comprising either individually or in combination of all Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT) and
- Imagery Intelligence (IMINT): [21] intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced electronically on display devices or other media. (Clark 2019, 178–179.)

Further, the collection disciplines consist of a multitude of often very technical sub-disciplines[22] that are not necessary to cover in the scope of this research. The separation of these various disciplines is also not always clear, and finalized products utilize a combination of evidence from different sources. For the analyst, Clark notes a fundamental division[23] of intelligence sources between *literal information* – that is, such information that humans use for communication – and *nonliteral information*, which requires the technical expertise in

[21] In some instances, IMINT is replaced by GEOINT, but as Clark notes, it is IMINT that is collected by various systems, not GEOINT, which is an all-source form of intelligence (Clark 2019, 178).
[22] For instance, MASINT sources alone could encompass the likes of acoustic signals (ACOUSTINT), infrared signals (IRINT), laser signals (LASINT), nuclear debris and radiation (NUCINT), nonimaging optical intelligence (OPTINT) and radar tracking and measurement of aerospace vehicles (RADINT) (Clark 2013, 13).
[23] This division Clark credits to the late Michael Herman, who at the conceptual level ideated the categories of "textual or message-like intelligence" and "observation/measurement intelligence" (Herman 2001, 55–56).

processing and exploitation to be useful (2013, 1–2). Thus, according to this taxonomy, literal intelligence collection would consist of OSINT, HUMINT, COMINT, and cyber collection, whereas nonliteral intelligence would encompass of IMINT, ELINT and FISINT, radar, acoustic and seismic, materials sampling and sensing, biological and medical, biometrical, and materiel sources (Clark 2019, 180).

Given the role of open source intelligence (which forms the bulk of data available to the analyst in contemporary times),[24] and human intelligence in matters of strategic analysis, these two disciplines will be given some additional attention here. First, OSINT itself is not new, but digital technologies have brought vast corpora of information available to anyone. Open source intelligence has strong overlaps with other collection disciplines, such as GEOINT (geospatial intelligence composed of various geospatial information, imagery, and imagery intelligence), IMINT (e.g., Google Maps and other services that provide satellite images), SIGINT (television and social media provide real time video streaming), MASINT (for example, public seismometer, and airborne radiation sensor data provided by national weather services among others), and HUMINT (journalistic contacting of human sources). (Bowman 2018, 706–707.)

A different issue is the sifting and processing of these oceans of data for anything useful, and increasingly sophisticated methods for exploiting openly available (white) or grey information and literature are constantly developed.[25] A plethora of OSINT collection method courses, blogs, and websites are available online, as are different software that specialize on network analysis among other methods. Certainly, a thriving, global online community of open source “investigators” operating in the World Wide Web has emerged (Perrigo 2022). Commercially, OSINT is a discipline that has most clearly spread to the domain of competitive intelligence and brought about new avenues for private intelligence. One market research company estimated that the global OSINT industry was valued at $5,4 billion in 2021 and was projected to grow to around $36,2 billion by 2030 (Custom Market Insights 2022). As explained in a practically oriented OSINT-handbook, the collection discipline is

[24] Different figures estimate that the proportion of OSINT is around 80–90% of all intelligence collection (Clark 2013, 18; Bowman 2018, 703.)

[25] According to this classification, information designated as *white* is completely available to the public. In contrast, grey literature as a subcategory of grey information is often published in hard copies, and in limited distribution. Such documents may include research and manufacturing publications for proprietary use, or historically, Soviet military journals. As the obtainment of grey literature may involve agents or intelligence officers, it is borderline confidential. Internet equivalents for such content are password-protected spaces. *Black information*, on the other hand, is classified and requires covert operations or activities to be collected. (Clark 2013, 28; Hribar *et al*. 2014, 533.)

harnessed not only by government, business, and non-governmental organizations, but criminals and terrorist networks as well. By extension, OSINT-methods have come to serve the traditional purpose of reconnaissance of an intelligence target, now shifted to the digital arena. (Hassan & Hijazi 2018, 12–13.)

Formerly, OSINT consisted of published, hard copy literary material such as newspapers, books and periodicals (referred to as LITINT). Now, sources include traditional newspapers and magazines, and radio, television, computer-based information; professional and academic material from conferences, symposia and professional associations, and academic papers; government reports and official data; user-generated social networking sites; and paid commercial databases. According to Clark, open sources serve as the starting point for the all-source analyst, as they are easy to use and inexpensive. An analyst should ideally rotate between open sources and more expensive sources, as the latter provide new leads to open-source investigations. Open sources also serve as fundamental information for intelligence agencies for maintaining global and regional coverage. This baseline – often compiled in an unclassified set of basic encyclopedias – may contain intelligence on regional infrastructure, and country-specific data. Examples of this are the Basic Encyclopedia (BE) maintained by the US military intelligence (which contains information on potential targets and non-targets), and the CIA World Factbook's public version, available online at the agency's website. (Clark 2013, 17–20.)

Human intelligence encompasses the classical notions of spying and espionage – the ancient tradecraft of intelligence – and then some. The use of human intelligence collection has been especially prevalent throughout the wars of history, much of it conducted at the tactical level. Nowadays HUMINT is collected and produced by intelligence (case) officers and their agents (assets), defense attachés, diplomats, defectors and émigrés, detainees, and travelers, among others. HUMINT is usually either clandestine or overt. Clandestine HUMINT is collected secretly from a foreign source to provide classified data, or an intelligence officer's direct access to secret data. Overt collection is conducted by Department of Defense attachés or Foreign Service officers of State Department. Émigrés, defectors, and travelers are also debriefed overtly. Additionally, detainees are interrogated for human intelligence. Notably, the CIA's role as the dominant HUMINT collector allows for the agency to maintain a wide global intelligence officer network, stationed in various embassies and consulates around the world. (Richelson 2016.)

Human intelligence collection is often associated with notorious defectors and intelligence failures. For instance, the CIA counterintelligence officer Aldrich Ames was recruited in 1985 by the Soviets, and his defection compromised hundreds of US intelligence operations and led to the deaths of at least ten US spies. Ames' arrest in 1994 brough about public outrage and severe damage to the CIA's reputation. In another well-publicized defector case, the FBI officer Robert Hanssen began turning over US espionage information to the Soviets in the late 1970s until his arrest in 2001. (Hitz 2006, 124.) The materials acquired during the span of this dual betrayal must have had an impact at the strategic level, as among them were some most sensitive US operations themselves devised to provide HUMINT of strategic value. In terms of intelligence failures, the Iraqi Weapons of Mass Destruction (WMD) affair was, according to the 9/11 Commission and the Silberman-Robb Commissions, very much caused by the lack of well-placed human sources on the ground. In an infamous National Intelligence Estimate (NIE), the existence of Iraqi WMD was argued in 2002 based on 1991 data, UN Inspector reports that ran to 1998, unilateral sources like the "Curveball", and analytically deficient tradecraft. This belief in the existence of WMD was one of the main reasons justifying the costly invasion of Iraq in 2003. (Hitz 2010, 257; Hitz 2006, 126–127.)

Returning to the intelligence cycle, the subsequent procedure after collection is *processing*, as the raw intelligence is translated, decoded or otherwise converted into a comprehensible form. The great disparity between the vast amounts of raw information collected and the capacity to process it to anything useful renders processing a perennial issue of intelligence, now even more pronounced with the increasing quantity of global communications. Johnson remarked that "the United States is always short on translators, photo-interpreters, and codebreaking mathematicians". (Johnson 2010, 19–20.) After having been processed, potential intelligence is *analyzed*. Indeed, intelligence analysis is "the mainstay of intelligence", not espionage, counterintelligence, or operations (Lowenthal 2017, 987). Yet intelligence analysis is based on incomplete information, and it constantly faces human cognitive limitations. Great and often unrealizable expectations are set upon intelligence analysis, and failures follow. However without the sweeping knowledge that timely and accurate intelligence brings to decision-makers, their odds to navigate the world would be far worse off. (Johnson 2010, 20.)

Finally, in the linear conception of intelligence cycle ends in *dissemination* – that is, the distribution to decision-makers – before continuing or beginning again (Johnson 2010, 21).

Intelligence products can be principally classified in four types. Current intelligence addresses daily developments around the globe. Research intelligence provides an in-depth look into relevant themes to support specific operations or decisions, or basic intelligence on geographic, demographic, social, military and political variables. Estimative (or recently, anticipatory) intelligence anticipates future events. Warning intelligence is a subset of anticipatory intelligence, which is provided to give notice of imminent or long-term dangers. (Marrin 2011, 11–12.) Such products as the President's Daily Brief (PDB) and National Intelligence Estimates (NIEs) at the hands of the chosen few represent the end products. The PDB is collated daily, to produce a current intelligence picture of the last and next 24 hours. It is distributed to the president and a few top officials each morning. However, as Johnson describes, the product itself is an interactive process. Customers such as the President, Vice President, Secretaries of State and Defense, the White House Chief of Staff, and National Security Adviser may ask additional briefings from analysts for their specific questions. (Johnson 2008, 334; 338.)

National intelligence estimates, on the other hand, are strategic and anticipatory in nature, and usually take several months to prepare (ibid., 342). NIEs are prepared by the cross-IC National Intelligence Council (NIC), which was established in 1979 and is now located within the ODNI (Meese et al. 2018, 261). The NIEs have only quite recently drawn the media's eye, as was the case with the faulty Iraq WMD NIE of 2002, and a controversial 2007 NIE on Iran's nuclear capabilities that was partly publicized on The New York Times. Many NIEs have been now partly declassified and have been researched in *postmortems*. For instance, a 2017 study examined the lack of policy response to a 1990 NIE that presciently anticipated the collapse of Yugoslavia. The authors found that even when the NIE gained policymakers' attention, it provided no opportunity analysis – a fact that may have stymied policy action (Treverton & Miles 2017, 507). Other intelligence products include and have included the Senior Executive Intelligence Brief (SEIB), a current intelligence product that resembles the PDB but is less sensitive and distributed more widely. CIA's Intelligence Reports, classified serial publications, situation reports, and periodical open source based reports represent the category of research intelligence. (Marrin 2011, 17–18.) As the general process of intelligence has now been defined, the following chapters look more deeply into intelligence analysis.

4.2. Intelligence Analysis and (Social) Science: Uneasy Friends?

This subchapter breaks the *analysis* in intelligence analysis to its component parts. The foundations of intelligence analysis, modelled after social scientific (Kent 1965, 156), and other scientific features are examined. Questions of science and non-science are important in the sense that they affect which scientific features are expected of intelligence analysis, and which are not. Moreover, these questions are assumed to trickle down to the institutional and programmatic curricula – for example, in the contents of the strictly academic courses that are deemed useful for future analysts and thus included in intelligence education curricula.

Analysis is performed universally across disciplines of arts, tradecrafts, and sciences and has different connotations in different domains. According to general dictionary definitions, analysis is "a detailed examination or study of something so as to determine its nature, structure, or essential features," but also "the result of this process; a detailed examination or report; a particular interpretation or formulation of the essential features of something." Further, analysis would translate to the "the resolution or breaking up of a complex whole into its basic elements or constituent parts" (especially that of the logical structure of arguments and discourses) (Oxford English Dictionary Online 2022.) Intelligence analysis, however, is as much analysis in the sense of decomposition outlined above as it is *synthesis*; the "composition of a hypothesis or explanation built on inference, context, and conjecture". Moreover, intelligence analysis is constant cycling between these two modalities. (Waltz 2014.)

A well-sourced treatment of intelligence analysis, and a taxonomy of its elements was compiled in the 2005 ethnographic study *Analytic Culture in the U.S. Intelligence Community* by Rob Johnston. Accordingly, intelligence analysis was defined as "the socio-cognitive process, occurring within a secret domain, by which a collection of methods is used to reduce a complex issue to a set of simpler issues". This definition incorporates the decompositional view of analysis, the methods, tools and techniques used in the tradecraft, as well as the cognitive dimension, ending up in a very broad understanding of intelligence analysis. (Johnston 2005, 37.) Johnston's taxonomy draws from 374 relevant texts, comparing many approaches to intelligence analysis and ending up listing tens of variables that interact with the analysts' psyche. He organized these variables at the systemic, systematic, idiosyncratic, and communicative levels. *Systemic variables* include items that

affect both an intelligence organization and the analytic environment such as organizational structures and cultures, external variables such as consumer aspects, and internal and external politics. *Systematic variables* affect the analysis process, and include the categories of user requirements, operations, information archive, analytical methodology, and reporting. *Idiosyncratic variables* influence the analysts' world views (Weltanschauung), and comprise of the categories of affiliation, psychology, education, training, and readiness. Finally, communicative variables pertain to the interaction within and among groups, and include formal and information communication within, among organizations, and between individuals and their social networks. (Johnston 2005, 39–42)

The fundamental difference between the conduct of science and intelligence analysis is the secrecy and lack of transparency in the tradecraft of intelligence. Whereas intelligence products are subjected to multiple rounds of peer review, such measures are often compartmentalized. Hank Prunckun (2015, 68) mentions the significance of such scientific principles as the cumulative nature of scientific knowledge, collegial peer review, and sharing of findings in journals and professional conferences, which do not extend to intelligence analysis to a meaningful degree. Thus, unlike scientific research, which is intrinsically open to scrutiny by outside actors,[26] intelligence assessments are sanitized secret research, and their sources and logic of inference are excluded from the final product (ibid.). Consequently, any *postmortem* of their judgments, conducted by an intelligence scholar, for instance, remains theoretical, as such checks are performed within-agency (Schneider 2020, 199). Complete access to "the file" remains the privilege of official historians or officials conducting *post hoc* reviews (Warner 2006, 18), such as CIA's in-house historians performing archival research. Thomas Fingar establishes a parallel between academic conduct and intelligence analysis:

> "In most respects, the requisites for good intelligence analysis are identical to the requirements for good academic analysis and good analysis of all other kinds, and IC analysts can—and must—rely heavily on the analytic methods they learned in graduate school. There are differences between academe and the world of intelligence (for example, deliberate efforts to hide information and to deceive or mislead foreign governments are much more common in the work of the Intelligence Community than they are in academic research), but the differences should tip the balance in the direction of enforcing even higher standards for IC analysis than for peer-reviewed academic papers." (Fingar 2011, 4.)

[26] While in principle science is "open", in practice, however, scientific publications and resources are only partially disclosed to those outside the academia, due to their licensing structure and paywalls.

And unlike in science, the stakes in intelligence analysis, Fingar argues, involve the potential direction of American foreign or security policies, discrediting or endorsing the positions of foreign leaders or governments, raising doubts about the loyalty of citizens or corporate actors, or causing the US to undertake unwarranted or counterproductive military actions. Fingar 2011, 4.)

As the demarcation question between science and non-science remains unsolved, and is not likely to be solved anytime soon, it is of course difficult to define "science". It is not helpful that the demarcation question particularly plagues the social sciences, which themselves are the keystones of intelligence analysis methodologies. Regarding the social sciences (and International Relations in particular), Patrick Thaddeus Jackson's broad, Weberian criteria for science has utility in distinguishing intelligence analysis from science. First, a scientific knowledge-claim must be *systematically* related to its presuppositions – something a logically consistent intelligence judgments may achieve. Connected to systematicity is the *public criticism* of science, and thus, access to the premises and conclusions of scientific knowledge-claims. (Jackson 2011, 193.) Whereas intelligence is often publicly criticized and scrutinized, it can never meet the criteria of a public scientific community examining its reasoning, as intelligence must protect that very reasoning, along with its methods and secret sources. That is not to say that intelligence agencies do not take part in rigorous peer-review among other analytical checks and balances. On the contrary, they form "intelligence-scientific" communities within themselves and figuratively perform this function of criticism. The whole idea of Structured Analytic Techniques (SATs) and diagnostic tools has been to increase the recording and transparency of the logical chains implicit in intelligence judgments. The compartmentalization and different tiers of classification and access ensure that the very organization and logic of intelligence escape this criterion. Jackson's (2011, 194–195) third scientific criterion of producing *worldly knowledge* also applies to intelligence, as the intelligence analysis enterprise does not, for instance, derive moral code from mystic, celestial creatures and disseminate it as relevant fact for politicians. The worldly knowledge of intelligence analysis, however, does not seem to accommodate many other metatheories and methodologies than (neo)positivism, as it most resembles the "canonical" features of an elusively pursued Science, as explained in more detail below.

This study is not about the philosophical or metatheoretical foundations of intelligence analysis, but it cannot overlook the prevalence of (neo)positivistic methodologies in the literature regarding intelligence analytic tradecraft. In an abstracted description, positivist

methodology often deduces hypotheses from theory and previous knowledge. Claims on causal relationships and empirical falsifiability feature often across such research designs. Usually, positivistic methodologies operationalize their theories into variables. In search of generalizable findings, positivist research designs are concerned with general or universal "nomothetic" laws. (della Porta & Keating 2008, 28–32.) In this regard, whether the number of cases in (neo)positivistic methodologies is small-n or large-n, cross-case covariation of causal factors is sought to test hypotheses to see whether they cases conform to general laws. (Jackson 2011, 200.)

There is plenty of evidence that in the United States, positivistic epistemological and methodological commitments in the research and teaching of IR have been embedded in the recent decades. Due to the significance of the American IR scholarly community, this continuing trend is likely to influence the field of IR at large. (Eun 2017, 595.) It follows that those practices of strategic intelligence analysis, especially pertaining to international affairs and their structures, draw from positivistic conduct. Illustrative of the positivistic scientific image that intelligence analysis is mirrored against is an argument for intelligence analysis as an art:

> "…intelligence analysis deals with an infinite number of variables that are impossible to operationalize because they cannot be adequately quantified or fully collected. … Because in many cases the variables are so complex, countless, and incomplete, attempting to analyze them using scientific methods is pseudo-science. Therefore, any attempt to make predictions based on quantifying these variables is futile." (Folker in Marrin 2011, 37.)

Ironically, if uniformly applied across social sciences, this definition would exclude many few methodologies, rendering them pseudo-scientific.

With regards to the demarcation debate, intelligence analysis is often compared to medicine, which is recognized as art, tradecraft and science. Practitioners of medicine form their judgment rather intuitively by drawing on their expertise (and diagnostic tools) in medicine, and medicine as a discipline is built on such natural sciences as biology, chemistry, and physics. As Johnston observes, however, intelligence analysis, unlike medicine, has not undergone revolutionary change, as the disciplines underpinning its conduct have not experienced such as revolution. (Johnston 2005, 43.) Indeed, social sciences have not been received with such acclaim and global social prestige as natural sciences, and such a sea change seems elusive. Nevertheless, intelligence analysis, as an art, has undergone a change towards tradecraft in recent decades, not least in the 1990s and after the events of

9/11 in 2001 (Marrin 2011, 28–29). And this focus on tradecraft, including more rigorous methodological standards and professionalization, has paved way for intelligence analysis to adapt more scientific features. In their 2015 work, Wilhelm Agrell and Gregory F. Treverton suggest that

> "…We are witnessing a process in which intelligence intentionally and unintentionally is becoming more "scientific," not necessarily in the traditional academic disciplinary sense, but resembling more the emerging complex, cross-boundary, and target-oriented research efforts." (Agrell & Treverton 2015, 8).

Perhaps in the future, after years of proliferation of intelligence analysis in the civilian sector, intelligence analysis performed in the academia and other public institutions indeed achieves the recognition of a science, as it no longer is confined to secret organizations that initially brought about its existence.

Intelligence analysis is subjected to high political expectations of a more urgent timeframe than science. The global scientific community may not have the cornucopia of secret intelligence resources at their disposal, but they hardly need it to advance scientific endeavors openly. Unlike scientific achievements, which are regularly cherished as historical feats and awarded, intelligence analysis is often framed with recurring intelligence failures. Moreover, intelligence successes rarely see the light of day, and the value of good intelligence is very complex to demonstrate in hindsight. Science has had its own controversies as well, especially related to the exploitation of a hegemonic position within a scientific field or harnessing the means and authority of science to totalitarian acts. And science in general has also seen its share of frauds and misconduct that have risked public and collegial credibility. The expectations placed on the self-correcting nature of science, however, appear to be more forgiving than the politicization of affairs acted under inaccurate or altogether erroneous intelligence. (Agrell & Treverton 2015, 55–59.)

Historically, the close relationship between the academic scientific research and modern security institutions owes much to the scientific policies of the World Wars. The war efforts of the Second World War harnessed research institutes and academic institutions as a major war resource. The implementation of research policy, planning and management contributed to the bureaucratization and even militarization of science. Such sciences as physics, chemistry, and mathematics were mobilized for military purposes, along with social

sciences.[27] Military organizations in turn became dependent of scientific research as a key strategic instrument in their domain. Many intelligence-specific technical systems (such as radar) in signals intelligence and cryptanalysis were borne out of technical research and utilized mathematics, statistics, and linguistics successfully. (Agrell & Treverton 2015, 13–16; Warner 2014, 103.)

The social scientific approach to intelligence analysis can be traced back to the 1940s. Many authors of the time and the following decades paid attention to behavioralist ways of conducting social science. Behavioralist formulations of scientific principles such as formation of hypothesis, predictive models and data collection were considered useful in intelligence analysis. (Marrin 2011, 25.) An ODNI-sponsored study published in 2011 concluded that the IC can "derive great benefit, in short time and at a relatively low cost, by building available behavioral and social science knowledge". Further, the study committee believed "that dramatic improvements in the analytic process are possible within existing organizational constraints". In their recommendations, the authors regarded such analytical methods as probability theory, statistics, game theory, and qualitative analysis as methods with strong scientific foundations, and proposed all analysts were familiarized with them. Interestingly, the committee also described the relationship between "the behavioral and social science community" as distant but went to say that the national unity of 9/11 attacks had lowered such barriers. (Fischhoff & Chauvin 2011, 81–84; 88.)

Recognizing the positivistic bias of intelligence analysis in general, various authors in a 2017 journal volume of *Intelligence and National Security* discussed the prospects of integrating more "qualitative" approaches of social science to intelligence analysis. Marrin (2017, 545), holds that comparative study of different multi-, inter-, and transdisciplinary methodologies helps improve intelligence analysis practices, and suggests the same may be true vice versa. He notes that epistemological comparisons with different domains and disciplines of sciences also illuminates the limits of what knowledge intelligence analysis as a government function can attain (ibid.). Walsh (2017a) examines the possibilities of the methodologies of ethnography, phenomenology, and grounded theory for strategic intelligence analysis. He maintains these methodologies are more about *understanding* (interpretivism and

[27] An interesting example is the US IC's early analysis of Soviet economy, which has been anecdotally called the "largest single social science research project in the history of humanity". Indeed, the US IC (though mainly CIA) had to develop its own models to understand the actual size of the Soviet economy in the 1950s, hiring hundreds of specialists to decipher its workings. (Warner 2014, 153.)

constructivism) as opposed to *explaining* (positivist and empirical). Walsh proposes that ethnographic studies could be used to uncover reasons behind the different forms of radicalization and the links between terrorism and organized crime. Moreover, the methods of data collection inherent in the methodology such as observation, interviews and document analysis may benefit strategic intelligence analysis. (Walsh 2017a, 554–556.)

For phenomenological approaches, Walsh argues that their emphasis on subjective experience may help to understand the perceptions behind certain foreign policy decisions of leaders and contest the mirror imaging of different actors. Grounded theory, on the other hand, could help intelligence analysis more robust categories and clarify relationships between categories, and by the frequent use of both deductive and inductive reasoning result in more confident assessment. (Walsh 2017a, 552; 556–558.) Phythian (2017) notes that that intelligence organizations and analysts could benefit from exploring some post-positivist approaches. He writes that perspectives such as (social scientific) self-reflexivity within the operating environment, knowledge management and alternative conceptions of the intelligence cycle may offer hitherto untapped potential for intelligence organizations. Finally, he stresses the importance of replicating the testing culture of the analysts' hypotheses and theory testing – or risking being little different from "government lawyers" (Phythian 2017, 602–609).

In a 2020 article, Marrin criticized the scientific image present in the Intelligence Community Directive (ICD) 203 "Analytic Standards". According to Marrin, the standards reflect an understanding of the scientific method "as a kind of value-neutral epistemological framework used to develop knowledge 'objectively'". In Marrin's articulation, this image provides a poor foundation for contemporary conceptualizations of the applied epistemology of intelligence analysis, as well as performance standards. Instead, Marrin recommends that the US IC shift their analytic expectations from absolutes such as 'seeking truth' to more relative considerations like honesty and integrity. (Marrin 2020, 350–351; 360–362.) An even more interesting observation from Marrin is that of the limitations of applying scientific methods in the intelligence analysis context. He continues to say:

> "These limitations are so significant that the adoption of best practices based on the scientific method is currently vulnerable to the charges that it is more of a pseudo-science intended to borrow the perceived legitimacy of science rather than achieve actual improvement in practice." (Marrin 2020, 361.)

Added to the notions of social scientific features of intelligence analysis as presented above, Marrin's insight is troubling. If the bias towards positivistic social science in intelligence analysis methodologies truly is this strong, one should ask whether the selection of accepted "scientific" features has in fact limited what intelligence analysis can be? Neopositivistic methodologies themselves are not the issue. They provide ample tools for social analysis. Considering the range of other scientific disciplines intelligence analysis utilizes, it remains scientifically pluralistic. It is certainly possible that the social scientific strains of intelligence analysis have, due to various institutional, cultural and political understandings of science, invoked the "legitimacy of science" as Marrin puts it, at least in terminology, to appear more scientific. And for instance, if the intra-discipline discourses of IR have used the rhetorical commonplaces of "science" to legitimize or delegitimize different authors' work (Jackson 2011, 9), why would not a similar development happen in another environment that is pressured to improve its analysis? Be as it may, a case in point with regards to adopting tradecraft bestowed with a scientific aura are the Structured Analytic Techniques (SATs). The SATs have adopted a familiar positivist lexicon including such terms as induction, deduction, independent and dependent variables, hypotheses and hypothesis testing without displaying specifically "scientific" characteristics (Marrin 2017a, 541).

The development of the now popular SATs started in the 1970s (then called alternative analysis) with the work of Richards Heuer and the CIA officer Jack Davis. Along with the Congressional reforms known as the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) affirmed the doctrinal position of the SATs, and the term was first used in 2005 in the CIA analyst training program. High expectations were placed on the SAT doctrine during the restructuring of the US Intelligence Community after the politicized intelligence failures the 2001 terrorist attacks and erroneous assessments of Iraq's WMD programs. (Chang et al. 2018, 337.) SATs have been described as "a set of processes for externalizing, organizing and evaluating analytic thinking," ranging from the simple such as structured brainstorming to the complex, e.g., scenario generation, and to pure text-based methods to visual ones. The benefits of utilizing SATs are believed to be the mitigation of cognitive biases, better coping with information overload, and with the rigor of additional transparence, increased accountability to both the analysts and decision makers. (Chang et al. 2018, 337–338.) In their widely adopted handbook *Structured Analytic Techniques for Intelligence Analysis* (2014), Richards J. Heuer and Randolph H. Pherson define structured analysis as

> "…a mechanism by which internal thought processes are externalized in a systematic and transparent manner so that they can be shared, built on, and easily critiqued by others. Each technique leaves a trail that other analysts and managers can follow to see the basis for an analytic judgment. These techniques are used by individual analysts but are perhaps best utilized in a collaborative team or group effort in which each step of the analytic process exposes participants to divergent or conflicting perspectives." (Heuer & Pherson 2014, 25.)

However, the ability of SATs to mitigate cognitive biases in analysis has not yet been subjected to substantive empirical validation. In 2019, Martha Whitesmith remarked that only one such published study had been conducted in 2004 (and a limited one at that). Further, Whitesmith's own 2019 study regarding the SATs was limited to how efficacious Analysis of Competing Hypotheses (ACH) method might be in the mitigation of serial position effects, which is just one cognitive bias among many. (Whitesmith 2019, 226; 238–239). In a 2020 study, Whitesmith conducted two meta-analyses which indicate that serial position effects or confirmation bias do not affect intelligence analysis differently from non-intelligence analysis. Moreover, her results also suggest that the ACH is not effective in mitigating cognitive bias. (Whitesmith 2020a, 381; 388–389). Regarding the impact of confirmation bias, she recommends that different types of information are examined and further compared with non-intelligence scenarios (Whitesmith 2020b, 222–223). The SATs have been popularized to the extent that many Western security and intelligence services have at least partially adopted the SAT framework for their analytical tradecraft (Whitesmith 2020a), based on commercially available intelligence analysis literature (for instance see Borg 2017), and perhaps intelligence liaison with other countries (Svendsen 2012a).

The lengthy overview above has highlighted some of the issues present in the development of intelligence analysis tradecraft. While it has been argued here that intelligence analysis is not a science, intelligence has utilized different disciplines of science impressively. The critical approach towards intelligence analysis appropriating positivistic terminology is particularly relevant to the evaluation of the institutional and programmatic curricula via the two coding unit themes of the institutional curricula, *Improvement of Analytic Tradecraft and Intelligence Analysis* and *Strategic, Disciplinary, and Scientific Knowledge.* For instance, as the critique towards the SATs and the positivistic bias of intelligence analysis is known, a different light is cast upon the widespread teaching of SATs.

4.3. Probing the Future: Forecasting, Foresight, and Anticipatory Intelligence

This subchapter presents an overview of one of the more problematic facets of intelligence analysis, the elusive prediction of future events. In popular imagination, it is mostly the perceived lack of foresight that has led into the various intelligence failures throughout the American intelligence history, although the actual reasons in *postmortems* have often pointed out flawed tradecraft or unreliable sources. The enormous pressure of prediction is assumed to burden the institutional and programmatic curricula of intelligence education, but as later noted, no Futures Studies methodologies had found their way into the Intelligence Community Centers of Academic Excellence curricula sample of this study.

The future is a central domain for intelligence to chart, at various levels of intelligence. Afterall, much of the 20th century high politics were conducted under the fear of a reciprocal nuclear exchange. The era just after World Wars gave new momentum for science to blossom, but science's dependence on public institutions was never 'demobilized'. (Wenger et al. 2020, 5–8; Agrell & Treverton 2015, 26.) As did various operations research and RAND's pioneering forecasting methodologies, so did intelligence set its sights to future, particularly in the domain of predicting nuclear proliferation (Bell 2003, 29–31; Schneider 2020, 197).

Anticipatory intelligence has faced numerous criticisms since. Some have criticized the ability of futures intelligence to anticipate surprises and abrupt discontinuities and pointed out the presence of a variety of intellectual and methodological flaws. Others have noted that strategic surprises and major changes will be more difficult to identify by utilizing linear approaches such as pattern and trend analysis. (Landon-Murray 2017, 788.) Unfortunately, the effective inertia of political and bureaucratic realities constrains the realization of reform, fostering cynical and risk-averse cultures in the intelligence sector. In contrast, alternative information brokers during "post-Moneyball[28], post-FiveThirtyEight[29] world" make use of futures studies and forecasting techniques sophistically, unlike ever before. (Mandel & Irwin 2021, 571.)

[28] Moneyball refers to the Oakland Athletics baseball team's success in utilizing sabermetrics to assembling the team's roster. An account of those events is present in the 2003 book *Moneyball: The Art of Winning an Unfair Game*, by Michael Lewis.
[29] FiveThirtyEight (538) is an opinion poll analysis company created by Nate Silver that also has successfully utilized sabermetrics, for instance in elections forecasting.

Useful for illustrating the complexity of anticipation are the three levels of futures study. First, *forecasting* attempts to, often quantitatively, predict future events. Its methodologies range from to the short temporal range of econometric models to the very long temporal range of climate change models. These futures as past-based. The second level, *foresight*, is common for traditional futures studies. It produces a variety of possible futures but is not predictive. Foresight is often qualitative, and it includes discontinuities and different explorative and normative scenarios for decision makers. The third level, *anticipation*, aims to implement both forecasting and foresight outcomes to decisions. Anticipation is nonpredictive, qualitative, and focused on discontinuity. (Poli 2019, 6–7.) Not all intelligence addressing the domain of future necessarily adhere to these characteristics, but the terms represent a useful distinction. Aligning with the conceptualization of the Futures Studies modalities above, anticipatory intelligence includes both forecasting and foresight approaches, as well as the synthesis of both (see ODNI 2019, 9).

As put by Ian Spiegel (2021), ever since Sherman Kent's notions of 'estimative' or 'warning' types of intelligence, intelligence communities have occupied themselves with producing descriptions of the future by amassing and synthesizing knowledge of the past and present. Methodically, this presents intelligence analysts with the humble challenge of identifying trends, causal mechanisms and creating forecasting models. According to Spiegel's interpretation, the Western intelligence community's current forecasting paradigm is "processual" and is affected by over-reliance on the contested SATs. In this sense, the process-oriented forecasting has been concerned with reducing the impact of cognitive biases, with scientifically untested methodologies. Spiegel, instead, is in favor of adapting what he calls the "verification paradigm", that has already been tested by volumes of research. With the verification paradigm, he refers to the incremental calibration of forecasting accuracy by "predicting" future events and scoring the results against the reality of transpired events. The accumulating knowledge is then used as a metric to achieve better forecasting results. (Spiegel 2021, 961–962; 964.)

Such an approach has already been tested by a US IC-sponsored project, and the results have produced volumes of new research. The Good Judgment Project (GJP) was created by Philip E. Tetlock and his University of Pennsylvania team and funded by ODNI's Intelligence Advanced Research Projects Activity (IARPA). In the project, several thousand people took part in geopolitical forecasting, out of which a group of "superforecasters" emerged. These people had exceptional talent for accurate "predictions" of future events,

whose attributes Tetlock's later research examined. The superforecasters had performed some 30% more accurately than seasoned intelligence analysts taking part in the project. Research on forecasting accuracy continues in various fields continues to yield useful results for the intelligence community. (Tetlock & Gartner 2015, 88–91.)

Given the vagaries of the strategic environment intelligence attempts to navigate, complexity science and complexity theories have been applied to strategic intelligence and forecasting since the operating environment of intelligence actors is characterized by complex interactions. (Landon-Murray 2017, 788–789.) In practice, an increasing turn to complexity theories would mean a stronger acknowledgement and reliance on mixed-methods approach (Speigel 2021, 971). A handbook example of the complexity approach is Robert M. Clark's *Intelligence Analysis: A Target-Centric Approach* (first published in 2003). In his reiteration of the intelligence cycle, Clark imagines the typical intelligence target as a system. In his view, a system comprises structure, function, and process – all of which are facets an analyst must deal with in systems thinking. Furthermore, Clark argues that all intelligence targets are systems and *complex* systems at that, since they exhibit dynamic, evolving, and nonlinear properties. To operationalize this application of complexity theory, Clark pictures each target or system as a network as well, with its nodes and links to be analyzed with (social) network analysis, a common tool in intelligence analysis. (Clark 2019, 46–50.) In their article, Bram Spoor and Maarten Rothman (2021) found that the increased complexity in the domain of intelligence operations (and thus research) has coincided with the rise of critical or post-positivist theoretical perspectives. Spoor and Rothman are critical of the positivist paradigm of intelligence analysis, noting that intelligence agencies may still act as "bastions of modernist meta-narratives, constituting a positivist monoculture". (Spoor & Rothman 2021, 564–565.) As Spoor and Rothman's article displays, the uninviting concessions to complexity for intelligence agencies seem to translate to a language of less pronounced and less certain judgments, antithetical to the wishes of the clients.

Others have called for increased attention to the *sensemaking* process, arguing in favor of the sensemaking paradigm. David T. Moore *et al*. (2021, 46–47) define sensemaking as "the deliberate attempt to understand a situation and how it emerged," while having the goal of achieving an explanation in terms of causes, which can include human intentions, beliefs, and actions, and deriving courses of action from that understanding. As a continuous process of problem solving or data exploration, sensemaking does not have a distinct terminus. In Moore et al.'s view, the concept of sensemaking, initially introduced in the 1960s

in the context organizational analysis, is considered a fundamental process of macrocognition, defined as the adaptation of cognition to complexity (Moore et al. 2021, 48).

This subchapter has addressed the difficulty of predictive efforts for intelligence. Intelligence must always think ahead, and the expectations of "prediction" are often unrealistic. As noted, various non-governmental organizations such as FiveThirtyEight and the superforecasters have gained public recognition, whereas the US IC's foresight and forecasting methodologies have faced methodological criticism. The US IC, of course, has also utilized the results of such developments to improve their own tradecraft, as was the case with the Good Judgment Project (GJP).

4.4. An Uncertain World: The Probability Calculus

As established above, intelligence analysis produces judgments on future events and scenarios and assigns linguistic estimative values to their likelihood. Certainly, a paramount objective of intelligence is to reduce the uncertainty that haunts decision makers in a dynamic operating environment. Thus, an important orientation of research in the world of intelligence analysis is the one examining how *uncertainty* (i.e., probability and confidence) is addressed and expressed in intelligence assessments. According to Jeffrey A. Friedman and Richard Zeckhauser (2015, 80), *uncertainty* relates to situations in which probabilities are ambiguous, and cannot be determined with precision. Uncertainty can be *epistemic*; borne out of lack of knowledge of something that is unknown, but at least in theory, knowable. *Aleatory uncertainty* refers to knowledge that is simply unknowable and results in a degree of irreducible uncertainty. (Tetlock & Gardner 2015, 143–144.) *Risk*, on the other hand, involves situations in which the probabilities of different outcomes can be calculated precisely – such as in the game of roulette. (Friedman & Zeckhauser 2015, 80.)

David R. Mandel and Daniel Irwin (2021, 560) have compared the various lexicons for communicating probability via linguistic probabilities in the Anglo-American intelligence community, providing ample critique of the flaws inherent in contemporary standards. Based on various studies, the authors locate factors in linguistic probabilities that risk miscommunication. First, individuals interpret linguistic probabilities differently, depending on contextual factors such as content domain, outcome valence among others. Personal characteristics such as numeracy, language, personal attitudes, and locus of control affect how personnel see linguistic probabilities. For instance, organizations such as NATO face

challenges in interpretation depending on whether a person is a native English speaker or not. Second, the authors assert that probability phrases are used to minimize blame and manage face, for instance by overstating negative-outcome probabilities, or minimizing positive-outcome probabilities. Third, translation tables and probability lexicons are interpreted inconsistently with the prescribed meanings. Subsequently, to counter the risk of miscommunication, the authors suggest analysts be encouraged to assign numeric probability intervals (e.g., 65–85%), from which one can easily derive a best estimate from the midpoint (i.e., [65 + 85]/2) and an associated margin of error (i.e., [85 – 65]/2), resulting in an equivalent point estimate of 75% plus or minus 10%. (Mandel & Irwin 2021, 561–563.) To illustrate the current paradigm, Table 3 lists the current ODNI guidance for expressions of likelihood or probability (ODNI 2015, 3)

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain(ly)
Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
01–05%	05–20%	20–45%	45–55%	55–80%	80–95%	95–99%

Table 3 Expressions of Likelihood or Probability in Analytic Products

Friedman and Zeckhauser, on the other hand, argue that the information in probability ranges can always be condensed to single points. For instance, they argue, that for decision makers, the range between 40 and 80% is just the same as an estimate of 60% probability. According to Friedman and Zeckhauser, expressing probability intervals is logically equivalent to the decision makers trying to establish probabilities themselves. The authors utilize the often-used example of the US president Barack Obama being briefed by his top intelligence advisors about Osama bin Laden's presence in Pakistan's Abbottabad. According to Mark Bowden's 2012 account, intelligence officials offered varying probabilities to the chances of Osama bin Laden living in Abbottabad, ranging from the Red Team's 40% to 60%, 80%, and 95%. As the intelligence officials reportedly offered no average probability figure, the president defaulted to a 50/50 assessment, signaling a cautionary estimation as the average of above figures would be 69%. (Friedman & Zeckhauser 2015, 77–78; 86)

Mandel and Irwin (2021) also criticize how intelligence community treats its analytic confidence, requiring analysts to convey their confidence using coarse ordinal ratings that usually have low, medium, and high levels. Moreover, they explain, that analysts are usually instructed to assess probability and confidence as if they were independent constructs. Although such instructions, Mandel and Irwin argue, fail to explain the fact that the expression of confidence in each judgment captures the analyst's own, subjective margin of error *in* a probabilistic estimate. Specifically, the less the analyst's confidence in their estimate, the wider the credible intervals should be (i.e., an analyst who believes the probability of an event lies between 50% and 90% is less confident than one that believes the probability lies between 65% and 75%, and the first provides a more ambiguous but a safer estimate). The implications of this probability–confidence dissociation are undesirable to the intelligence customer, as previous research on the 2007 NIE on Iranian nuclear capabilities has shown in its miscommunication of the probability–confidence relationship in many of its key judgments. In the case of the Iran NIE, an academic *postmortem* revealed that "confidence" was continuously used to express probability rather than qualify it, directly contradicting the IC guidance for such communication. (Mandel & Irwin 2021, 563–565.)

Friedman and Zeckhauser, while remaining cognizant of the issues of expressing confidence with Words of Estimative Probability (WEPs), stress that point estimates themselves do not convey confidence, and the concepts of likelihood and confidence should be kept separate. Indeed, the authors argue that for decision makers, expressions of confidence are most useful when they serve the function of describing how much predictions might shift in response to *new information*. Thus, they refer to the "responsiveness" of an estimate – that is, whether the clients should act on current intelligence or wait for more information. In the operation regarding Abbottabad, for example, in addition to deeming the confidence of their judgments low or medium, they could have assessed that it remained unlikely their estimates were to change in the light of new information that might be gathered within a reasonable timeframe. This practice would have allowed for better responsiveness of the analysts' intelligence. (Friedman & Zeckhauser 2015, 78, 89–90).

In another study, Irwin and Mandel (2019) dissect the ways information evaluation standards affect intelligence assessment. Before being collated and shaped into intelligence products containing judgments of potential scenarios and developments, the collected, raw information must be evaluated. A well-known anecdote of misjudging the reliability of intelligence sources took place in the context of the Korean War in 1950, as the US IC

dismissed the repeated warnings from local sources about North Korea planning to invade South Korea. The authors start by introducing the doctrinal NATO information evaluation criteria also known as the Admiralty Code (or Admiralty System, or NATO System), first developed by the Royal Navy in the 1940s. The Admiralty Code is used to evaluate the *source reliability* and *information credibility* of the information in question. For instance, information assigned 'B2' would be considered 'probably true' and the source deemed 'usually reliable', as per the current standard Allied Joint Doctrine for Intelligence Procedures (AJP-2.1). (ibid., 504.)

Irwin and Mandel remark that the Admiralty system does not associate the qualitative descriptions such as *usually reliable* (B) with numeric values, introducing the pitfall of varying interpretations of the confidence in the source – quite similarly in principle as the probability language addressed above. The authors also highlight the difference of terminology and varying adherence to NATO doctrine between allies, undermining communication. In addition to communication issues, the authors list the Admiralty Code's lack of situational considerations and the implied constancy of source reliability across different contexts as problematic. For instance, a HUMINT source with a proven track record on certain domain may lack the expertise to observe and report other domains. Accordingly, the same applies to 'objective' sources such as technical sensors, that are subject to external conditions that alter the fidelity of information. Moreover, according to Irwin and Mandel, the extant methods of source reliability evaluation do not formally define or operationalize the concepts that determine reliability, such as authenticity, competency, or trustworthiness, likely increasing subjectivity and undermining the internal consistency of source reliability evaluations. Inadequate procedures of evaluating information as it passes through multiple sources might also introduce challenges to the integrity of that information, as well as the potential distortion of information as it undergoes additional formal evaluations and adjusted analytic conclusions in the process towards a final product. (Irwin and Mandel 2019, 503–507.)

Whereas Irwin and Mandel admit that given the diversity of intelligence contexts the implementation of a reliable, all-encompassing scoring method may be unrealistic, the propose a unitary measure of information accuracy as an alternative approach, expressed as a numeric probability estimate (e.g., Information A having a .75 probability of being accurate). They argue that such an evaluation principle would be less vague and ambiguous than current scale levels and refer to forecasting literature that supports the argument. In addition to bypassing potential semantic confusion, the authors suggest that probabilistic

expression for information accuracy could be 'objectively' measured to generate performance metrics, with the application of Brier scoring, for instance. Moreover, Irwin and Mandel argue, that expressing accuracy as numeric probability would allow for the use of Bayesian networks capture information between pieces of information during evidence marshalling. The authors propose that intelligence collectors and analysts provide individual accuracy statements of the information processed, so that aggregate probability could be calculated. (2019, 512–513; 515–516.)

Within the black box of assigning probability estimates in intelligence analysis commonly lies the logic of Bayesian statistics, named after the English theologian and mathematician, Reverend Thomas Bayes, who published his famous theorem in 1763. In Gregory F. Treverton's words:

> "In an important sense, almost all intelligence analysis is and always has been Bayesian, for even with regard to puzzles, finding the piece that will solve the puzzle with certainty is rare. However, the uncertainty and unboundedness of transnational targets, especially terrorists, underscore the need for both a Bayesian attitude and more formal approaches to making that approach concrete." (Treverton 2009, 39.)

Many other authors of Intelligence Studies similarly stress the ubiquity, necessity, and supremacy of Bayesian statistics in forming probability estimates in intelligence analysis. For example, Sir David Omand writes in his 2021 book on the general nature of intelligence analysis, establishing Bayesian inference as an integral part of the respective analysis mindset. Omand's overview is very much in line with the current Anglo-American paradigm to intelligence analysis as explored within these pages. The author also presents a multiplicity of commonsensical examples of Bayesian inference in famous intelligence analysis case studies, such as the Cuban missile crisis of 1962. However accessibly presented in intelligence analysis manuals, some have noted how Bayesian analysis is neither easy to teach nor easy to apply in practice, although such analysis can now be conducted with the help of certain software packages (Clark 2019, 202).

In mathematics, probability (as defined by A. N. Kolmogorov circa 1930) is a "countably additive set function on a σ -field, with a total mass of one" (Freedman 2009, 4). Generally, in statistics, Bayesianism[30] is the other prevailing approach to probability, in contrast with

[30] Interestingly, however, Bandyopadhyay & Forster (2011, 5) posit that in the field of Statistics, supporters and critics alike agree that Bayesianism is currently the dominant view in the philosophy of science. Moreover, the authors say, that some scholars even project Bayesian statistics to claim the place of the dominant statistics for the twenty-first century.

the more dominant “objectivist” school of frequentist orientations. As explained by the late Professor David A. Freedman, for subjectivists, probabilities describe *degrees of belief*[31]. For classical subjectivists such as Thomas Bayes, unknown, objective *parameters* (numerical characteristics of a statistical model for data, such as the probability of a coin landing heads) would be estimated from the data. Classical subjectivists would have information about those parameters beforehand, in the form of a *prior probability distribution*. Whereas classical subjectivists would make probability statements about those parameters, such as claiming there is a 25% chance of the probability of heads exceeding 0.67, the objectivists would view the probability of heads as an unknown constant – either being or not being bigger than .67. For objectivists, probabilities are inherent properties of the systems being studied, such as coin landing. Therefore, for objectivists, the probability of a coin landing would have its own existence separate from the data, whereas the data could be used to estimate the probability, or test hypotheses concerning it. (Freedman 2009, 4–6).

Accordingly, as Treverton writes, Bayesian inference could be used to test whether a coin is fair. If suspiciously many heads are yielded, one might start to revise their judgment (*prior degree of belief*) about the coin’s nature and the probability of getting heads towards a *posterior degree of belief* (Treverton 2009, 39; Omand 2021, 22). Thus, Bayesianism allows for the updating of opinions considering new data, requiring the computing of a *conditional probability* using Kolmogorov’s calculus (Freedman 2009, 5–6). The same logic of revising and updating (probability) judgments applies to intelligence analysis, as new evidence regarding the analyzed events is uncovered. A posterior probability could be calculated with the following formula (Omand 2021, 23–24):

$$p(N \mid E) = p(N).\ [p(E \mid N)/p(E)]$$

If the 1962 Cuban missile crisis would be used as the example to demonstrate Bayesian inference, as Omand does, N would stand for the hypothesis of ‘nuclear missiles being introduced to Cuba’. If this were considered very unlikely, the prior degree of belief in N, that is the prior probability p(N), might have a probability value of 0.1 (10% likely). However, if credible contradictory evidence, E, was presented (as was the case with consistent IMINT

[31] Freedman, a frequentist-objectivist himself, passingly criticizes the Bayesian approach for not answering what subjective degrees of belief are, where they come from, or why they can be quantified (Freedman 2009, 7).

and HUMINT sources), the posterior probability p(N | E) would have to be found (read as the reassessed probability of the hypothesis N given the evidence E). And when a situation develops towards (perhaps a less suspected) hypothesis, such a revised estimation should be taken into account when considering the analysts' situational awareness. (Omand 2021, 23–24.)

One can of course view the reliance on Bayesian inference in intelligence analysis in a more critical light, as intelligence collection does not necessarily provide such concise data sets as systematic statistical analysis would require – especially if collected from HUMINT sources. Whereas all sort of mundane and incommensurable data can be turned to probability estimates in a Bayesian fashion, such applications of statistical inference do not necessarily make the process more "scientific" (as David Omand continues to insist) – as has been argued previously in this study regarding the art versus science -debate in intelligence analysis. Bayesianism does, however, give the analysts the confidence of referring to formal and scientific methods to bolster the reliability of the intelligence judgments.

Chapter 4 has made a case to illustrate the myriad of profound methodological issues and debates intelligence analysis faces. It has also shown what kind of parallels between social scientific principles and intelligence analysis exist, and how the demarcation discourse has interacted with intelligence analysis. Above all, this chapter has demonstrated how many aspects of intelligence analysis have been probed by the social sciences, and how much fertile ground is left be covered by scholars from pluralistic perspectives. As the two research questions are now approached from the perspective of analysis, all the two main coding unit themes of *Improvement of Analytic Tradecraft* and *Intelligence Analysis* and *Strategic, Disciplinary, and Scientific Knowledge* have been contextualized.

5. ANALYSIS OF THE INSTITUTIONAL AND PROGRAMMATIC CURRICULA OF AMERICAN INTELLIGENCE EDUCATION

5.1. The Institutional Curriculum: A Crucible of Expectations

According to the theoretical framework model, the global strategic environment constantly influences the upper echelons of the universities-security-intelligence nexus, and its influences are transmitted to the institutional curricula, and further into the programmatic curricula. At the level of globalizing intelligence, a strategic backdrop emerges from the historical overview of Chapters 3.1. and 3.2. This backdrop is a microcosm of administration-specific and more enduring interpretations of the global state system and its power relations, the American posture within that strategic environment, and a set of global drivers that constantly shape this operating environment. Chapters 3.3. and 3.4., in turn, have illustrated the various workings of the universities-security-intelligence nexus and its respective operational, ethical, and epistemological domains. Chapter 4 looked deeper into the foundations of intelligence analysis, establishing the important coding unit themes of *Improvement of Analytic Tradecraft and Intelligence Analysis* and *Strategic, Disciplinary, and Scientific Knowledge* and their component parts: the intelligence cycle, the (social) scientific art of intelligence analysis, the anticipation of futures, and the ways intelligence tradecraft assesses uncertainty.

To comprehend this strategic environment, the NISs, ODNI documentation, and the SSCI reports imply a set of domains for the knowledge and sciences that is necessary for different intelligence analysts to master. ODNI's fact sheet (ODNI 2022b) renders the preferred teaching subjects, the "IC CAE study areas", explicit. These are Intelligence, National Security, Critical Technologies, Science, Technology, Engineering, and Mathematics (STEM), and languages. (ODNI 2022b, 3.) This scope of knowledge and sciences is already demonstrated at the levels of strategic and anticipatory intelligence. Strategic intelligence and anticipatory intelligence are both the top priorities of the 2014 and 2019 NISs. This is not surprising as many of the events regarded as intelligence failures supposedly stem from the inability to predictively anticipate future events. In the case of the 2014 NIS, strategic intelligence is defined as "the process and product of developing deep context, knowledge, and understanding to support national security decision-making" (ODNI 2014, 7). An

expanded notion is included in the 2019 NIS: “the process and product of developing the context, knowledge, and understanding of the *strategic environment* [emphasis added] required to support U.S. national security policy and planning decisions” (ODNI 2019, 8). Both strategies acknowledge the profundity and all-source nature of strategic intelligence analysis variables, such as “global political, diplomatic, military, economic, security, and informational development” (ODNI 2019, 8), and “histories, languages, and cultures of nations and non-state entities, their key leaders and opponents, their objectives and concerns, as well as natural resources, technology and transnational issues” (ODNI 2014, 7). These articulations already directly imply the gravity of the IC CAE study areas. Similarly, the significance of research and outreach are connected to strategic intelligence, with the 2019 NIS specifying “outreach to experts in academia and industry” (ibid.).

For anticipatory intelligence, the 2014 NIS regards foresight, forecasting, and alerting (strategic warning) as its integral component parts. The strategy also commits to deepening understanding of “conditions, issues, and trends” in the strategic environment, but also to “forecast the impact on U.S. national security” (ODNI 2014, 7). The latter, according to Poli’s (2019, 6–7) definitions, would involve a quantitative and predictive component, and as such seems like an ambitious goal for any kind of analysis. Another observation related to anticipatory intelligence the 2014 NIS is the integration of alerting capabilities within the IC to “provide timely and relevant warning to our customers” (ODNI 2014, 7). This connects to the overarching commitment of the US IC to further intelligence integration and fusion, featured across the NISs. The anticipatory intelligence section of the 2019 NIS is more nuanced compared to the 2014 iteration, although similar in general expressions. It sees anticipatory intelligence in terms of foresight as “identifying emerging issues” and forecasting as “developing potential scenarios”. The 2019 NIS, like the 2014 iteration, commits to expanding quantitative analytic methods and “reinforcing qualitative methods”, in identical wording (ODNI 2014, 7; ODNI 2019, 9). In support of the anticipatory intelligence objective, the 2019 NIS seeks to increase common understanding of the “scope, definition, tradecraft, and methods of anticipatory intelligence across the community to develop workforce proficiency in these skills” (ODNI 2019, 9). Though in this regard, there is no mention of outreach to scientific communities which have various Futures Studies methodologies at their disposal. Fittingly, both 2014 and 2019 NISs transition from anticipatory intelligence to current operations or current operations intelligence. Afterall, a warning intelligence given in a timely manner must be both anticipated and current, yet often

stemming from strategic considerations. Current intelligence, in both strategies, encompasses military, diplomatic, and homeland security operations. Moreover, it is connected to domestic and global partners. (ODNI 2014, 8; ODNI 2019, 10.)

The SSCI activities reports were touched upon in Chapter 3.4, were several contextual and critical perspectives were highlighted. These reports address analytical and workforce themes principally under the heading “Intelligence Community Issues”. Above all, the 2019 report said HPSCI was told that the IC cannot provide statistical evidence as to whether the IC CAE program is fulfilling its objectives (SSCI 2019b). Regarding the institutional curriculum level, the 2011 SSCI report for years 2009–2011 mentioned multiple issues affecting intelligence analysis: community-wide standards for analytic tradecraft; analyst recruitment, training, utilization, and retention; the balance between reporting current intelligence and long-term strategic analysis; and the status of analytic collaboration and intelligence-sharing within and among intelligence agencies. These issues were current as part of the ongoing wider “analytic transformation” of the IC, as mandated by the 2004 IRTPA reforms. Regarding the IC CAE program, the Committee wanted to ensure the program provided potential returns of investment, and that educational programs produced “quantitative and qualitative increases in the national talent pool from which the IC recruits”. Additionally, the Committee found “serious shortfalls” for languages capabilities critical to the IC mission. Interestingly, these deficits combined with the proliferation of open source information and other means were found to have affected intelligence collection and analysis. (SSCI 2011, 25–27)

The SSCI 2013 (2011–2013) report contained similar and virtually identical remarks on the progress of the IC’s “analytic transformation”. The Committee reviewed the regional intelligence analysis of the 2011–2012 “Arab Spring”. Regarding languages, the Committee maintained that foreign language development across the IC had been “intermittent and inconsistent”. IC CAEs were mentioned briefly in a monitoring context, as the Committee had met academic professionals and program managers regularly. Moreover, the DNI Clapper had told the Committee in a Worldwide Threat Hearing, that the IC elevated cyber threats in the same category as terrorism and proliferation of WMD. Subsequently, the Committee undertook a review in 2012 to study the IC’s cyber analytic programs and workforce. (SSCI 2013, 20–21; 18.) SSCI’s 2015 report (2013–2015) did not address the IC CAE programs. The Committee said it believed the IC could improve its warning intelligence capability, as it perceived the “government was partly caught off guard by global events such

as the Arab Spring, Russia's incursion into Crimea, and the ability of ISIL to quickly overrun a significant amount of territory in Iraq. The Committee wrote it had reviewed the IC's warning offices and tradecraft. Furthermore, it said it had met with ODNI representatives to discuss methodologies and analytic tools behind IC's forecasting capability. The Intelligence Authorization Act for Fiscal Year 2015 had required the DNI to better implement anticipatory intelligence across the IC. (SSCI 2015, 15.) During 2015–2017, the SSCI said it had continued its review of the IC's management methods for ensuring "high-quality, timely, relevant, and impartial analysis" by holding several hearings. It also said it assessed ODNI's efforts to lead IC's analytic workforce, training, practices, and products. (SSCI 2017, 15.) Science, Technology, Engineering, and Mathematics (STEM) fields were specifically mentioned in connection with a respective investment strategy for outreach and recruiting efforts, and salary increases for IC employees with STEM backgrounds (SSCI 2017, 5–6). The Committee expressed its satisfaction with the passing of the Cybersecurity Act of 2015 into law and stressed the priority of the IC to develop its cybersecurity tools and talent to anticipate and mitigate cyber threats. (SSCI 2017, 9.)

For the 2019 SSCI report (2017–2019), the Committee said it had continued its oversight of the space domain. Hearings and roundtables assessed budget issues, cross-cutting technology developments, as well as analytic challenges. NRO and NGA were mentioned as IC points of contact with whom the space overhead architecture topics were engaged. Another theme arising from the report was analytic outreach to various external partners pertaining to Information Influence Operations (IIOs) and other exploitation of social media. Four hearings were held on subjects such as state-sponsored actors manipulating public discourses using social media platforms, and the corporate response to such use by "agents linked to Russia". (SSCI 2019a, 12.) The Committee said it had heard the groups Data for Democracy, Graphika, and the Oxford Internet Institute, who had "specialized expertise in digital data and social media intelligence, as well as data analytic capabilities otherwise unavailable to the Committee". Social media companies Facebook, Twitter, and Google provided the data for this analysis, which addressed the Russian Internet Research Agency's (IRA) information operations in the US around the 2016 elections. (SSCI 2019a, 14–15.)

The additional SSCI report of 2019 (SSCI 2019b) addressed the IC CAE's curricular content more closely than any other of the SSCI report sampling units. Under the subheading "Leveraging Academic Institutions in the Intelligence Community", the Committee wrote:

> "The Committee encourages the DNI and the Director of the DIA to ensure that *IC elements continue to forge tighter partnerships with leading universities and their affiliated research centers* in order to enhance *mutual awareness of domestic and international challenges, leverage subject matter experts from higher education* in *a manner that uses cutting edge technologies and methods*, and bolsters the recruitment of top-notch, diverse, and technically proficient talent into the IC's workforce [emphasis added]. (SSCI 2019b.)"

This citation illustrates the value that outreach to academia is expected to produce. The goals of "enhancing mutual awareness of domestic and international challenges" is indicative of the interface of institutional and programmatic curricula, as these security concerns are shared within the national political domain. Outreach to the academia, then, is expected to produce not only new insight, but analytical innovation ("cutting edge technologies and methods"), and expert workforce. And to the Committee continues to elaborate on curricular wishes:

> "The Committee further believes that IC-sponsored academic programs such as the Intelligence Community Centers for Academic Excellence (IC-CAE) should work closely with educational institutions that offer *interdisciplinary* courses of study and learning opportunities in *national and international security; geopolitical affairs, international relations and national security; interdisciplinary courses of study in the culture, history, languages, politics, and religions of major world regions; foreign language instruction; computer and data science; or cybersecurity* [emphasis added]." (SSCI 2019b.)

To its merit, this report is the only observed instance within the sampling units which so explicitly specifies the SSCI's expectations of the IC CAE programs' curricular content (or study areas) at the intersection of the institutional and programmatic levels. Combined with the additional investments in STEM fields of expertise mentioned in SSCI 2015 and SSCI 2017, the inclusion of all these academic disciplines is emblematic the SSCI's acceptance of the all-encompassing quest for knowledge that the IC is expected to pursue.

The most recent SSCI report of 2021 (2019–2021) said the Committee conducted oversight of the IC's analytic enterprise, emphasizing analytic objectivity and duplication. They also paid attention to the analysis "meeting customer demands, devoid of politicization and compliant with standards for objectivity, and properly resourced". Committee staff engaged with the IC to understand and reduce analytic duplication, while "recognizing the virtue in analytic redundance to promote diversity of perspective". Further, they addressed hiring and retention for "hard-to-fill analytic positions". Another theme under the "IC Issues" heading was fifth-generation telecommunications technology (5G). To that end, the Committee mentioned engagement with "Five Eyes nations and other allies to mitigate potential national security vulnerabilities". Regarding cybersecurity, a new senior position of Cyber Executive

was created by the ODNI to oversee cyber threat intelligence. The Committee also observed "turbulence" in various personnel, organizational, and policy changes during the 116th Congress (which coincided with the last two years of Donald Trump's administration). The Committee said personnel changes, principally the forced resignations of the DNI Dan Coats, PDDNI Sue Gordon, among other senior leadership. These changes "created instability and leadership gaps that demanded close attention to ensure the DNI's statutory functions could still be performed. In review of ODNI policy and programmatic initiatives, the Committee said it closely monitored "workforce initiatives to recruit, hire, develop, and retain a quality, diverse, and trusted workforce. (SSCI 2021, 11–14.) The IC CAE program was not addressed directly in the report. A final theme that continued from the 2019 report was oversight of the IC's role in space intelligence. The Committee saw the space environment as increasingly hostile, prompting urgency in responding to respective intelligence requirements. (SSCI 2021, 15.)

The six Intelligence Community Directives (ICDs)[32] included in the sampling units start from ICD 203 Analytic Standards (ODNI 2015a). It is the ICDs that serve as the bridge between IC's basic analytical expectations applicable to the whole analyst workforce of the IC, and programmatic curricula that nurtures these skills. The ICDs, however, are not representative of the substantive knowledge and sciences areas that the IC must employ in intelligence analysis. They describe the general analytic procedures underlying *all* analysis. The Analytic Standards of the ICD 203 (D.6.a–e) "govern the production and evaluation of analytic products" across the IC ("purely law enforcement information" notwithstanding), containing the five Analytic Standards themselves, and nine Analytic Tradecraft Standards (D.6.e.1–9). In sum, the Analytic Standards comprise the following principles:

- D.6.a: Objectivity: Analysts are aware of their own assumptions and reasoning. They employ reasoning techniques and practical mechanisms that reveal and mitigate bias. Analysts must consider alternative viewpoints and contrary information and be aware of existing analytic positions.
- D.6.b: Independence of political consideration: Particular audiences, agendas and policy viewpoints must not distort analytic assessments.

[32] Each section of the ICDs is referenced here the same way the documents self-reference and cross-reference each other. Each ICD usually has six sections (A. Authority, B. Purpose, C. Application, D. Policy, E. Responsibilities, and F. Effective Date), out of which D. outlines the actual content of the ICD. So below, for instance, ICD 203's Policy section D and its subheadings are referenced in an ordinal sense.

- D.6.c: Timeliness of analysis: Analysis must be disseminated in time to be actionable.
- D.6.d: Analysis must be based on all relevant, available sources of intelligence information: Analytic and collection elements must cooperate to identify and address critical information gaps. (ODNI 2015a, 1–2.)

These standards contain a range of expectations. Objectivity includes the mitigation of cognitive biases, which is done in the IC with the help of Structured Analytic Techniques (SATs), or "practical mechanisms" as put in the ICD 203. The problem is that dozens of biases have been identified in affecting various analytical tasks, and the SATs remain empirically untested as to how they contribute to mitigating these biases. So far, research applied to two common biases (confirmation bias and serial position effects) are not compelling. (Whitesmith 2019, 225–226; Whitesmith 2020a, 226). Consideration of alternative viewpoints and contrary information point out to the fact that intelligence agencies build on existing intelligence, such as baselines, previous sources, and products (Marrin 2011, 21; Clark 2013, 17–20). Analysts, therefore, must be able to accommodate information that may introduce discontinuity – just as researchers adjust their conjectures when conflicting information comes to light.

Standards D.6.b and D.6.c are quite self-explanatory, but D.6.d is, once again, a lofty goal. Certainly, such organizational gaps as "the Wall" that obstructed effective intelligence sharing between the domestic and foreign intelligence settings have been dealt with in intelligence reform (Durbin 2017, 213–214). Considering the range of open and clandestine sources available, even attaining "all relevant information" is very case-specific, may require expensive and expansive collection, and involve intelligence liaison. To summarize, these Analytic Standards do set high standards for analysts. Objectivity entails the use of SATs or other ways to acknowledge and mitigate bias. Such problems are examined in various academic courses of critical thinking, philosophy and logic, and those themes are expanded below in the analysis of the programmatic curricula. The inclusion of all relevant data and exclusion of other is a common issue in social research in general. Compromises must be made at certain times, and sometimes relevant information is simply left out obliviously. Thus, despite the expectations, even intelligence conducted with the highest of diligence is may unwittingly leave out relevant facts.

The fifth Analytic Standard is D.6.e. the implementation and exhibition of the nine Analytic Tradecraft Standards. The first tradecraft standard D.6.e.1 is about the quality and credibility

of sources, addressed in depth in ICD 206. Standard D.6.e.2, however, pertains to uncertainty and Words of Estimate Probability (WEPs). As tradecraft holds, analytic products must indicate and explain the basis of the uncertainties related to their major analytic judgments. Two estimates are therefore integrated to these judgments: degree of *likelihood* of an event occurring, and the analyst's *confidence* in the basis of their judgment. The standard encourages analytic products to both note causes of uncertainty (e.g., type and amount of information), and explain how uncertainties affect analysis (e.g., the judgment's dependence on assumptions). For the WEPs, two parallel lexicons are given (probably due to different agencies utilizing different sets of terms; the WEPs were listed in Table 3, Chapter 4.4.). Analyst confidence, on the other hand, is directed to use a confidence level "e.g., high confidence". (ODNI 2015a, 3.) For these expectations, scholars have noted many discrepancies (Chapter 4.4). First, the basic problem with WEPs such as "remote", and "almost no chance" signifying the same level of likelihood (1–5%) is the fact that people in general interpret these linguistic probabilities differently, based on different personal attributes. In addition, analysts can exploit linguistic probabilities to minimize blame by assigning overly negative-outcome probabilities or minimizing positive-outcome probabilities. One suggestion to avoid miscommunication is to rather assign numeric probability intervals, where one can infer the midpoint and margin of error. (Mandel & Irwin 2021, 561–563.)

Friedman and Zeckhauser have argued that these numeric probability intervals would better serve their purpose if condensed to single points (numeric interval of 1–5% resulting in a single point of 3.5%). They specifically argue against decision-makers having to calculate the averages from numeric intervals, as decision-makers may default to an incorrect assessment (such as Obama's 50/50 assessment in the Abbottabad example, whereas the correct average was 69%). (Friedman & Zeckhauser 2015, 77–78; 86.) Admittedly, the calculation of probability averages should not be the decision-makers' task. As for the expression of confidence in a given probability figure, Mandel and Irwin criticize the "coarse" ordinal ratings of low, medium, and high levels. Moreover, the demonstrate how the analyst's confidence is reflected in the numeric probability interval (the wider the interval, the less confidence there is in the probability figure), and how analysts have mixed confidence and probability estimates. (Mandel & Irwin 2021, 563–565.) These propositions for improved WEPs are ultimately questions of tradecraft within the IC, but it is evident from the articles cited above that academic scrutiny may insightfully point out analytic deficits. If translated to

curricular expectations at the intersection of the institutional and programmatic level, basic literacy in mathematics and statistics, as well as logic of argumentation are expected in this regard.

And there are more expectations in the ICD 203's Analytic Tradecraft Standards. Standard D.6.e.4 is about the incorporation of analysis of alternative hypotheses. It is not clear whether it includes the eponymous ACH, but it predicates a degree of creative intuition and abduction. More relevant to the curricular levels coding units and themes is Standard D.6.e.6, which requires analysts to use clear and logical argumentation. Main analytic messages are drawn from subsets of arguments, reasoning must be coherent, and language and syntax should convey meaning unambiguously (ODNI 2015, 4), just as in soundly reasoned research. Standard D.6.e.6 expects products to explain change to or consistency of analytic judgments communicated in previous analysis or coverage of a topic, underlining the continuity of reporting in, for instance, recurrent crisis reports. (ibid.) Standard D.6.e.9 advices analysts to incorporate effective visual information where appropriate, "to clarify analytic message and to complement or enhance the presentation of data and analysis". (ibid.) Standards D.6.e.4, D.6.e.6, D.6.e.7, and D.6.e.9, therefore, are comparable to basic tenets of systematicity, coherence, logic of argumentation and other fundamentals of research in general. These requisites are basic academic skills, but their gravity is emphasized in the intelligence analysis context, as political expectations are high and intelligence informs fast-paced decision-making (Fingar 2011, 4.) The foundations for these analytical skills can be strengthened in the academic environment, and as the analysis level of programmatic curricula below demonstrate, intelligence minors and degrees often apply composition and communication courses to this specialized need.

ICD 204, National Intelligence Priorities Framework, concerns national intelligence priorities and the President's role in directing those efforts. Apart from elaborating on the role of the DNI vis-à-vis the President (ODNI 2017a), it contains no relevant information on the institutional of programmatic curricula. ICD 205 Analytic Outreach on the other hand, "establishes policy for Analytic Outreach as an essential factor in the production of intelligence analysis that responds to the National Intelligence Priorities Framework". Analytic outreach is defined as "overt and deliberate engagement by an IC analytic component with individuals and organizations outside the IC", which are referred to as Outside Experts (OEs). OEs may be either US or non-US person and may be compensated for their participation in these outreach activities. OEs are by definition separated from overt

or clandestine HUMINT collection, as well as formal liaison relationships with foreign intelligence services, domestic partners (Federal, State, local, tribal, and private sector), or contracting of OSINF (ODNI 2013, 1). These distinctions are important in understanding the ethical and operational relationship between academic institutions and intelligence agencies in the universities-security-intelligence nexus. The ICD 205 demonstrates how OEs are expected to provide depth and context to the analysis of intelligence questions, and new lines of inquiry. Contributions by OEs may be used in finished intelligence products and are instructed to be identified and cited accordingly. “Significant risks” to OEs and related IC personnel, and missions in outreach activities are also acknowledged, necessitating the maintenance of appropriate counterintelligence and security, especially regarding overseas OEs. (ODNI 2012, 2–3.) All in all, the ICD 205 sets expectations for the analysts to utilize outside expertise to improve the quality of intelligence analysis, although the standard does not associate the OEs directly with the academia.

ICD 206 Sourcing Requirements for Disseminated Analytic Products details the sourcing aspect of ICD 203. ICD 206 requires sourcing information to be included in analytic products for credibility and transparency of intelligence analysis, and to “enable readers to discover and retrieve sources”. Exhaustiveness of sourcing, however, is to be avoided. Sourcing is extended to all analytic products, though if distributed to foreign partners, classification scheme may be more sensitive, and some exemptions may be requested. (ODNI 2015b, 3–4; D.4, D.7.) ICD 206 offers little insight to institutional or programmatic curricula but shows how traceability of sources for the agencies themselves, and inclusion of references for audience readability attempt systematize and render the analytic process more transparent. ICD 207 establishes the functions and personnel of the National Intelligence Council. In addition to other NIC personnel, ICD 207 assigns the role of the National Intelligence Officers (NIOs) as the most senior intelligence analysts drawn from the ranks of intelligence analysts, and substantive experts from other government agencies, academia, and the private sector. In supporting the DNI and the NIC, the NIOs are expected to “bolster analysis in the IC through exemplary use of analytic tradecraft and standards, effective use of alternative analyses, collaboration within the IC, and by experimenting with and creatively applying new analytic techniques and tools to substantive issues”. Moreover, the NIOs are set to lead strategic analysis in the IC, and articulate substantive intelligence priorities within the IC. The NIC in general is assigned to perform outreach functions to nongovernmental experts in academia, think tanks, private sector and foreign governments to “broaden the

IC's knowledge". (ODNI 2008, 3–4.) ICD 207, then, elaborates on the NIC's role, as the NIC bears responsibility for such high-profile products as the NIEs, and demonstrates the all-source knowledge the NIC as part of the ODNI is expected to synthesize.

Finally, ICD 208 Maximizing the Utility of analytic Products, seeks to maximize utility of analytic products by "facilitating wider dissemination and enhancing the quality of information and analysis shared", which essentially refers to the customer end of intelligence products. The D.2.c.1–3 contain subsections on producing analytic products for tailored re-use, and for many non-traditional customers (federal, state, local, and tribal levels, and foreign governments) and international partners such as NATO and Five Eyes. For instance, tearlines, analytic products with lowest classification levels, will be produced (they are governed by ICD 209 Tearline Production and Dissemination). Sections D.2.d and D.2.e promote the discoverability, accessibility, and transparency of analytic products. (ODNI 2017b, 1–2.)

Based on the analysis above, several observations have converged into an image of the institutional curriculum. The institutional curriculum, of course, is not a policy document or a real-world object. It is abstracted theoretically to describe what is desirable in the social and cultural orders, and what is valued and sought after by members of a society and nation (in this case, in the national security and the intelligence analysis enterprise) (Deng 2009; Gearon 2020; Svendsen 2012b.) The primary sources at the institutional level of curriculum involve the conjunction of two dimensions of curricular areas. First, the theme of *Improvement of Analytic Tradecraft and Intelligence Analysis* is apparent from the detailed and standardized ICD guidance as to how analytic products are made. The ICDs establish parallels between social scientific and academic conduct and intelligence analysis (Marrin 2011; Walsh 2020, 98), including objectivity, impartiality, logical and linguistic coherence of argumentation, sourcing, and transparency of the contents of an analytic product (ICDs 203, 206). While the image of science conveyed in the foundational ICD 203 it has been criticized (Marrin 2020), some have nevertheless seen the development of professional standards for intelligence analysis as a positive step, as it allows for the tradecraft to evolve on its own specific terms (Reinhold *et al*. 2021). And the SSCI as congressional overseer of intelligence analysis, and well-informed one at that, no longer referred to the "analytic transformation" after its reports of 2011 and 2013, which might indicate they deemed the standardization efforts well enough implemented for now. Indeed, the set of themes called *Improvement of Analytic Tradecraft and Intelligence Analysis* implies the continuing evolution of analytic

practices, constantly keeping up with the changes that transpire in the strategic environment and the offerings of parallel provides of information (Mandel & Irwin 2021).

A fundamental issue, however, lingers on in the analytic tradecraft. It does not seem plausible for the IC to adapt analytic tradecraft to outside critique dexterously, as ICDs would have to be constantly updated at the ODNI level. For instance, the criticisms of Friedman and Zeckhauser (2015), and Mandel and Irwin (2021) towards the use of WEPs in ICD 203 (probability expressions and confidence in said probabilities) are elaborately argued, but could the ODNI reactively implement new standards, for instance, annually, without introducing corrosive effects to analyst morale? Furthermore, as the SATs have become increasingly popular outside the IC, their effectiveness has been questioned on scientific grounds (Whitesmith 2019, Whitesmith 2020a). If Spiegel's (2021) interpretation of the SAT's underlying the IC's forecasting paradigm is true, this concerningly puts the credibility of anticipatory intelligence under question. These remarks highlight the significance of analytic outreach and OEs, not only in one-way substantive consultations, but in the dialog between academia and intelligence analysts in general. While Landon-Murray (2011) was wary of intelligence education reactively adopting the IC's "pathological" tendencies, academies can also provide checks and scrutinize these methodological deficiencies (such as the overreliance on SATs). The intelligence community can incrementally implement better practices at the pace it can – that is, the pace of bureaucracies.

The second curricular area that conjuncts with the coding unit theme of *Improvement of Analytic Tradecraft and Intelligence Analysis* is the *Strategic, Disciplinary, and Scientific Knowledge* coding unit theme. This theme sets the foundations for understanding the phenomena underlying strategic, anticipatory, and ultimately, all intelligence (Walsh 2020, 98). Gearon (2020) conceptualized the totality of the epistemological pursuits of the IC as all-source intelligence. The substantive knowledge, then, must address deep context, and understanding (ODNI 2014), and be strategic in its depth, as it concerns most observable natural and social phenomena. This strategic knowledge is not only connected to the operational, epistemological, and ethical domains of the universities-security-intelligence nexus, but also the existential. Universities were involved in researching the existential threat of nuclear devastation during the Cold War, as were intelligence agencies. After 9/11, universities joined to research terrorism, and were affected by counterterrorism policies. (Gearon 2020, 58–59.) Still, it could be argued, that intelligence agencies prioritize the nation

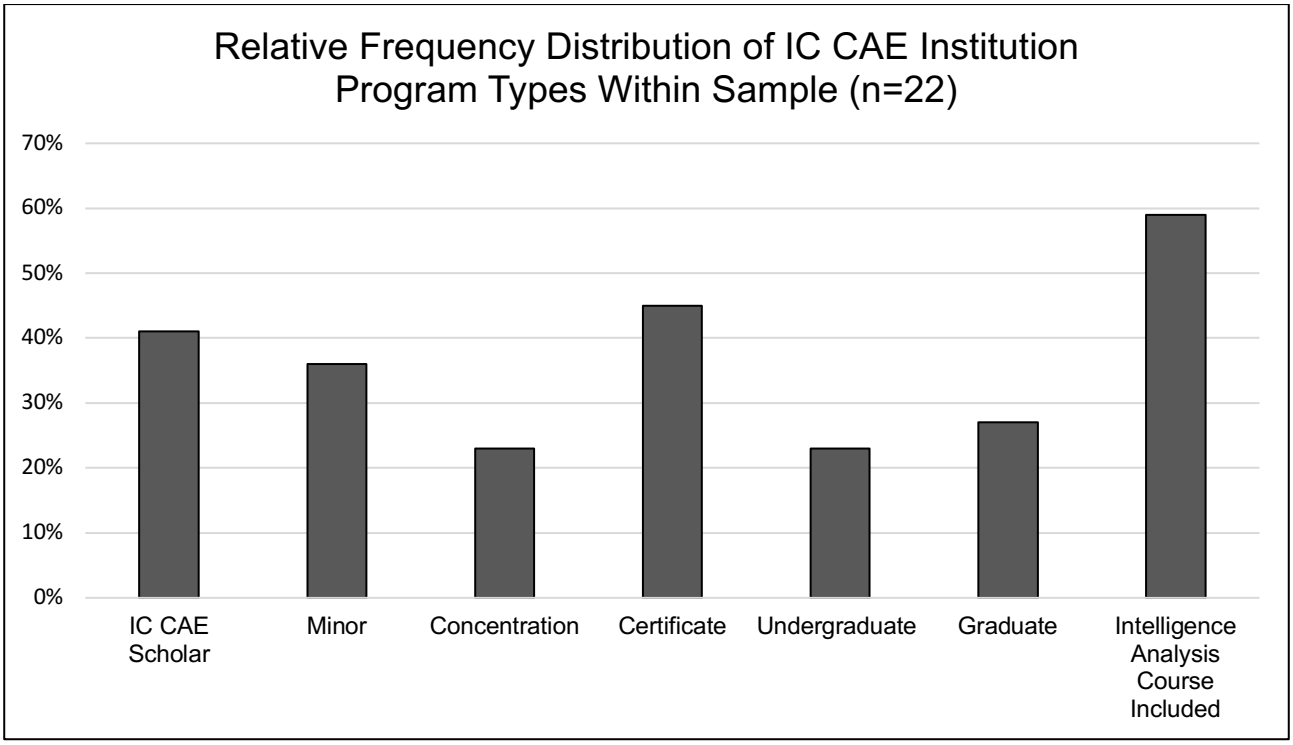
instead of the collective of nations and peoples in the quest for knowledge against threats, and this is where intelligence and the universities diverge in the existential domain.

The themes of *Strategic, Disciplinary, and Scientific Knowledge*, ultimately, rather unite than separate intelligence actors and the academia, and therefore the need for academic deep knowledge is so important for the intelligence agencies, and the institutional and programmatic curricula. Analytic tradecraft informs how the overarching domains of knowledge are synthesized in intelligence analysis. The above analysis above provided some explications of the scientific domains involved. The NISs variables for analysis and the ODNI's IC CAE guidance readily converge with the substantial expectations of the SSCI (2019), whose surprisingly "curricular" statements mentioned various interdisciplinary courses. These domains of knowledge include social sciences (international affairs, geopolitics, national security, intelligence studies, politics etc.), humanities (culture, history, languages, religions), computer and data science, cybersecurity, and Science, Technology, Engineering, and Mathematics (STEM). In summary, it can be said that at the level of institutional curriculum, the need for professional workforce with substantive expertise is all-encompassing. This need is connected to the trends occurring within the sample of the IC CAE institution program types, as analyzed below.

This subchapter has established reoccurring indications that the institutional curriculum, as conceived within the theoretical framework of the study, consists of the conjunction of expectations towards analytic tradecraft, and strategic knowledge areas of intelligence analysis. Further, the analyzed ODNI and SSCI documentation has recursively consolidated the significance of academic outreach (as evident in the policies of Analytic Outreach and OEs) for strategic intelligence analysis, the intelligence community's general awareness of the strategic environment, and prospective workforce emerging from multiple domains of higher education. These findings are now reflected against the theoretical level of the programmatic curriculum, examined through the sample of 22 IC CAE institutions' curricula.

5.2. The Programmatic Curriculum: The Benefits of Academic Rigor

Figure 3 Relative Frequency Distribution of IC CAE Institution Program Types Within Sample (n=22).



Some noted trends are observable in the sample of the IC CAE institutions' program types. Figure 3 shows the relative frequencies of IC CAE Scholar, minor, concentration, certificate, undergraduate and graduate types of content offered within the sample. The program type categories are not mutually exclusive. In addition to the baseline IC CAE Scholar mentioned in 41% of the curricular descriptions, 45% of the programs offered certificates, and 36% minors in intelligence-related content. These trends align with the observations of Landon-Murray & Coulthart (2020, 270–274),[33] and are supported by some prominent instructors' arguments for intelligence education (Dujomovic 2017; Lowenthal 2017). Few of the program types were undergraduate (23%) or graduate (27%) degrees. Moreover, out of the sample, majority (59%) of the programs had integrated dedicated intelligence analysis courses to their curricula. The high frequency of IC CAE Scholar, certificate, and minor types of programs indicate that the IC CAE program may act as a bridge for potential recruits in substantive areas by introducing the intelligence enterprise to students otherwise detached from national security policy themes. The formal requirements to be accepted as an IC CAE Scholar, after all, are not very demanding, as they minimally require at least one completed

[33] See also Figure 4 Relative Frequency Distribution of IC CAE Institution Program Types Within Population (N=71) in Appendix.

course in the IC CAE study areas (ODNI 2022b). Since the professionalization of intelligence tradecraft has been driven by the "codification" and consolidation of intelligence analysis practices in the ICDs, the gap between substantive areas of study and intelligence analysis can be bridged via in-house training and education. The continuing dominance of intelligence studies minors and certificates within the IC CAE curricula indicate the openness towards the multiplicity of scientific avenues that are needed in intelligence analysis.

The coding units applied to the analysis of the sample IC CAE curricula consist of the four themes within procedural knowledge: *Data Management, Analysis, Communication, and Operational Skills*. They are further divided to more specific, operational themes. Based on the coding, most prevalent code categories were both *Intelligence Analysis (General)* (21) and *Intelligence Analysis (Methodologies and Methods)* (20), and *Communication (Written Communications* (18), and *Verbal Communications* (13)), which almost always occurred congruently. Within the intelligence analysis-specific subset of coding units of *Intelligence Analysis (Methodologies and Methods)*, *Critical Thinking*, and *Structured Analytic Techniques (SATs)* occurred almost equally many times (11 and 10). Moreover, *Geoinformatics (GIS)*, and *Open Source Intelligence (OSINT)* were featured in equal frequency (6). *Structured Analytic Techniques (SATs)* occurred 10 times. Table 4 in Appendix lists the frequencies of the programmatic curriculum coding units and subunits.

In general, what characterizes the sampling unit is the methodological and methodical poverty compared to Coulthart and Crosston's relative plurality of analytical subjects in their curricular sample (2015, 59–60; Figure 4). Subsequently, most of the course descriptions for introductory intelligence courses were expository, where general principles of intelligence analysis, critical thinking, intelligence-specific verbal and written reporting, and SATs were combined. Most degree programs featured general academic courses on mathematics, statistics, composition, and sometimes philosophical logic in addition to these intelligence-specific introductory courses. This may indicate that there is a general acceptance for the programmatic content for introductory intelligence courses to include analytic tradecraft features, as specified in the ICDs. For instance, University of Arizona (2022a), University of Kansas (2022b), University of North Carolina in Charlotte (2022b), Chicago State University (2022b), and University of South Florida (2022b, 2022c) had direct reference to Analytic or Analytic Tradecraft Standards as expressed in the ICD 203. These occurrences were often congruent to *Critical Thinking*. For example, University of Arizona's (2022b) course

“INTV326 Introductory Methods of Intelligence Analysis” was almost purely tradecraft-oriented course. Its description was as follows:

> “INTV326 will provide students with an introduction to Intelligence Analysis and how intelligence professionals can incorporate tradecraft, including critical thinking and structured analytical techniques, to challenge judgements, identify mental mindsets, stimulate creativity, and manage uncertainty within the framework of providing sound assessments to decision-makers at the Strategic, Operational and Tactical level of war.” (University of Arizona 2022b.)

The course description also included the ICD 203’s Analytic and Analytic Tradecraft Standards, as well as several intelligence frameworks (ASCOPE, DIME, PMESII),[34] and network analysis. The University of Arizona’s Bachelor of Applied Science (BAS) was one of the only proper intelligence analysis degree program-level offerings within the sample, having three specialized tracks for intelligence (Operational Intelligence, Information Warfare, Law Enforcement Intelligence). The program has multiple intelligence collection and analysis-centered courses with a seemingly hands-on approach. (University of Arizona 2022b.)

An omission related to ICD-informed tradecraft were the Words of Estimative Probability (WEP) as described in Chapter 4.4. and deemed important for the institutional curriculum of intelligence tradecraft above in 5.1. One course did refer to “managing uncertainty within the framework of providing sound assessments to decision-makers at the Strategic, Operational and Tactical level of war”, in congruence with ICD 203-informed tradecraft and thus, likely included these practices (University of Arizona 2022b). No course within the sample mentioned assessments of probability or likelihood within the intelligence analysis context, although such content is probably addressed in courses like “MATH112 Contemporary Mathematics”, “Statistics I”, or “Intermediate Algebra” (New Jersey City University 2022, B.S. in National Security Studies). Additionally, it is likely that programs like University of Texas at San Antonio’s (2022b) Master of Science in Data Analytics or more cyber oriented programs feature foundational skills in probabilistic modeling. Whereas several programs included basic statistical analysis in their curricula, none had mentions of Bayesian statistics, perhaps due to the advanced nature of such statistics (Clark 2019, 202).

[34] ASCOPE (Areas, Structure, Capabilities, Organizations, People, Events), DIME (Diplomacy, Information, Military, Economic), and PMESII (Political, Military, Economic, Social, Information, Infrastructure) are common frameworks for assessing the factors at play at various analysis scenarios (see e.g., Clark 2019).

A surprising finding within the curricula was the lack of anticipatory intelligence, or Futures Studies course content. University of New Mexico's (2022b) undergraduate certificate in National Security and Strategic Analysis (NSSA) did mention "skills in analysis methods and strategic forecasting" as one knowledge area of the certificate, but no dedicated course was required. University of Arizona's (2022b) course "INTV344 Target Centric Analysis" had the learning goal to "examine and improve the estimative process to utilizing predictive analysis, estimative forces, and alternative scenarios and competitive simulations," while the course focus itself was not anticipatory. The lack of anticipatory course content was peculiar since the institutional curriculum, as conceived above, highly values various social scientific, humanistic, and STEM disciplines that provide contextual understanding to anticipation, foresight, forecasting, and warning intelligence. Anticipatory intelligence, as said, is the second priority of the NIS, and the 2019 iteration sought to increase the respective tradecraft and methods further (ODNI 2019, 9). The SSCI demonstrated its interest in the IC's warning intelligence tradecraft and forecasting methodologies and analytic tools, as it perceived geopolitical events between 2011 and 2015 had partly surprised the government (SSCI 2015, 15). It is interesting how many discussions of the predictive efforts of intelligence have sidelined the field of Futures Studies (e.g., Agrell & Treverton 2015 discuss about forecasting and prediction at length without mentioning Futures Studies), given that the discipline offers an established field of philosophical and methodological foundations for a multiplicity of anticipatory techniques (Bell 2003; Poli 2019). Possible explanation could be the general immaturity of the IC CAE program content if measured against the IAFIE standards, as noted in one study (Ramsay & Macpherson 2022, 13–14), or suspicions about the "futurology" involved.

This subchapter of the analysis has established several connections and disconnections between the conjectured institutional curriculum analyzed in Chapter 5.1, and the programmatic curriculum. Whereas the analysis indicates that most introductory courses of intelligence had synthesized general academic principles (coherent written and verbal communications, argumentation, and critical thinking), the had also tailored these supportive elements in terms that complement the writing and briefing practices of the intelligence enterprise. Furthermore, Structured Analytic Techniques (SATs) were often associated with critical thinking and the awareness of cognitive biases, although their efficacy has been questioned. These observations may indicate that among the sample curricula, a general acceptance of analytic tradecraft methodologies has emerged, which treat intelligence

analysis as a specific practice among other, more academically inclined teaching content. Few of the sample curricula were degree program-based, instead favoring minors and certificates. This observation readily connects with the projected institutional curriculum need for various disciplines of science and domains of knowledge.

While there is a clear theorized connection between the coding unit themes of *Improvement of Analytic Tradecraft and Intelligence Analysis* and *Strategic, Disciplinary, and Scientific Knowledge* and the programmatic content of the procedural knowledge areas, the most pronounced disconnection was the relative lack of anticipatory curricular content. It would stand to reason that the academia educates prospective analysts with the foresight, forecasting, and anticipation techniques offered by Futures Studies, unless the IC specifically wanted to train the methodologies used in anticipatory intelligence in-house. This omission stands out as the most peculiar feature, the anticipation of futures is so inherently part of the predictive attempts of intelligence, and the heavy political expectations placed upon intelligence analysis. Then again, if the true reasons of prominently publicized intelligence failures lie in faulty sources, tradecraft and other practices and not incorrect anticipations, perhaps it is not the anticipatory methodologies but the general analytic tradecraft that needs improvement. And while that process has evidently progressed in the last decades, it is also something the academia continues to contribute to.

6. CONCLUSIONS: THE QUEST FOR KNOWLEDGE RE-EVALUATED

6.1. Results

This research set out to investigate the phenomena of institutional and programmatic curriculum formation with two research questions. The first question inquired *what kind of themes arise as expectations for intelligence analysis for the institutional curriculum of intelligence education*. Broadly, two sets of themes arose from the groundwork done in Chapters 3–4 and the analysis of Chapter 5.1., which are conjectured here to describe the institutional curriculum of intelligence education.

The first set of themes, *Improvement of Analytic Tradecraft and Intelligence Analysis* expects intelligence analysis to be objective, impartial, timely, logically and linguistically coherent and to apply scientific practices as reflected in the Intelligence Community Directives standards. The intelligence community, the SSCI, and the ICD standards see intelligence as a continuously improving process that must adhere to high standards but acknowledge the analytic evolution transpiring over time. The ICDs have clear parallels with (social) scientific conduct. The second set of themes, *Strategic, Disciplinary, and Scientific Knowledge*, saw social sciences, humanities, computer and data science, cybersecurity, and Science, Technology, Engineering, and Mathematics (STEM) disciplines as the substantive foundations of all-source, strategic intelligence. Strategic intelligence, then, is expected to be predictive and utilize multidisciplinary domains of science and knowledge to achieve its anticipatory objectives and forewarning.

The second question addressed the effects of the institutional curriculum in the more empirically accessible programmatic curriculum, asking *how the themes of the institutional curriculum are present in the procedural knowledge courses of the IC CAE institutions' programmatic curriculum* (Chapter 5.2.). The program types within the sample were most frequently IC CAE scholar, certificates, and minors, as previous studies have suggested. Compared to earlier research, the selection of intelligence analysis methodologies and methods was limited, with OSINT and GIS-based courses appearing most frequently. Most of the course descriptions for introductory intelligence courses were expository, where general principles of intelligence analysis, critical thinking, intelligence-specific verbal and written reporting, and SATs were combined. A notable feature in the IC CAE programmatic

curriculum was the lack of anticipatory intelligence, or Futures Studies content. The finding was peculiar since the institutional curriculum highly values anticipatory and warning intelligence. Based on the programmatic data, the established field of Futures Studies and its multiplicity of anticipatory techniques remain underutilized in the intelligence education sample.

The results may indicate that there is a general acceptance for the programmatic content for introductory intelligence courses to include analytic tradecraft features, as specified in the ICDs. This prevalence of ICDs could translate to the institutional curriculum successfully consolidating the practitioner tradecraft of the IC as a professional skill, in line with Reinhold *et al*.'s (2021) observations. The academia may in turn inherit some unsound analytic practices (Landon-Murray 2011), such as the use of untested SATs, or unrealistic expectations towards objectivity as present in the ICD 203 (Marrin 2020).

To conclude, the results provide a preliminary glimpse into the phenomenon of curriculum-making. There is a wider dynamic between the academia and intelligence community, in which the academia is valued as an outside expert and counsellor that may point out gaps of knowledge, new lines of inquiry, as well as analytic deficits. Intelligence analysts are educated in undergraduate, graduate, or doctoral degree programs, and provide state-of-the-art competencies to the intelligence community's workforce. In turn, it is well established that the dynamic of intelligence practitioners moving from the intelligence community to the academia transfers knowledge of the intelligence realm to academic study. The theoretical component of universities-security-intelligence nexus has demonstrated the operational, epistemological, ethical, and existential domains at play in this exchange.

The present study has exploratively suggested that it is possible that the sample academia is playing a part in the analytic tradecraft becoming more institutionalized, *with* the incentive coming from the IC CAE program's funding and the national security community. This may provoke more critical voices from the academia yet to come, but also contribute to intelligence analysis attaining a more recognized status as an academic tradecraft, art, or profession. These inferences, however, must be tested in more robust research designs.

6.2. Evaluation of the Results

The present study has prototyped a novel theoretical framework, which has succeeded in informing the institutional and programmatic levels of curriculum. To my knowledge, this is

the first attempt at applying curriculum theory to intelligence education, as previous research has rather mapped the categories of the curricular contents (Crosston & Coulthart 2015; Landon-Murray & Coulthart 2020). The institutional organizations of the ODNI and the SSCI were found to have expectations whose themes featured readily at the programmatic level and were supported by previous research (Landon-Murray & Coulthart 2016; Riehle 2021). Whereas the level of globalization of intelligence, and the universities-security-intelligence nexus were left underdeveloped, they have theoretical potential if further enhanced with more detailed theoretical elements.

The validity of this research rests on three components: face validity, social validity, and empirical validity. This research contributes theoretically and empirically to the academic discussions about the curricular content of Anglo-American intelligence education (e.g., Crosston & Coulthart 2015; Marrin 2018; Landon-Murray & Coulthart 2016; Walsh 2017b), which has seen a surge in research in the past decade (Landon-Murray & Coulthart 2020; Johnson 2020). The connection with this growing body of research establishes the face validity of this study, as these scholars, for instance, had found multiple perspectives on inquiring whether current intelligence education purposefully cultivates new workforce for the IC (Dujmovic 2017; Johnson 2020), or new scholars and experts for other professions (Riehle 2021). The face validity of this study can be further evaluated by members of the academic community (Krippendorff 2019, 361–363). Face validity is connected to the social validity, that is, social and cultural relevance. At the level of the US government, return of investment, transparency, accountability and intelligence oversight are significant questions that define the viability of the IC CAE program (ODNI 2020, GAO 2019, SSCI 2019, Gentry 2021), and research into the curricular context of that program should be useful to them as well. As for empirical validity, this study has not employed validity metrics due to its qualitative nature. However, its research design, coherence, logic of inference and internal validity are described for transparency throughout the study.

6.3. Recommendations for Future Research

Future research should theoretically focus on the universities-security-intelligence nexus level to understand the interchange between the academia and the intelligence community better. Research into the basic dynamics of outreach from the IC to academia could shed light on how intelligence-minded workforce is cultivated, and how intelligence analysis (among other) practices are transferred from the IC to the academia. Conversely, another

avenue is to find out how academic knowledge is transferred to the IC in exchange. These studies could utilize different varieties of network analysis, among other methodologies suitable for studying policy networks. While the efficacy of the IC CAE program is evaluated within the IC at an undisclosed level, public research would allow the public to judge whether the program produces meaningful gains for the investments.

Additionally, a holistic look at the programmatic curricula, including course literature, should be conducted to publicly evaluate whether the curricula offer meaningful content regarding analysis, or whether the common analysis pitfalls such as overreliance on the SATs still befalls the analytic tradecraft. For instance, a bibliometric analysis of the used course literature could be made to identify the inventory of common literature across the program, as has been done before for some programs (Landon-Murray 2013). And certainly, research more cognizant on the educational history of the United States could place the whole phenomenon of intelligence education in its respective political and intellectual context, along the lines of Educational Studies and Curriculum Studies, and zoom in on the phenomenon with the various tools available to these disciplines.

The level of classroom curricula remains obscure within the constraints of this study. Various ethnographic, focus group, and action research designs, and interview-based data collection methods could illuminate this level of teaching and learning with prospectively very useful findings. Both students and educators could be observed and surveyed for classroom curriculum research. The classroom curriculum is an integral realm regarding the IC CAE's workforce goals, where intended future intelligence professionals absorb knowledge of various world phenomena and develop capacity for analysis. It remains unclear whether the ODNI could possibly audit teaching events in sufficient capacity to tap into the classroom curriculum-making. Such an approach, however, even in limited research application would enhance public accountability of intelligence funding (compare: GAO 2019), even if related research would have to be sensitively conducted to not "coerce" or otherwise intrude on students in their learning environment.

Finally, the IC CAE program institutions among others that teach intelligence analysis globally form a prospective pathway for intelligence analysis to be accepted as an academic art, perhaps even science. Observing this potential trajectory enables interesting research designs in philosophy of science and metatheory, but such a development is contingent on how exclusively intelligence analysis is viewed to belong in the realm of secret organizations.

Thus, previous definitions of intelligence analysis need to be re-evaluated against the diffusion of its methodologies into the public sphere.

ACKNOWLEDGEMENTS

This study is a product of the Finnish public education system and scientific community. During the study's gestation period, I have attempted to immerse myself in the scene that is the United States Intelligence Community. My perspective is necessarily that of a cultural and political outsider. Yet volumes of literature, media monitoring and news reading, podcast-listening, and popular culture have painted an interesting picture of the forces and imaginaries at work in the American intelligence context.

Many people have helped realize this academic work, reflecting the collegial nature of the enterprise. I owe my gratitude to the Tampere University Politics Program staff and fellow students that have shared and nurtured my interests in Intelligence Studies. I extend my thanks to those involved in the peer review process of the study and those who have commented on it. Similarly, I am very grateful to all the likeminded and supportive persons I have worked with in the last few years. Your expertise and example have greatly encouraged my professional growth.

APPENDIX

Figure 4 Relative Frequency Distribution of IC CAE Institution Program Types Within Population (N=71).

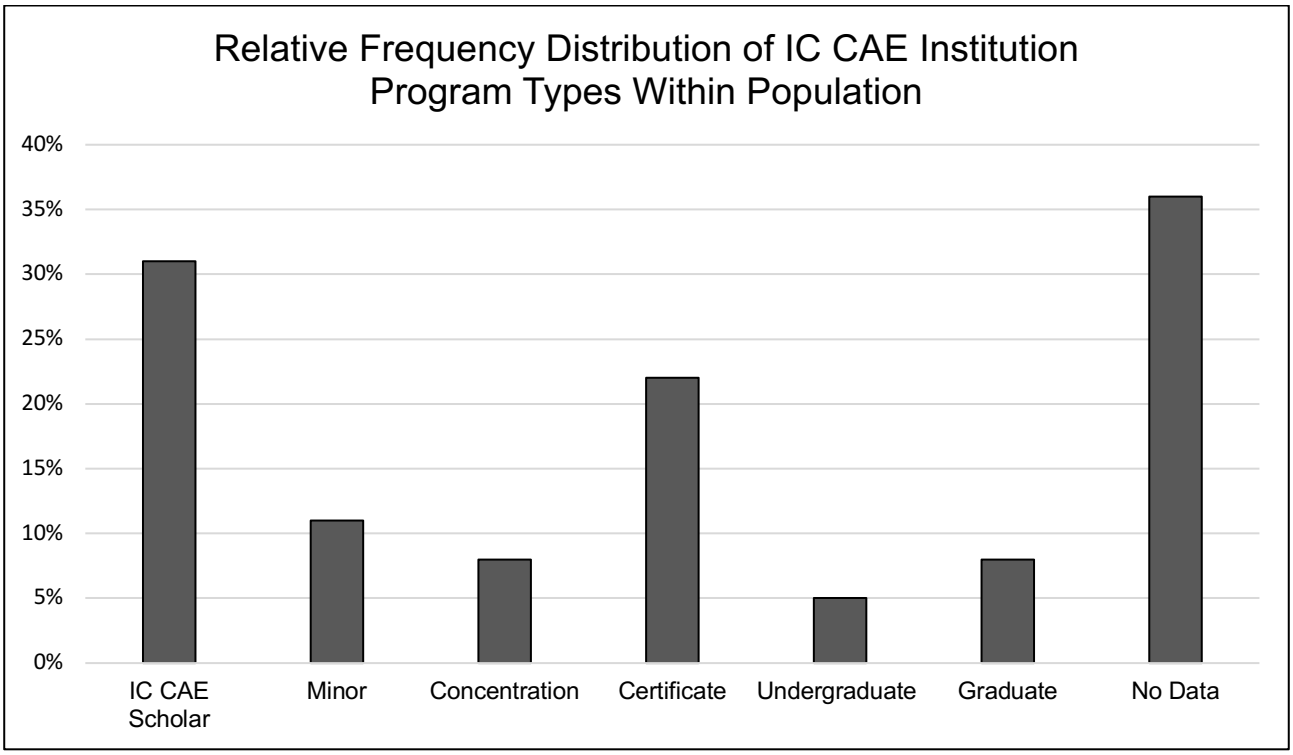


Table 4 Programmatic Curriculum Coding Unit Frequencies.

Procedural Knowledge Operational Themes	**Frequency**
Data Collection	9
Data Manipulation	1
Intelligence Analysis (General)	21
Intelligence Analysis (Methodologies and Methods)	20
Written Communications	18
Verbal Communications	13
Interviewing	2
Espionage Tradecraft	0
Deception Techniques	1
Private and Government Investigations	1

Intelligence Analysis (Methodologies and Methods) Subcodes	**Frequency**
Anticipatory Methodologies	2
Comparative Analysis Methods	0
Criminal Intelligence Analysis	0
Critical Thinking	11
Cryptanalysis (SIGINT, EW)	4
Cyber Threat Analysis	6

Data Analysis	2
Geoinformatics (GIS)	6
Leadership Analysis and Profiling	0
Open Source Intelligence (OSINT)	6
Political Analysis	1
Qualitative Analysis	0
(Social) Network Analysis	2
Structured Analytic Techniques (SATs)	10
Systems and Simulation	0
Threat Analysis	2

Table 5 Legacy IC CAE Institutions as of January 2022 (ODNI 2022a; data compiled by author).

Institution (* denotes a subunit / partner institution to above institution)	**Program type and name**	**Data eligible for research**	**Mandatory intelligence analysis courses**
California State University - Fullerton	IC CAE Scholar	Yes	No
California State University - Long Beach	N/A	No	N/A
California State University - San Bernadino	M.S. in National Cybersecurity Studies, M.A. in National Security Studies	Yes	Yes
Chicago State University	Certificate in Security and Intelligence Studies	Yes	Yes
Duke University	N/A	No	N/A
Eastern Kentucky University	Concentration (Intelligence Collection and Analysis; Threat Specialist; Regional Analysis; Security Operations; Science and Technology), Certificate in Intelligence Studies	Yes	Yes
Elizabeth City State University	N/A	No	N/A
Kentucky State University	IC CAE Scholar, Certificate in Interdisciplinary Intelligence Studies	Yes	No

Miles College	IC CAE Scholar	No	N/A
North Carolina Central University	Certificate in Security Studies	No	N/A
North Carolina State University	N/A	No	N/A
Palo Alto Community College	N/A	No	N/A
Penn State University	N/A	No	N/A
Texas A&M University of San Antonio	N/A	No	N/A
Texas State University	Certificate in Intelligence Analysis	No	Yes
University of Alabama in Huntsville (lead)	Critical Technology Studies Program / N/A	No	N/A
Tuskegee University*	N/A	No	N/A
Alabama Agricultural and Mechanical University*	N/A	No	N/A
University of Mississippi	Minor (Intelligence & Security Studies, Global Security Studies	Yes	Yes
University of Nebraska - Lincoln	IC CAE Scholar	No	No
University of Nebraska - Omaha	IC CAE Scholar	No	No
University of North Carolina, Chapel Hill	N/A	No	N/A
University of New Mexico	IC CAE Scholar, Concentration (Global & National Security), Certificate (National Security & Strategic Analysis; Community Safety & Human Security), P.M.S. in Global and National Security	Yes	Yes
UNM Gallup*	IC CAE Scholar, Consortium partner to UNM	No	No
UNM Los Alamos*	IC CAE Scholar, Consortium partner to UNM	No	No

UNM Valencia*	IC CAE Scholar, Consortium partner to UNM	No	No
New Mexico Highlands University*	IC CAE Scholar, Consortium partner to UNM	No	No
San Juan College*	IC CAE Scholar, Consortium partner to UNM	No	No
Northern New Mexico College*	IC CAE Scholar, Consortium partner to UNM	No	No
Navajo Technical University*	IC CAE Scholar, Consortium partner to UNM	No	No
University of South Florida	M.S. in Cybersecurity Intelligence and Information Security, M.S. in Intelligence Studies (Cyber Intelligence; Strategic Intelligence), B.S. in Information Science, Concentration (Intelligence Analysis), Minor (Intelligence Studies)	Yes	Yes, No (B.S. in Information Science other concentrations)
University of Texas at San Antonio	M.S. in Data Analytics, Certificate in Intelligence Studies	Yes	Yes
University of Texas Rio Grande Valley	N/A	No	N/A
University of the Incarnate Word	N/A	No	N/A

Table 6 Grant Receiving IC CAE Institutions as of January 2022 (ODNI 2022a; data compiled by author).

Institution (* denotes a subunit / partner institution to above institution)	**Program type and name**	**Data eligible for research**	**Mandatory intelligence analysis courses**
Florida International University	Certificate (National Security Studies, Global Cybersecurity Policy)	Yes	Yes
Broward College*	Consortium partner	No	N/A

Florida Memorial University*	Consortium partner	No	N/A
Miami Dade College*	Consortium partner	No	N/A
Rutgers, The State University of New Jersey	Minor (Critical Intelligence Studies)	Yes	Yes
Borough of Manhattan Community College*	Consortium partner	No	N/A
New Jersey City University*	B.S. (National Security Studies) M.S. (National Security Studies), Minor (National Security Studies)	Yes	No
City College of New York*	M.S. in Cybersecurity	No	N/A
Syracuse University	IC CAE Scholar	Yes	No
CUNY-CCNY/Grove School of Engineering*	N/A	No	N/A
CUNY/John Jay College of Criminal Justice*	N/A	No	N/A
Norfolk State University*	IC CAE Scholar, National Security Certificate	No	N/A
Wells College*	N/A	No	N/A
University of Arizona	B.A.S. (Operational Intelligence; Information Warfare; Law Enforcement Intelligence)	Yes	Yes
Eastern Arizona College*	N/A	No	N/A
Estrella Mountain Community College*	N/A	No	N/A
University of Central Florida	B.A. (Political Science, Intelligence, and National Security), Minor (Intelligence and National Security), Certificate (Intelligence and National Security)	Yes	Yes
Seminole State College*	N/A	No	N/A
University of Kansas	Minor (Intelligence and National Security Studies, Certificate	Yes	Yes

	(Intelligence and National Security Studies)		
Dodge City Community College*	N/A	No	N/A
Donnelly College*	IC CAE Scholar, Certificate (Intelligence & National Security Studies)	No	N/A
Seward County Community College*	IC CAE Scholar, Certificate (Intelligence & National Security Studies)	No	N/A
University of North Carolina in Charlotte	Minor (Security and Intelligence Studies), Concentration (Security and Intelligence Studies)	Yes	Yes
Johnson C. Smith University*	N/A	No	N/A
South Carolina State University*	B.S. (Cyber Security Concentration)	No	N/A
Winston Salem State University*	N/A	No	N/A
University of Oklahoma – Norman	Certificate (Intelligence Studies)	No	N/A
Cameron University*	N/A	No	N/A
College of the Muscogee Nation*	N/A	No	N/A
Langston University*	N/A	No	N/A
University of Southern California	IC CAE Scholar	Yes	No
Florida Agricultural and Mechanical University*	IC CAE Scholar, M.A. Social Science Concentration in Global Security and International Affairs, M.A. Social Science in Criminal Justice, Minor in International Relations, Minor in Cybersecurity, Certificate in Cybersecurity	Yes	No
San Jose State University*	IC CAE Scholar	Yes	No

Santa Monica College*	IC CAE Scholar, B.A. (Interaction Design), A.A. (Political Science; Global Studies; Public Policy; Computer Programming; Computer Science), Certificate (Cybersecurity; Global Studies; Public Policy; Geospatial Programs)	Yes	No
Virginia Polytechnic Institute & State University	IC CAE Scholar	Yes	No
Danville Community College*	N/A	No	N/A
Morehouse College*	N/A	No	N/A

REFERENCES

PRIMARY SOURCES

Government publications

Government Accountability Office (2019): GAO-19-529 Intelligence Community: Actions Needed to Improve Planning and Oversight of the Centers for Academic Excellence Program, available https://www.gao.gov/products/gao-19-529, accessed August 26th, 2022.

Office of the Director of National Intelligence (2022a): IC CAE Grant Receiving & Legacy Institutions, available: https://www.dni.gov/files/CHCO/documents/CAE/2022ICCAE_Schools_Final_508_011022.pdf, accessed August 22nd, 2022.

Office of the Director of National Intelligence (2022b): IC CAE Frequently Asked Questions. Available: https://www.dni.gov/files/CHCO/documents/CAE/ICCAE_FAQs.pdf, accessed August 22nd, 2022.

Office of the Director of National Intelligence (2020): Intelligence Community Centers of Academic Excellence Strategy 2020 – 2023, available https://www.odni.gov/files/CHCO/documents/CAE/IC_CAE_Strategy.pdf, accessed August 16th, 2022.

Office of the Director of National Intelligence (2019): National Intelligence Strategy of the United States of America 2019. Available: https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf, accessed January 7th, 2022.

Office of the Director of National Intelligence (2017a): Intelligence Community Directive 204 National Intelligence Priorities Framework. Available: https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf, accessed October 14th, 2022.

Office of the Director of National Intelligence (2017b): Intelligence Community Directive 208 Maximizing the Utility of Analytic Products. Available: https://www.dni.gov/files/documents/ICD/ICD%20208%20-%20Maximizing%20the%20Utility%20of%20Analytic%20Products%20(09%20Jan%202017).pdf, accessed October 14th, 2022.

Office of the Director of National Intelligence (2015a): Intelligence Community Directive 203 Analytic Standards. Available: https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf, accessed October 14th, 2022.

Office of the Director of National Intelligence (2015b): Intelligence Community Directive 206 Sourcing Requirements for Disseminated Analytic Products. Available: https://www.dni.gov/files/documents/ICD/ICD%20206.pdf, accessed October 14th, 2022.

Office of the Director of National Intelligence (2014): The National Intelligence Strategy of the United States of America 2014. Available:

https://www.dni.gov/files/documents/2014_NIS_Publication.pdf, accessed October 14th, 2022.

Office of the Director of National Intelligence (2013): Intelligence Community Directive 205 Analytic Outreach. Available: https://www.dni.gov/files/documents/ICD/ICD%20205%20-%20Analytic%20Outreach.pdf, accessed October 14th, 2022.

Office of the Director of National Intelligence (2008): Intelligence Community Directive Number 207 National Intelligence Council. Available: https://www.dni.gov/files/documents/ICD/ICD_207.pdf, accessed October 14th, 2022.

U.S. Senate Select Committee on Intelligence (2011): REPORT of the SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE covering the period JANUARY 3, 2009 to JANUARY 4, 2011. Available: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-covering-period-january-3-2009-january-4-2011, accessed September 30th, 2022.

U.S. Senate Select Committee on Intelligence (2013): R E P O R T of the SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE covering the period JANUARY 5, 2011 to JANUARY 3, 2013. Available: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-covering-period-january-5-2011-january-3-2013, accessed September 30th, 2022.

U.S. Senate Select Committee on Intelligence (2015): REPORT of the SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE COVERING THE PERIOD JANUARY 3, 2013 to JANUARY 5, 2015. Available: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-covering-period-january-3-2013-january-5-2015, accessed September 30th, 2022.

U.S. Senate Select Committee on Intelligence (2017): REPORT of the SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE COVERING THE PERIOD JANUARY 6, 2015 to JANUARY 2, 2017. Available: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-covering-period-january-6-2015-january-2-2017, accessed September 30th, 2022.

U.S. Senate Select Committee on Intelligence (2019a): REPORT of the SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE COVERING THE PERIOD JANUARY 3, 2017 to JANUARY 3, 2019. Available: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-3, accessed September 30th, 2022.

U.S. Senate Select Committee on Intelligence (2019b) DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020. Available: https://www.intelligence.senate.gov/publications/damon-paul-nelson-and-matthew-young-pollard-intelligence-authorization-act-fiscal-years, accessed September 30th, 2022.

U.S. Senate Select Committee on Intelligence (2021): REPORT of the SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE COVERING THE PERIOD JANUARY 4, 2019 to JANUARY 3, 2021. Available:

https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4, accessed September 30th, 2022.

Intelligence Community Centers for Academic Excellence Program Institutions Resources

California State University, Fullerton (2022): Intelligence Community Scholars Program. Available: http://hss.fullerton.edu/paj/intelligence_comm.aspx, accessed October 18th, 2022.

California State University, San Bernardino (2022): Department of Political Science Intelligence Community Center of Academic Excellence. Available: https://www.csusb.edu/political-science/graduate-programs/intelligence-community-center-academic-excellence, accessed October 18th, 2022.

Chicago State University (2022a): Centers & Projects. Available: https://www.csu.edu/cimst/infostudies/centers.htm, accessed October 18th, 2022.

Chicago State University (2022b): Course Listing 2022–2023. Available: https://www.csu.edu/catalogs/documents/Course_Listing_2022-2023.pdf, accessed October 18th, 2022.

Eastern Kentucky University (2022): Bluegrass State Intelligence Community Center of Academic Excellence. Available: https://bgsiccae.eku.edu/, accessed October 18th, 2022.

Florida International University (2022a): Intelligence Analysis Track. Available: https://gordoninstitute.fiu.edu/workforce-development/intelligence-fellowship/intelligence-analysis-track/index.html, accessed October 18th, 2022.

Florida International University (2022b) Intelligence Fellowship. Available: https://gordoninstitute.fiu.edu/workforce-development/intelligence-fellowship/index.html, accessed October 18th, 2022.

Florida International University (2022c): Cyber Threat Intelligence Track. Available: https://gordoninstitute.fiu.edu/workforce-development/intelligence-fellowship/cyber-threat-intelligence-track/index.html, accessed October 18th, 2022.

Florida International University (2022d): Graduate Catalog 2022-2023. Available: https://catalog.fiu.edu/2022_2023/graduate/Steven_J_Green_School_of_International_and_Public_Affairs/GD_Steven_J_Green_School_of_International_and_Public_Affairs_Certificate_Programs.pdf, accessed October 18th, 2022.

Kentucky State University (2022): Master of Arts in Interdisciplinary Behavioral Sciences. Available: https://www.kysu.edu/academics/college-hbs/school-of-bss/master-of-arts-in-interdisciplinary-behavioral-sciences.php, accessed October 18th, 2022.

New Jersey City University (2022): Study Cybersecurity at NJCU. Available: https://www.njcu.edu/academics/schools-colleges/college-professional-studies/departments/professional-security-studies/study-cyber-security-njcu, accessed October 18th, 2022.

Rutgers, the State University of New Jersey (2022a): Minor in Critical Intelligence Studies. Available: https://static1.squarespace.com/static/54d79f88e4b0db3478a04405/t/5a255b0e8165f55746ed9293/1512397583024/CIS+Minor+at+Rutgers.pdfm, accessed October 18th, 2022.

Rutgers, the State University of New Jersey, Center for Critical Intelligence Studies (2022b): About Us. Available: http://intel.rutgers.edu/about-us/about-the-program, accessed October 18th, 2022.

Syracuse University (2022): Become an IC CAE Scholar! Available: https://experience.syracuse.edu/career/services/intelligence-community-center-academic-excellence/program-requirements/, accessed October 18th, 2022.

The University of Arizona (2022a): IC-CAE – Intelligence & Information Operations. Available: https://iio.azcast.arizona.edu/content/ic-cae, accessed October 18th, 2022.

The University of Arizona (2022b): IC-CAE – Curriculum. Available: https://iio.azcast.arizona.edu/content/curriculum, accessed October 18th, 2022.

The University of Mississippi (2022): Center for Intelligence and Security Studies CISS Courses. Available: https://ciss.olemiss.edu/the-program/courses/, accessed October 18th, 2022.

The University of New Mexico (2022a): Critical Technology Studies Program (CTSP). Available: https://ctsp.unm.edu/index.html, accessed October 18th, 2022.

The University of New Mexico (2022b): National Security & Strategic Analysis. Available: http://lais.unm.edu/about-us/lais-programs/nssa.html, accessed October 18th, 2022.

The University of Texas at San Antonio (2022a): Graduate Certificate in Intelligence Studies. Available: https://catalog.utsa.edu/graduate/business/#certificatestext, accessed October 18th, 2022.

The University of Texas at San Antonio (2022a): 2021-23 Graduate Catalog Carlos Alvarez College of Business. Available: https://catalog.utsa.edu/graduate/business/#degreestext, accessed October 18th, 2022.

University of Central Florida (2022a): Intelligence Community Center for Academic Excellence. Available: https://sciences.ucf.edu/politics/iccae/, accessed October 18th, 2022.

University of Kansas (2022a): Graduate Military Programs Intelligence Community Center for Academic Excellence. Available: https://iccae.ku.edu/, accessed October 18th, 2022.

University of Kansas (2022b): Graduate Military Programs Intelligence Community Center for Academic Excellence Courses. Available: https://iccae.ku.edu/courses, accessed October 18th, 2022.

University of North Carolina in Charlotte (2022a): About - Peace and Conflict Innovations Lab | - UNC Charlotte. Available: https://pacis.charlotte.edu/about/, accessed October 18th, 2022.

University of North Carolina in Charlotte (2022b): Courses - Peace and Conflict Innovations Lab | - UNC Charlotte. Available: https://pacis.charlotte.edu/curriculum/, accessed October 18th, 2022.

University of South Florida (2022a): School of Information Programs. Available: https://www.usf.edu/arts-sciences/departments/information/undergraduate/, accessed October 18th, 2022.

University of South Florida (2022b): Intelligence Studies, M.S. Available: https://catalog.usf.edu/preview_program.php?catoid=18&poid=7684&returnto=3153, accessed October 18th, 2022.

University of South Florida (2022c): Cybersecurity Intelligence and Information Security, M.S. Available: https://catalog.usf.edu/preview_program.php?catoid=18&poid=7884, accessed October 18th, 2022.

University of Southern California (2022): Intelligence Community Center for Academic Excellence. Available: https://sites.usc.edu/iccae/, accessed October 18th, 2022.

University of Southern California (2022): Intelligence Community Center for Academic Excellence FAMU Current Programs and Degrees at FAMU. Available: https://sites.usc.edu/iccae/programs/famu/, accessed October 18th, 2022.

University of Southern California (2022): Intelligence Community Center for Academic Excellence SJSU Current Programs and Degrees at SJSU. Available: https://sites.usc.edu/iccae/programs/sjsu/, accessed October 18th, 2022.

University of Southern California (2022): Intelligence Community Center for Academic Excellence SMC Current Programs and Degrees at SMC. Available: https://sites.usc.edu/iccae/programs/smc/, accessed October 18th, 2022.

Virginia Polytechnic Institute and State University (2022): Hume IC CAE Research Fellowship Program. Available: https://hume.vt.edu/education-outreach/scholarships/hume-iccae-fellowship.html, accessed October 18th, 2022.

SECONDARY SOURCES

Andrew, Christopher (2004) Intelligence, International Relations and 'Under-theorisation', *Intelligence and National Security*, 19:2, 170–184.

Andrew, Christopher (1996): *For the President's eyes only: Secret intelligence and the American presidency from Washington to Bush*. Harper Collins.

Andrew, Christopher, and Dilks, David, (eds.) (1984): *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*. Basingstoke: Macmillan.

Agrell, Wilhelm, and Gregory F. Treverton (2015): *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. New York: Oxford University Press.

Ahlbäck, Anders (2018): Unwelcome knowledge Resistance to pedagogical knowledge on a university setting, c.1965–2005, in Östling, Johan, Erling Sandmo, David Larsson

Heidenblad, Anna Nilsson Hammar, and Kari H Nordberg (eds.) (2018): *Circulation of Knowledge: Explorations in the History of Knowledge*. Lund: Nordic Academic Press.

Bandyopadhyay, Prasanta S., and Malcolm R. Forster (eds.) (2011): *Philosophy of Statistics*. 1st ed. Oxford, U.K: Elsevier.

Bandyopadhyay, Prasanta S, and Forster Malcolm R. "Philosophy of Statistics: An Introduction." In *Philosophy of Statistics*, 1–50. Oxford, U.K: Elsevier.

Bell, Wendell (2003): *Foundations of Futures Studies : History, Purposes, and Knowledge. Volume 1, Human Science for a New Era*. New Brunswick: Transaction Publishers.

Borg, Lars C. (2017) Improving Intelligence Analysis: Harnessing Intuition and Reducing Biases by Means of Structured Methodology, *The International Journal of Intelligence, Security, and Public Affairs*, 19:1, 2–22.

Bowman H. Miller (2018): "Open Source Intelligence (OSINT): An Oxymoron?", *International Journal of Intelligence and CounterIntelligence*, 31:4, 702–719.

Buzan, Barry & Hansen, Lene (2009): *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Campbell, Stephen H. (2011): A Survey of the U.S. Market for Intelligence Education, *International Journal of Intelligence and CounterIntelligence*, 24:2, 307–337.

Chang, Welton, Elissabeth Berdini, David R. Mandel & Philip E. Tetlock (2018): Restructuring structured analytic techniques in intelligence, *Intelligence and National Security*, 33:3, 337–356.

Clark, Robert M. (2019*): Intelligence Analysis: A Target-Centric Approach*. Thousand Oaks: CQ Press.

Clark, Robert M. (2013): *Intelligence collection*. CQ Press.

Coulthart, Stephen and Crosston, Matthew (2015): Terra Incognita: Mapping American Intelligence Education Curriculum, *Journal of Strategic Security* 8, no. 3 (2015) : 46–68.

Crosston, Matthew D. (2018): Fragile Friendships: Partnerships Between the Academy and Intelligence, *International Journal of Intelligence and CounterIntelligence*, 31:1, 139–158.

Custom Market Insights (2022): Global Open Source Intelligence (OSINT) Market Share Likely to Grow At a CAGR of 18% By 2030. Available: https://www.custommarketinsights.com/press-releases/global-open-source-intelligence-market/, accessed October 13th, 2022.

Davies, Philip H. J., and Kristian Gustafson (eds.) (2013): *Intelligence Elsewhere Spies and Espionage Outside the Anglosphere*. Washington, DC: Georgetown University Press.

Davies Philip H. J., and Kristian C. Gustafson (2013): "An Agenda for the Comparative Study of Intelligence: Yet Another Missing Dimension." *Intelligence Elsewhere*. Georgetown University Press.

della Porta, Donatella, and Michael Keating (2008): *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective.* Cambridge: Cambridge University Press.

della Porta, Donatella and Michael Keating (2008): "How Many Approaches in the Social Sciences? An Epistemological Introduction." In *Approaches and Methodologies in the Social Sciences*, 19–39. Cambridge University Press.

Deng, Zongyi (2009): The formation of a school subject and the nature of curriculum content: an analysis of liberal studies in Hong Kong, *Journal of Curriculum Studies*, 41:5, 585–604.

Department of Justice (2006): A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks Chapter Two Background, available: https://oig.justice.gov/sites/default/files/archive/special/s0606/chapter2.htm, accessed September 22nd, 2022.

Diderichsen Adam (2019): Spreading intelligence, Intelligence and National Security, 34:3, 409–420.

Dover, Robert, Michael S Goodman, and Claudia Hillebrand (eds.) (2014): *Routledge Companion to Intelligence Studies*. London: Routledge.

Durbin, Brent (2017): *The CIA and the Politics of US Intelligence Reform*. New York: Cambridge University Press.

Dylan, Huw, David Gioe, and Michael S Goodman (2020): *The CIA and the Pursuit of Security: History, Documents and Contexts.* Edinburgh: Edinburgh University Press.

Dylan, Huw & Maguire, Thomas J. (2022) Secret Intelligence and Public Diplomacy in the Ukraine War, *Survival*, 64:4, 33–74.

Edgar, Timothy H. (2017): *Beyond Snowden Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, D.C: Brookings Institution Press.

Eun, Yong-Soo (2017). To what extent is post-positivism "practised" in International Relations? Evidence from China and the USA, *International Political Science Review*, 38(5), 593–607.

Federal Bureau of Investigation (2022): Director's Remarks to Business Leaders in London. Available: https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622, accessed October 3rd, 2022.

Fingar, Thomas (2011): *Reducing Uncertainty: Intelligence Analysis and National Security*. Redwood City: Stanford University Press.

Fischhoff, Baruch & Chauvin, Cherie (2011): *Intelligence analysis for tomorrow advances from the behavioral and social sciences*. National Academies Press.

Freedman, David A. (2009): *Statistical Models and Causal Inference: A Dialogue with the Social Sciences*. New York: Cambridge University Press.

Friedman, Jeffrey A. & Richard Zeckhauser (2015): Handling and Mishandling Estimative Probability: Likelihood, Confidence, and the Search for Bin Laden, *Intelligence and National Security*, 30:1, 77–99.

Gearon, Liam Francis (2020): "The University-Security-Intelligence Nexus: Four Domains." In *The Routledge International Handbook of Universities, Security and Intelligence Studies*, 5–77. 1st ed. Routledge.

Gearon, Liam F., and Scott Parsons (2018): "Research Ethics in the Securitised University." *Journal of Academic Ethics* 17, no. 1 (2018): 73–93.

Gentry, John A. "Demographic Diversity in U.S. Intelligence Personnel: Is It Functionally Useful?" *International journal of intelligence and counterintelligence* ahead-of-print, no. ahead-of-print (2021): 1–33.

Gill, Peter, Stephen Marrin, and Mark Phythian (eds.) (2009): *Intelligence Theory: Key Questions and Debates*. Florence: Routledge.

Gill, Peter (2009): "Theories of Intelligence: Where Are We, Where Should We Go and How Might We Proceed?" In Gill, Peter, Stephen Marrin, and Mark Phythian (eds.) (2009): *Intelligence Theory: Key Questions and Debates,* 222–240. Florence: Routledge.

Gioe, David V. & Hatfield, Joseph M. (2021): A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective, *Cambridge Review of International Affairs*, 34:5, 704–738.

Goldman, Jan (2018): The Ethics of Research in Intelligence Studies: Scholarship in an Emerging Discipline, *International Journal of Intelligence and CounterIntelligence*, 31:2, 342–356.

Greenwald, Glenn & MacAskill, Ewen (2013): NSA Prism program taps in to user data of Apple, Google and others, available: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed August 27th, 2022.

Hager Ben Jaffel, Alvina Hoffmann, Oliver Kearns, Sebastian Larsson, Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon, *International Political Sociology*, Volume 14, Issue 3, September 2020, Pages 323–344.

Haggerty, Kevin, Kirstie Ball, and David Lyon (eds.) (2012): *Routledge Handbook of Surveillance Studies*. Taylor and Francis.

Hassan, Nihad A., and Rami. Hijazi (2018): *Open Source Intelligence Methods and Tools A Practical Guide to Online Intelligence*. 1st ed. Berkeley, CA: Apress.

Herman, Michael (2001): *Intelligence services in the information age*. Routledge.

Heuer, Richards J. & Pherson, Randolph H. (2015): *Structured analytic techniques for intelligence analysis. 2nd ed.* Thousand Oaks: CQ Press.

Historical Office of the Secretary of Defense (2017): National Security Strategy. Available: https://history.defense.gov/Historical-Sources/National-Security-Strategy/, accessed October 14th, 2022.

Hitz, Frederick P. (2006): Human source intelligence, in Johnson, Loch K. (ed.) *Handbook of Intelligence Studies*. London: Routledge.

Hitz, Frederick P. (2010): "Human Source Intelligence." In *The Oxford Handbook of National Security Intelligence*. Oxford University Press.

Hribar, Gašper, Iztok Podbregar, and Teodora Ivanuša (2014): "OSINT: A 'Grey Zone'?" *International journal of intelligence and counterintelligence* 27, no. 3 (2014): 529–549.

Jackson, Patrick Thaddeus (2011): *The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics*. Florence: Routledge.

Jasper, Ursula, Andreas Wenger, and Myriam Dunn Cavelty (2020): *The Politics and Science of Prevision : Governing and Probing the Future (Edition 1)*. Taylor & Francis.

Jeffreys-Jones, Rhodri (2002): *Cloak and Dollar: A History of American Secret Intelligence*. New Haven: Yale University Press.

Jensen, Carl J, David H McElreath, and Melissa Graves (2018): *Introduction to Intelligence Studies*. 2nd ed. Milton: Routledge.

Johnson Loch K. (2008): Glimpses into the Gems of American Intelligence: The President's Daily Brief and the National Intelligence Estimate, *Intelligence and National Security*, 23:3, 333–370.

Johnson, Loch K. (2010): *Oxford Handbook of National Security Intelligence*. New York: Oxford University Press, Incorporated.

Johnson, Loch K. (2020): "American Universities, the CIA, and the Teaching of National Security Intelligence." In *The Routledge International Handbook of Universities*, Security and Intelligence Studies, 79–93. 1st ed. Routledge.

Johnston, Rob (2005): *Analytic Culture in the US Intelligence Culture: An Ethnographic Study/Dr. Rob Johnston.* The Center for the Study of Intelligence Central Intelligence Agency: Washington, DC.

Kent, Sherman, 'The Need for an Intelligence Literature', *Studies in Intelligence* Spring (1955) pp.1–11.

Kent, Sherman (1965): *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press.

Landon-Murray, Michael (2011) Social Science and Intelligence Analysis: The Role of Intelligence Education, *Journal of Applied Security Research*, 6:4, 491–528.

Landon-Murray, Michael (2013) Moving U.S. Academic Intelligence Education Forward: A Literature Inventory and Agenda, *International Journal of Intelligence and CounterIntelligence*, 26:4, 744–776.

Landon-Murray, & Coulthart, Stephen (2016). Academic Intelligence Programs in the United States: Exploring the Training and Tradecraft Debate, *Global Security and Intelligence Studies*, 2(1).

Landon-Murray, Michael (2017) Putting a Little More "Time" into Strategic Intelligence Analysis, *International Journal of Intelligence and CounterIntelligence*, 30:4, 785–809.

Landon-Murray, Michael & Coulthart, Stephen (2020) Intelligence studies programs as US public policy: a survey of IC CAE grant recipients, *Intelligence and National Security*, 35:2, 269–282.

Leigh, Ian, and Wegge Njord (2019): *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. Taylor and Francis.

Leigh, Ian, and Njord Wegge (2019): "Intelligence and Oversight at the Outset of the Twenty-First Century." In *Intelligence Oversight in the Twenty-First Century*, 1:7–24. 1st ed. Routledge.

Lemieux, Frédéric (2019): *Intelligence and State Surveillance in Modern Societies : an International Perspective*. Bingley, UK: Emerald Publishing Limited.

Lester, Genevieve, and Jeffrey Rogg (2019): "Intelligence and Oversight: A View of the US System." In *Intelligence Oversight in the Twenty-First Century*, 1:135–151. Routledge.

Lowell, Hugo (2022): FBI sought national defense documents at Trump's Mar-a-Lago, affidavit shows. Available: https://www.theguardian.com/us-news/2022/aug/26/doj-redacted-trump-affidavit-mar-a-lago-search, accessed September 27th, 2022.

Lowenthal, M. (2015). *Intelligence: From secrets to policy. 6th ed*. Thousand Oaks, CA: Congressional Quarterly Press.

Lowenthal Mark M. (2017) My take on teaching intelligence: why, what, and how, *Intelligence and National Security*, 32:7, 986–994.

Marrin, Stephen (2011): *Improving Intelligence Analysis*. 2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN: Routledge.

Marrin, Stephen (2012) Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful, *Intelligence and National Security*, 27:3, 398–422.

Marrin, Stephen (2014): "The United States." 163–171 in Dover, Robert, Michael S Goodman, and Claudia Hillebrand (2014) (eds.). *Routledge Companion to Intelligence Studies.* London: Routledge.

Marrin, Stephen (2016): "Improving Intelligence Studies as an Academic Discipline", *Intelligence and National Security*, 31:2, 266–279.

Marrin, Stephen (2017a) Understanding and improving intelligence analysis by learning from other disciplines, *Intelligence and National Security*, 32:5, 539–547.

Marrin, Stephen (2017b) Why strategic intelligence analysis has limited influence on American foreign policy, *Intelligence and National Security*, 32:6, 725–742.

Marrin, Stephen (2018) Evaluating intelligence theories: current state of play, *Intelligence and National Security*, 33:4, 479–490.

Mazzetti, Mark (2022): The Poisoned Relationship Between Trump and the Keepers of U.S. Secrets. Available: https://www.nytimes.com/2022/08/11/us/politics/trump-fbi.html, accessed September 27th, 2022.

McDowell, Don. (2009): *Strategic Intelligence: a Handbook for Practitioners, Managers, and Users*. Rev. ed. Lanham (Md.): Scarecrow Press.

McEvoy, Jemima (2021): U.S. Intelligence Agencies Did Not Predict Taliban's Rapid Takeover Of Kabul, Report Says. Available: < https://www.forbes.com/sites/jemimamcevoy/2021/10/28/us-intelligence-agencies-did-not-predict-talibans-rapid-takeover-of-kabul-report-says/?sh=545bcd5f6543>, accessed September 29th, 2022.

Mclaughlin, John E. (2021) Four Phases of Former President Trump's Relations with the Intelligence Community, *International Journal of Intelligence and CounterIntelligence*, 34:4, 787–794.

Meese, Michael J., Suzanne C. Nielsen, and Rachel M. Sondheimer (2018): *American National Security*. JHU Press.

MI5 (2022): Joint address by MI5 and FBI Heads. Available: https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi, accessed October 3rd, 2022.

National Intelligence University (2022): Eligibility Criteria. Available: https://ni-u.edu/wp/eligibility-criteria/, accessed August 4th, 2022.

NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats (2022): *Attributing Information Influence Operations Identifying those Responsible For Malicious Behaviour Online*. Available: https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf, accessed October 12th, 2022.

Nolan, Bridget Jones (2022): From the "Lavender Scare" to "Out and Equal": LGBTQIA+ Diversity in the U.S. Intelligence Community, *International Journal of Intelligence and CounterIntelligence*, 35:4, 713–725.

OED Online, Oxford University Press (2022): "analysis, n.". Available: www.oed.com/view/Entry/7046, accessed October 5th, 2022.

Office of the Director of National Intelligence (2022b): U.S. Intelligence Community Budget, available: https://www.dni.gov/index.php/what-we-do/ic-budget, accessed August 16th, 2022.

Office of the Director of National Intelligence (2022c): Diversity & Inclusion. Available: https://www.dni.gov/index.php/how-we-work/diversity, accessed October 11th, 2022.

Office of the Director of National Intelligence (2021): Members of the IC, available https://www.dni.gov/index.php/what-we-do/members-of-the-ic, accessed January 7th, 2022.

Omand, David (2021): *How Spies Think: Ten Lessons in Intelligence*. Penguin UK.

Parsons, Scott (2020): “Intelligence Studies Degrees in intelligence and the intelligence community” In *The Routledge International Handbook of Universities, Security and Intelligence Studies*, 272–286. 1st ed. Routledge.

Pashakhanlou, Arash Heydarian (2017): “Fully Integrated Content Analysis in International Relations.” *International relations* (London) 31, no. 4 (2017): 447–465.

Perrigo, Billy (2022): How Open Source Intelligence Became the World's Window Into the Ukraine Invasion. Available: https://time.com/6150884/ukraine-russia-attack-open-source-intelligence/, accessed September 27th, 2022.

Phythian, Mark (2017): Intelligence analysis and social science methods: exploring the potential for and possible limits of mutual learning, *Intelligence and National Security*, 32:5, 600–612.

Phythian, Mark (2018): “Intelligence and the liberal conscience”, *Intelligence and National Security*, 33:4, 502–516.

Poli, Roberto (ed.) (2019): *Handbook of Anticipation: Theoretical and Applied Aspects of the Use of Future in Decision Making*. Springer International Publishing AG.

Poli, Roberto (2019): Introducing Anticipation. In *Handbook of Anticipation* (pp. 3–16). Springer International Publishing.

Prunckun, Hank (2015): *Handbook of Scientific Methods of Inquiry for Intelligence Analysis. Vol. 11.* Blue Ridge Summit: Scarecrow Press.

Ramsay, James, and Andrew Macpherson (2022): “The Integration of Statistical Learning in Intelligence Education: Is the Academy Equipping Tomorrow’s Intelligence Professionals to Analyze Data-Centric Threats?” *Journal of policing, intelligence and counter terrorism* ahead-of-print, no. ahead-of-print (2022): 1–19.

Ransom, Harry Howe (1984). "Secret Intelligence in the United States, 1947–1982: the CIA’s Search for Legitimacy." *The Missing Dimension*. Palgrave, London, 1984. 199–226.

Reinhold, Derek, Russo, Charles M. and Eisenfeld, Beth (2021): "Analytical Standards in the Intelligence Community: Are Standards Professionalized Enough?." *Journal of Strategic Security* 14, no. 1 (2021): 106–121.

Rich, Richard C., Craig Leonard Brians, Jarol B. Manheim, and Lars Willnat (2018): *Empirical Political Analysis : Quantitative and Qualitative Research Methods. Ninth edition*. New York: Routledge.

Richelson, Jeffrey (2016): *The U.S. Intelligence Community*. 7th ed. Boulder, Colorado: Westview Press.

Riehle, Kevin (2021): "Major or Minor?: For What Audiences are Intelligence Studies Programs Best Suited." *Journal of Strategic Security* 14, no. 1 (2021): 62–77.

Rietjens, Sebastiaan (2014): “Qualitative Data Analysis Seeing the Patterns in the fog of civil-military interaction”, in Soeters, Joseph, Patricia M Shields, and Sebastiaan Rietjens (eds.). *Routledge Handbook of Research Methods in Military Studies*. London: Routledge.

Salama, Vivian & Strobel, Warren P. (2021): Four U.S. Intelligence Agencies Produced Extensive Reports on Afghanistan, but All Failed to Predict Kabul’s Rapid Collapse. Available: https://www.wsj.com/articles/four-u-s-intelligence-agencies-produced-extensive-reports-on-afghanistan-but-all-failed-to-predict-kabuls-rapid-collapse-11635415201, accessed September 29th, 2022.

Schneider, Jonas (2020): “Predicting Nuclear Weapons Proliferation” in Jasper, Ursula, Andreas Wenger, and Myriam Dunn Cavelty. *The Politics and Science of Prevision : Governing and Probing the Future (Edition 1)*. Taylor & Francis.

Schreier, Margrit (2012): *Qualitative Content Analysis in Practice*. Los Angeles: SAGE.

Scott, Len (2014): Human intelligence, in Dover, Robert, Michael S Goodman, and Claudia Hillebrand (2014) (eds.). *Routledge Companion to Intelligence Studies*. London: Routledge.

Speigel, Ian (2021): Adopting and improving a new forecasting paradigm, *Intelligence and National Security*, 36:7, 961–977.

Stout, Mark & Michael Warner (2018): Intelligence is as intelligence does, *Intelligence and National Security*, 33:4, 517–526.

Strohm, Chris & Wilber Del Quentin (2014): Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers. Available: https://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says. accessed September 27th, 2022.

Svendsen, Adam D.M. (2012a): *Understanding the Globalization of Intelligence*. London: Palgrave Macmillan UK.

Svendsen, Adam D.M. (2012b): *The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem*. London: Palgrave Macmillan UK.

Svendsen Adam D.M. (2009): Connecting Intelligence and Theory: Intelligence Liaison and International Relations*, Intelligence and National Security*, 24:5, 700–729.

Tetlock, Philip, and Dan Gardner (2016): *Superforecasting: the art and science of prediction*. London: RH Books.

The International Association for Intelligence Education (2022a): IAFIE Mission & History. Available: https://www.iafie.org/page/MissionHistory, accessed August 25th, 2022.

The International Association for Intelligence Education (2022b): Intelligence Education Standards. Available: https://www.iafie.org/page/EducationStandards, accessed August 25th, 2022.

The National Security Archive (2004): President's Daily Brief, "Bin Ladin Determined To Strike in US" 6 August 2001 (2 pp.), declassified 10 April 2004. Available: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB116/pdb8-6-2001.pdf, accessed September 17th, 2022.

Tidd, John M. (2008): From Revolution to Reform: A Brief History of U.S. Intelligence. *The SAIS review of international affairs* 28.1: 5–24.

Toshkov, Dimiter (2016): *Research Design in Political Science*. London: Palgrave Macmillan.

Treverton, Gregory F. (2009): *Intelligence for an Age of Terror*. Cambridge: Cambridge University Press.

Treverton, Gregory F. & Renanah Miles (2017): Unheeded warning of war: why policymakers ignored the 1990 Yugoslavia estimate, *Intelligence and National Security*, 32:4, 506–522.

U.S. House of Representatives Permanent Select Committee on Intelligence (2022): Subcommittees. Available: https://intelligence.house.gov/subcommittees/, accessed October 13th, 2022.

van Puyvelde, Damien (2019): *Outsourcing US Intelligence: Contractors and Government Accountability*. Edinburgh University Press.

van Puyvelde, Damien & Sean Curtis (2016): 'Standing on the shoulders of giants': diversity and scholarship in Intelligence Studies, *Intelligence and National Security*, 31:7, 1040–1054.

Walsh, Patrick F. (2020): *Intelligence Leadership and Governance: Building Effective Intelligence Communities in the 21st Century*. Milton: Taylor and Francis.

Walsh, Patrick F. (2017a) Improving strategic intelligence analytical practice through qualitative social research, *Intelligence and National Security*, 32:5, 548–562.

Walsh, Patrick F. (2017b) Teaching intelligence in the twenty-first century: towards an evidence-based approach for curriculum design, *Intelligence and National Security*, 32:7, 1005–1021.

Walsh, Patrick F. (2011): *Intelligence and Intelligence Analysis*. Cullompton: Willan.

Waltz, Edward (2014): *Quantitative Intelligence Analysis : Applied Analytic Models, Simulations and Games*. Lanham, Maryland: Rowman & Littlefield.

Warner, Michael (2006): Sources and methods for the study of intelligence in Johnson, Loch K. (ed.) *Handbook of Intelligence Studies*. London: Routledge.

Warner, Michael (2014): *The Rise and Fall of Intelligence: An International Security History*. Georgetown University Press.

Wenger, Andreas, Jasper, Ursula & Dunn Cavelty, Myriam (2020): Governing and probing the future the politics and science of prevision, in Jasper, Ursula, Andreas Wenger, and Myriam Dunn Cavelty. *The Politics and Science of Prevision : Governing and Probing the Future* (Edition 1). Taylor & Francis.

Whitesmith Martha (2020a): Experimental Research in Reducing the Risk of Cognitive Bias in Intelligence Analysis, *International Journal of Intelligence and CounterIntelligence*, 33:2, 380–405.

Whitesmith, Martha (2020b): *Cognitive Bias in Intelligence Analysis: Testing the Analysis of Competing Hypotheses Method*. Edinburgh: Edinburgh University Press.

Whitesmith Martha (2019): The efficacy of ACH in mitigating serial position effects and confirmation bias in an intelligence analysis scenario, *Intelligence and National Security*, 34:2, 225–242.

Zhang, Zheng & Heydon, Rachel (2016): The changing landscape of literacy curriculum in a Sino-Canada transnational education programme: an actor-network theory informed case study, *Journal of Curriculum Studies,* 48:4, 547–564.

Östling, Johan, Erling Sandmo, David Larsson Heidenblad, Anna Nilsson Hammar, and Kari H Nordberg (eds.) (2018): *Circulation of Knowledge: Explorations in the History of Knowledge*. Lund: Nordic Academic Press.