Monarch Business School Switzerland

Doctor of Philosophy in Business Ethics
Dissertation Summary

Intelligence Collection and Ethical Behavior in the Post 9/11 Era

Dr. Lori Cole
June 2022

Abstract

The present summary abridges the research findings of the doctoral research submitted to Monarch Business School Switzerland entitled *Intelligence Collection and Ethical Behavior in the Post 9/11 Era.*

With the rapid technological advances of modern warfare, intelligence operatives face time-sensitive decisions that often carry ethical consequences. Scholarly research on ethics and intelligence gathering has generally lagged behind the update in technical surveillance capabilities and privacy concerns that arose in the post-9/11 era. Researchers have investigated intelligence practices, community responses to surveillance, and projected changes to the intelligence community. However, no study has analyzed the systemic lapses in military leadership that form the foundation of ethical dilemmas within the intelligence community from the perspective of intelligence operatives.

The primary purpose of this research is to determine the characteristics of a new ethical communication framework that better describes the relationship between intelligence collection and ethical behavior in a technologically advanced environment. The study offers qualitative research through institutional ethnographic and participant auto-ethnographic approaches to understand the lived experiences of intelligence operatives facing task-related ethical dilemmas. The research instruments included an open-ended research questionnaire and in-depth follow-up interviews to capture the personal beliefs and understanding of current and former intelligence operatives. Statistical and thematic participant interview analysis uncovered the foundational characteristics of a new conceptual model that could better describe the relationship between intelligence collection and ethical behavior in alignment with the operative, mission, and leadership.

The research provides a communication framework for the intelligence community and stakeholder groups that aids in disambiguating tasks and orders for those serving in the intelligence community. The Transactional Ethics Communication Framework (TECF) offers an original contribution to the present state of scholarship by scaffolding ethical dilemmas within a dialogic feedback loop between operatives and leadership.

Keywords: *Cyber Warfare, Intelligence, Whistleblowing, Ethics*.

1. Introduction

After the events of September 11, 2001, the U.S. intelligence community radically altered its position on intelligence gathering and usage from preventative to defensive collection. Most Western countries widened their collection scope and reduced restrictions in support of more robust, actionable intelligence (Herman, 2004). The National Security Agency (NSA) assumed control over massive data-collection programs, such as email, social media, and the bulk collection of telecommunications content and metadata, gaining the capacity to discover nearly anything about a target without directly collecting on them (Andregg, 2014).

Ethical hazards arose in intelligence analysis due to the powerful surveillance technology and advanced data mining of electronically stored information that agencies could now employ (Phythian & Omand, 2012). For instance, novel information tasking and collection processes using powerful technology allowed for unintended targeting of protected persons and placed intelligence operatives within ethically contentious situations, as they prioritized national defense missions and objectives over their own respect for privacy. Recent releases of volumes of classified information sparked ongoing criticism and examination of intelligence practices while raising new ethical quandaries by inflicting damage on U.S. national security (Anderson, 2015). Thus, the arrival of innovative technologies coupled with ethically dubious decisions produced the need for new leadership frameworks that could better serve the common good (Luthans & Avolio, 2003).

As a response, this qualitative study examines the ethical processes, methods, and regulations encompassing the intelligence community, as well as how whistleblowers negotiate these processes.

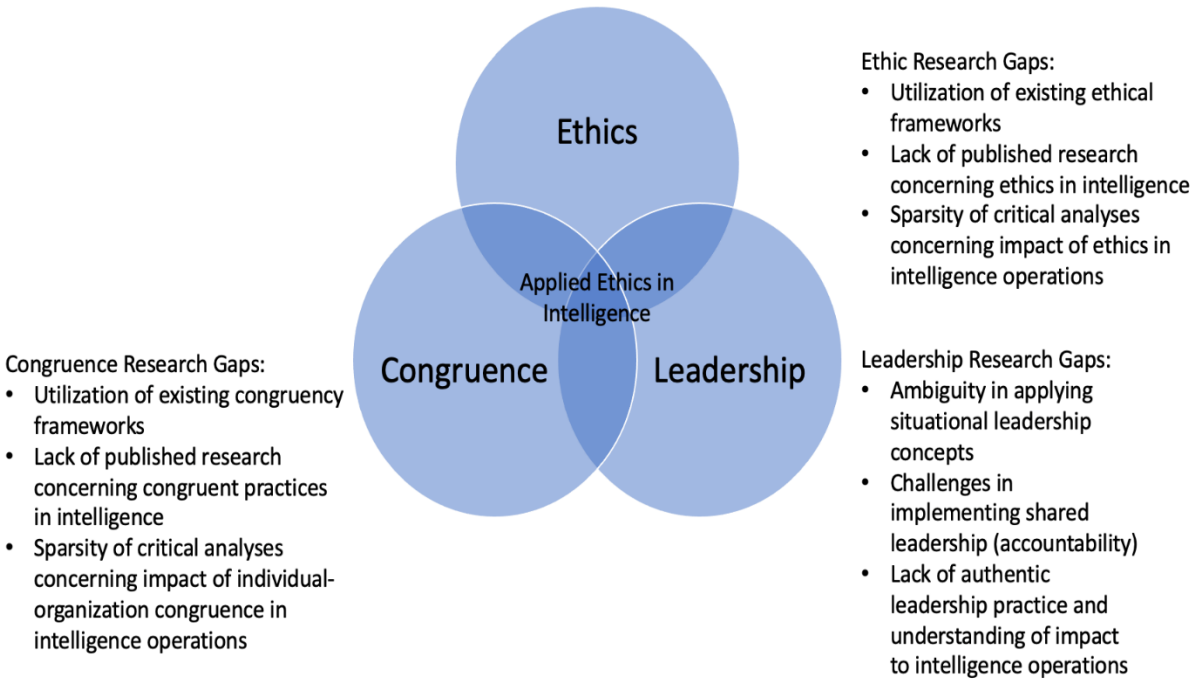
1.1 Research Problem

Scholarly research on ethics and intelligence gathering has generally lagged behind the update in technical capabilities that occurred in the post-9/11 era. Researchers have investigated intelligence practices, community responses to revelations of intrusive surveillance, and projected changes within the intelligence community (Andregg, 2016). Researchers have also recognized that technology is being leveraged to change the way people operate, thus prompting a need for a significant leadership change (Friman, 2007). Friman (2007) argued that future leadership and management principles must be rethought to manage future intelligence requirements. Military leadership must be disrupted so that more fluid situational leadership can replace strict step-by-step orders

(Friman, 2007). Rutkauskas and Stasytyte (2013) called for research involving leadership intelligence, the impact of leadership on subordinate ethical behavior, bi-directional communication efficiency, and resultant operational risk. However, scholars have not studied how intelligence operatives view the systemic lapses in leadership that form the foundation of ethical miscalculations within the intelligence community.

The gray literature on ethics in intelligence leadership validates the need for an overarching framework that could steer agents to consistently gather intelligence in accordance with ethical standards. Currently, the U.S. Army's doctrinal materials provide mixed messages on the matter of ethical issues in intelligence gathering (Barrett, 2012). The most prominent elements in the Army's coalesced publications regarding ethical governance validate the importance of Army ethics but offer disparate guidance at best (Giles, 2019). For instance, the recent 2005 edition of *The Army* (FM 1) provides three ethical tools: the Army Values, the Soldier's Creed, and the Army Warrior Ethos, but these ethical sources, however valuable, require nesting within an overarching institutional ethic, which does not seem to exist (Barrett, 2012).

FIGURE 1
Precise Knowledge Gap



Source: Cole, 2022

Figure 1 outlines the lack of research on ethics, leadership, congruency, and intelligence gathering, thus illuminating the need for research that could form the foundation of an overarching ethical framework for the intelligence community.

To date, no researcher has studied the congruence between ethics in intelligence leadership using a qualitative design to analyze the lived experience of intelligence agents navigating uncertain ethical processes while facing rapid technological advances. Rich data informed by interviews with intelligence agents was needed to ground operational rulesets in experience while preserving ethics during intelligence gathering and analysis.

1.2 The Main Research Question

The following main research question emerged from the literature on ethics, leadership, and intelligence collection:

> *"What are the characteristics of a new ethical communication framework that better describes the relationship between intelligence collection and ethical behavior in a technologically advanced post-9/11 era?"*

As reflected in the academic literature, new research concerning applied ethics could prove critical in addressing philosophical problems facing the Five Eyes (FVEY) intelligence community and related U.S. domestic communities, such as the Department of State, Federal Bureau of Investigation, and the U.S. Department of Homeland Security.

1.3 Purpose

Using a qualitative approach, the primary purpose of this research is to determine the characteristics of a new ethical communication framework that better describes the relationship between intelligence collection and ethical behavior in a technologically advanced environment. The purpose is broken down into five objectives:

- to understand how individual behaviors (ethical decisions) are influenced by intelligence operations;
- to understand how ethical boundaries are defined by intelligence community operations;

- to examine the divergence between intelligence agent conduct and intelligence community conduct guidance;
- to examine individual ethical deviation impact on the greater intelligence community; and
- to generate an operational model that more distinctly maps intelligence operations within ethical perimeters and can be leveraged within the intelligence community to inform operatives during times of ethical conflict.

This research filled the underlying research gap by providing a source for analysis—intimate accounts derived from interviews—of an evolving, crucial problem that impacts the vital interests of intelligence service members and civilians. The research also offers a new ethical communications framework that can help employees embody the ethics of intelligence operations while utilizing advanced technologies.

The research examines ethical behavior, intelligence agency accepted practices, and the individuals who deliberately commit actions the U.S. government deems unethical while operating under U.S. law. Further exploration of this phenomena may contribute to (a) improved oversight, (b) acceptable and explicit operational standards, and (c) an ethical framework that delineates between prohibited and permissible intelligence actions.

1.4 Definition of Terms

Table 1 provides definitions of frequently used terminology.

Table 1
Definition of Terms

Term	Definition
Congruence of values	Congruence of values involves three primary areas of work values: (a) employees' personal values, (b) the organization's values, and (c) the congruence between the two (Meglino et al., 1989).
Ethics	Ethics are based on well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues (Velasquez et al., 2010).

Intelligence operations	Intelligence comprises a cycle whereby information is acquired, analyzed, converted into its finished product, and made available to decision makers. Intelligence operations is an umbrella term that covers a range of different practices that intelligence actors use in the medium of cyberspace (Bellaby, 2016).
Leadership	Leadership is (a) a behavior, (b) a style, (c) a skill, (d) a process, (e) a responsibility, (f) an experience, (g) a function of management, (h) a position of authority, (i) an influencing relationship, (j), a characteristic, and (k) an ability (Northouse, 2013).
NSA	The National Security Agency (NSA) is the U.S. government lead agency for cryptology. The NSA's mission encompasses both signals intelligence (SIGINT) and information assurance activities (U.S. Department of Defense, 2010).
FVEY	An intelligence alliance comprised of the United States, Australia, Canada, New Zealand, and the United Kingdom.
Whistleblowing	Whistleblowing is the act of disclosing information from a public or private organization to reveal cases of corruption that present an immediate or potential danger to the public (Kumar & Santoro, 2017).
Power	One's potential or capacity to influence others through various means (French & Raven, 1959).
Source: Cole, 2022.	

2. Literature Review

The theoretical literature review incorporated scholarly and quasi-academic technical artifacts, including government publications, directives, and executive orders. The theory-driven literature review is separated into the categories of (a) ethics, (b) leadership, and (c) congruency theory in order to identify research gaps in the literature on ethics in the intelligence community. The literature review informed the main theoretical approach and the scope of potential applied methodologies.

2.1 Ethics

The research covers the classical foundations of Western ethics spanning from the contributions of Aristotle, Christian philosophers St. Augustine and St. Thomas Aquinas, and key Spanish scholastics to the Age of Enlightenment (Braun et al., 2022). The research covers classical and Christian conceptions of moral virtue (Dimmock & Fisher, 2017; Ward & Aristotle, 2001) and responsible decision making (Tornau, 2020) in the context of community citizenship (Elders, 2019). The review then focuses on moral development and behavioral ethics within the contemporary context of privacy, autonomy, and the defense of individual actions. The review uncovered a lack of

published studies on applied ethics in clandestine fields in a post-9/11 technological paradigm.

Within the context of the intelligence community, some of the central ethical principles presented in the research coalesce around the enduring contest between the pursuit of justice and the need for national security. Some of the sub-themes that emerged from that debate are as follows:

- Just Intelligence: War is considered morally permissible if authorized by proper authority for the common good (Bellaby, 2012). Since intelligence gathering is a vital part of national security, despite potential harm, the just war doctrine forms the basis for six just intelligence principles, which are cause, authority, intention, proportion, last resort, and discrimination (Bellaby, 2012). Under the just intelligence framework, leaders seek to mitigate threats before they present danger to the community. However, Herman (2004) challenged the concept of espionage as a "necessary evil" in the changing global climate of intelligence gathering directly before and after September 11, 2001 (p. 342). Herman invited researchers to view intelligence practitioners as members of a valued profession who remain subject to improved rules and oversight.
- Slippery Slope of Double Standards: One of the central ethical quandaries of intelligence gathering is the double standard Godfrey (1978) articulated as: ''What is unacceptable human behavior at home or in one's society can be forgiven in dealing with foreign societies or with representatives abroad of those societies" (p. 628). This type of double standard could lead to indifference or acceptance of immoral actions if left unchecked by an ethical governing body. The slippery slope of the permissiveness and double standards continues to grow as intelligence moves to the private sector, which can make its own rules within loosely constructed and loosely enforced ethical frameworks (Ronn, 2016). Public debate and inclusion when deciding the rules of agency operations could be part of a process that aligns national security with global human rights (Phythian, 2013).

- Right to Privacy: The research covers the ethical boundaries of intelligence gathering within the context of privacy (Pfaff & Tiel, 2004). Privacy may seem contrary to the interests of intelligence gathering for state security; however, Mackie (1977) defined privacy in two critical ways: (a) privacy as a set of boundaries and (b) privacy as a means of control. Individuals and societies set boundaries to retain privacy, protect psychologically sensitive information, and control public messaging. However, some room for surveillance must be allowed within the accepted norm.

- Passive Versus Active Collection in the Age of Technology: Technology caused a shift in the role of the intelligent agent from a passive gatherer to an active hunter of information (Cogan, 2004). While information gathering is intended to produce no direct harm (Harman, 2004, p. 46), passive collection of pertinent information is no longer feasible in this age of big data (Cogan, 2004). Powerful surveillance technology and the use of advanced data mining of electronically stored information produce new capabilities and raise the need for new ethical boundaries (Phythian & Omand, 2012).

- Participatory Consent: One boundary that could protect privacy is consent. While the current system relies on a holistic, voluntarily waived right to privacy, Pfaff and Tiel (2004) offered the idea of general consent as a given when individuals choose to enter society. Phythian (2013) raised the possibility of public debate and involvement in defining boundaries and achieving balance between intelligence activities, human rights, and privacy to reconcile ethics with intelligence gathering practices.

- Rule of Double Effect: To define the ethical boundaries of intelligence collection, theorists have recommended applying the rule of double effect. The rule of double effect states that collateral damage must be proportional to the information potential of the target. The rule is most known within a military context to determine whether an action might result in noncombatant casualties (Christopher, 1994). The rule of double effect also applies when intelligence is gathered from nonconsenting targets and results in unintended consequences. Intelligence targeting operations are permissible against legitimate targets and can also be used on third parties to gain legitimate information, which could lead to harm against unintended targets (Christopher, 1994).

- Do No Harm: During the Bush administration, the Bybee Memos redefined torture as activities that cause serious physical injury such as “organ failure, impairment of bodily function, or even death” or mental harm that would prove to last “months or even years” (U.S. Department of Justice, Office of Legal Counsel, 2002, p. 44). This legal memorandum allowed intelligence operators to inflict minor trauma. Yet the prisoner abuses that arose under this legal construct—such as those that occurred at Guantanamo and Abu Ghraib—may have caused long-term or potentially life-threatening injuries. Physical and mental integrity can take precedence over one’s autonomy and privacy; however, the Bybee Memos produced a national debate about whether torture was necessary for national security.

- Whistleblowing: Whistleblowing creates a conflict between the agent's loyalty to an institution or U.S. citizens (Lindblöm, 2007). Adhering to moral and legal obligations to support an employer can clash with the ethical imperative to stop harmful practices (Beauchamp & Bowie, 1988). To resolve this conundrum, Rawls (1971) set institutional justice as the pinnacle for achieving societal and global justice. Under Rawls' definition, if institutions promoted justice, whistleblowing would not be necessary (Lindblöm, 2007). Lindblöm (2007) invited further research to expand ethical frameworks within the intelligence communities to provide a means to manage actions in the event of an ethical dilemma that creates the need for whistleblowing.

Scholars in the field of intelligence ethics have discussed intelligence-gathering practices within the context of institutional, societal, and global justice (Christopher, 1994; Lindblöm, 2007; Phythian, 2013; Rawls, 1971; Ronn, 2016). However, the literature lacks an analysis of the complex internal experience that occurs within intelligence agents who face ethical quandaries over privacy, torture, whistleblowing, and surveillance while lacking a consistent framework for addressing those practices.

2.2 Leadership

With its tradition of hierarchical leadership and inherent detachment from subordinates, the military faces risks related to stagnation (Friman, 2007). Leadership and management principles must be rethought to address 21st-century intelligence requirements (Friman, 2007). Thus, an updated leadership approach should be implemented within the defense industry to promote innovation (Friman, 2007). As such, the literature review covered theories of leadership to assess and establish applicable avenues to create an updated leadership framework. The primary leadership theories covered in this section are situational leadership, shared/collaborative leadership, and authentic leadership.

- Situational Leadership: Paul Hersey and Kenneth Blanchard's (1996) theory of situational leadership suggests that there is no single best style of leadership. Instead, leadership efficacy depends on the organizational situation and the leader's relationship with subordinates. The theory posits four leadership styles (direct, coach, support, and delegate) that correspond to four degrees of task-maturity, ranging from immaturity through intermediate stages, and ending with total task maturity. This theory has faced criticism for its overgeneralization of task maturity (Graeff, 1983; Ramakanth, 1988). However, fluid situational leadership could benefit the military since it allows leaders to encourage

innovation while maintaining high productivity, organizational order, and positive performance (Friman, 2007; Graeff, 1983).

- Shared and Collaborative Leadership: Returning to Rawls (1971), the key to creating a just institution may be the implementation of shared leadership paradigm (Pearce et al., 2014). Shared or collaborative leadership is an integrated style in which the leader incorporates social responsibility and shares power by making decisions collectively (Chan, 2005; Crosby & Bryson, 2005; Huxham, 2003; Luthans & Avolio, 2003; Luthans et al., 1987; Pearce & Conger, 2003; Pearce et al., 2014; Van Wart, 2013). Despite having shared mission objectives and dispositions, a collaborative leadership style has not been implemented in U.S. military or intelligence organizations (Govinfo, n.d.), which could hamper their ability to achieve the common good (Pearce et al., 2014; Van Wart, 2013; Wang et al., 2014).

- Authentic Leadership: Authentic leaders derive their ethics and their actions from self-awareness, internalized moral perspective, balanced processing, relational transparency, and self-regulation (Caza & Jackson, 2011; Chan, 2005). Through introspective reflection, authentic leaders recognize their fundamental beliefs, core values, goals, and identity (Berkovich, 2014; Keller & Foster, 2000; Van Wart, 2013). In the context of national security, Keller and Foster (2012) found that leaders with an internal locus of control (LOC)—as indicated by strong beliefs in their ability to control events and high self-confidence—are more likely to use force for domestic political purposes than leaders with an external LOC, who tend to believe that situational outcomes are determined by the environment and are risk averse. Keller and Foster invited further exploration into how to better leverage authentic leadership to predict and prevent unnecessary political or military actions.

2.3 Congruence

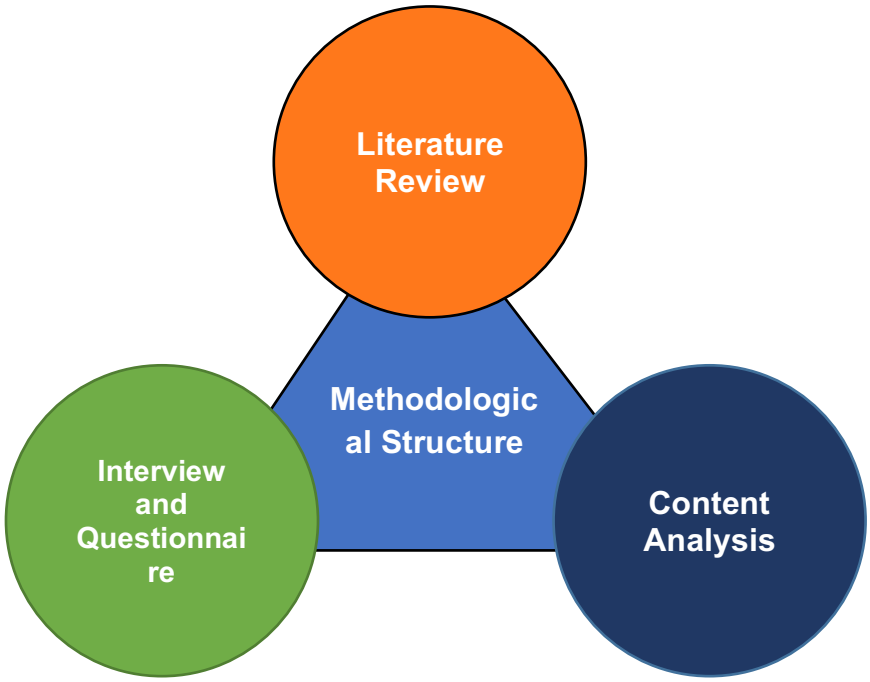
Lloyd Williams' (1993) congruence theory refers to an individual's capacity to align individual and organizational attitudes, thus leading to balance among core system elements. Williams (2002) focused on building functional congruence strategies by understanding the belief systems that impact and guide one's decision making, actions, performance, and ability to differentiate right from wrong (Williams, 2002). In an attempt to create congruence, leaders often base decisions on quantitative data, such as performance metrics (Esposito & Williams, 2010).

However, phenomenological (lived) experiences of employees within an organization are valid expressions of meaningful information that organizational leaders can use to create congruent change within an organization. This research considers phenomenological sources of information available to organizations (e.g., focused discussions and coworker dialogues) to provide a lens for understanding the potential alignment between leadership, ethics, and congruency within intelligence agencies.

3. Methodology

The research offers qualitative research through institutional ethnographic and participant auto-ethnographic approaches to understand the lived experiences of intelligence agents facing ethical dilemmas. The research follows the Monarch Standard Research Methodology and Triangulation Model by offering: 1. a theoretical literature review (see Section 3), 2. a questionnaire developed through field interviews, and semi-structured interviews (see Figure 2)., 3. along with content analysis of industry documents.

FIGURE 2
The Monarch Methodology Triangulation Model



Source: UGSM-Monarch Business School Switzerland

The findings from the study also informed the creation of a new artifact, an ethical framework designed to guide ethical decision making among leaders in the intelligence community.

3.1 Research Appropriateness

Institutional ethnography fills the research gap by offering a means to explore intelligence officers' internal perceptions of ethical decision making. Institutional ethnography serves as a collaborative practice between the researcher and the participant to weave diverse perspectives, biographies, and participant positions (Smith, 2005). According to Smith (2005), "the speaking or writing of experience is essential to realizing the project of working from the actualities of people's lives as the people themselves know them" (p. 125). As such, institutional ethnography contributes to a better understanding of the relationship between individual behaviors and the organizational ethics by uncovering the perspectives of employees' lived experiences.

3.2 Research Design

The research questionnaire, developed through field interviews, was composed of 10 open-ended questions. Participants completed interview questionnaires digitally at a location convenient to the subjects, and the questionnaires took approximately 30 minutes to complete. Interview questionnaire data were recorded digitally on the questionnaire and returned to the researcher via Google Forms.

A participant profile captured socioeconomic data points about the participant such as gender identity, military affiliation, title or ranking within the hierarchy of management or military, highest level of education, and years of intelligence experience. These factors may have influenced participant responses about their perceptions of their ethical behavior.

To deepen the study's findings, a smaller subset of five respondents from each stakeholder group (selected from the first-round sample) took part in subsequent, in-depth follow-up interviews. The interview questions concerned personal beliefs and understanding regarding the research on leadership, ethics, and congruence in relation to operational decision making. The subsequent interviews were designed to uncover deeply held personal beliefs and understanding regarding participants' lived experiences in relation to the initial survey responses. These follow-up interviews afforded participants the opportunity to further explain or clarify any information. These interviews occurred digitally via Google Meets.

3.3 Population and Sample

The present research specifically targeted field intelligence officers and direct management personnel as a research population based on their significant role in operational decision making and use of existing policies and procedures within operational frameworks. The final sample consisted of 39 direct-line managers and intelligence operatives serving in various organizational roles and capacities, including those forward deployed, domestically assigned, and working in undisclosed locations across North America and Europe.

3.4 Data Analysis

The analysis of ethnographic data enabled participants to identify their perceived issues, concerns, and problems with organizations in the intelligence community. Interview response texts allowed for ethnographic exploration of clandestine institutions. The researcher focused the ethnographic lens on the ethical behavior of operatives as they negotiated the operational intelligence environment to (a) understand participants' daily patterns of activity within the intelligence environment, and (b) identify the associative conditions that may have influenced individual operative behaviors.

The level of analysis matrix identifies the groups that were studied based on a three-part division of perspective levels (see Table 2). The green-shaded levels (meso and micro) were considered for this research.

TABLE 2
Level of Analysis and Stakeholders Schema

Level	Organizational Level	Unit Level
MACRO	Societal	Department of Defense, NSA, Central Intelligence Agency, Federal Bureau of Investigation
MESO	Institutional / Organizational	Intelligence Community Supervisors, Operational Team Leads
MICRO	Individual	Intelligence Agents

Source: Cole, 2022

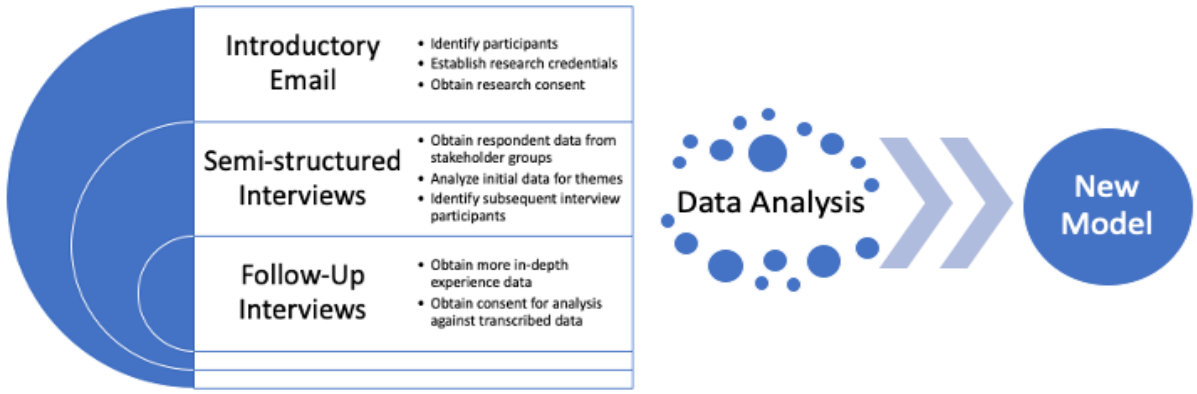
A constant comparative method of qualitative analysis served as a means to convert qualitative data into a quantifiable form so that a provisional test against the hypothesis could be performed. All relevant questionnaire data was systematically coded and analyzed to constitute proof of the given position using Amazon Comprehend and the

process of topic modeling. The machine learning model revealed patterns or associative connections among data points to derive topical themes. Further, the coding of the questionnaire responses unearthed topics for the subsequent interview questions to produce more in-depth experiential insight.

3.5 Artifact Creation

As a final step, the conceptual model formed the foundation for a new ethical framework for the intelligence community. For an outline of the research design, see Figure 3.

FIGURE 3
Research Design



Source: Cole, 2022

3.6 Validity and Reliability

To ensure that the research methodology and data analysis methods were valid, credible, and beneficial to consumer communities, the research followed Lincoln and Guba's (1985) method for attaining trustworthiness. The following techniques were implemented within the research design to maintain credibility, transferability, dependability, and confirmability (Lincoln & Guba, 1985):

- A portion of the gathered data were enclaved during initial analysis and analyzed post-research via sampling to prove the research findings were credible and valid;

- Ethnographic data (ethnographic phenomenon) were gathered and transcribed at a sufficient level of detail so that external examiners could clearly understand the findings and easily discern their applicability in other contexts;

- An external researcher examined the research process and research findings to evaluate the accuracy of the methodology and ensure that any conclusions were data-driven and repeatable;

- Audit-trail reporting categories for qualitative research, as defined by Schwandt and Halpern (1988), were used to ensure that the research was well documented, transparent, and avoided researcher biases. To maintain an accurate audit trail, raw data were cataloged upon receipt and proper version control was implemented to ensure data integrity and demarcate data citation changes. Further methods for validating data accuracy included:

    1. Coding of data occurred to represent analytical notes and observances;

    2. Data synthesis enabled exploratory, associative, and thematic analysis to be performed;

    3. Process notes were kept concerning research methods, evidentiary items, and correspondent data that may be subject to audit;

    4. Researcher notes concerning hypotheses, supplemental research ideas, subjective perspectives, biases, and parallel inquiries were catalogued for reference;

    5. Developmental, beta, or other versioning of data concerning research instrumentation, digital media, data schemas, and chronicles were preserved.

3.7 Limitations

The primary limitations were participant sample size, access and availability of participants, and a lack of previous research conducted on the study topic.

Ethnographic research requires more time than was available to develop a deep level of trust with the participants and solicit an adequate level of research participation. To prevent bias from coloring the interpretation of findings, the researcher remained intentionally objective. Despite these limitations, the strengths, precision, and efficacy of institutional ethnography outweigh the limitations, particularly for phenomena within a compartmentalized population.

3.8 Delimitations

The following primary delimitations impacted the scope of the present research: (a) not all literature could be considered or critiqued; (b) the level of structure provided in participant interviews impacted data collection; (c) not all populations could be represented in the participant groups; and (d) the research methods and investigatory parameters determined the scope of knowledge gathered.

3.9 Assumptions

Five main assumptions shaped the claims in this dissertation about the ethics of intelligence gathering.

1. FVEY intelligence agency directives are lawful. According to the Office of the Director of National Intelligence, the Intelligence Authorization Act is enabled by Public Law 111-259, which authorizes intelligence and intelligence-related activities (The National Counterintelligence and Security Center, n.d.);

2. Legal standards and strict regulations are in place to ensure regulation of the FVEY intelligence community. For example, the U.S. government instituted the Foreign Intelligence Surveillance Act federal statute, Executive Order No. 12333, and the Constitutional Fourth Amendment to reflect balance between U.S. intelligence operations and the privacy and protection of U.S. citizens (U.S. Department of Defense, 2010);

3. FVEY intelligence agents are expected to perform operational duties as assigned. Intelligence operatives are constantly engaged and actively participate as required by their role (Bellaby, 2016);

4. Ethical conflict causes deviation from intelligence operational conduct. Deviance from intelligence operational normalcy involves personal risk

and potential legal prosecution under treason laws (Kumar & Santoro, 2017). Strong ethical convictions can drive individual deviances in intelligence conduct despite irrevocable repercussions;

5. Intelligence agent choices and behaviors reverberate beyond the individual to include domestic and foreign intelligence services, U.S. and international law and strategy, public opinion, media outlets, and the dynamics of electronic warfare (Thompson, 2018).

4. Results

The findings from the semi-structured interview questionnaire revealed significant themes that contextualized participant behaviors. The participants exhibited a thorough understanding of conceptualized ethics within intelligence operations. The participants defined ethics with a mostly neutral sentiment (.74 confidence) using synonymous word choices such as moral, principle, and right. Participant examples of ethical behaviors included obeying the law, telling the truth, doing the right thing, being a good person, refraining from harming others, and acting with integrity. The results were used to inform subsequent in-depth interview focus questions, improve understanding of the situational context affecting behaviors, and identify significant components of the phenomenon under consideration.

4.1 Participant Profile

The 39 participants were divided into two distinct groups: operational managers and intelligence operatives. The top-level findings from the profile data were as follows:

- Highest Level of Education Completed: Seventy-four percent of the participants held higher education degrees (e.g., bachelor's or master's degree).

- Gender (self-identified): Twenty-three percent of the participants identified as female, and 77% percent of participants identified as male; thus, the distribution of participants was unequal.

- Military Branch of Service (if applicable): A sizeable percentage of the participants (51%) served in the U.S. Army.

- Title/Rank (civilian or military): Sixty-four percent of the participants served in the noncommissioned officer or officer ranks (E-5–E-9, O-1, O-6).

- Current or Previous Intelligence Community Affiliation: The participants were unequally distributed across a technical practitioner spectrum, with a sizeable percentage (50%) of the participants serving in an analyst role (intelligence analyst or cryptologic language analyst) and nearly 12% serving in an operational leadership role.

- Number of Years Served (within the intelligence community): The average service length was 12.31 years with a median of 12.5 years. A sizeable percentage of the participants (44%) served over 8 years, and 15% of participants served 15 years or more.

- Dates Served (within the intelligence community): The service dates were unequally distributed across critically transformative times in the National Defense (e.g., events of 9/11), with 84% of the participants having served after September 11, 2001, and over 46% after 2010.

- Years Deployed (civilian or military): The average deployment length of the 39 participants was 1.56 years with a median of one year.

4.2 Conceptualizing Ethics in Intelligence Operations

The findings from the semi-structured interview responses fell into three categories relating to interview questions 1–10. The first three questions related to the participants' understanding of ethics and role-based ethical behavior. The subsequent three questions concerned circumstances surrounding informed ethical decision making. The remaining four questions pertained to the components of unethical behaviors and residual effects.

4.2.1. Ethics and Role-Based Ethical Behavior

For the first question of the interview (Part B-1), participants were asked to define ethics. When discussing their perceptions of ethical behavior, the bulk of the participants described such behavior as "doing the right thing." Further response data indicated that participants defined "doing the right thing" as making moral choices and living by a code of morality recognized by law.

Subsequent questions (Part B-2 and B-3) extrapolated participants' ideals of generalized ethical behaviors and asked participants to examine their roles in the intelligence community through an ethical lens. The participants identified ethics as moral conduct or behaviors grounded in moral principles. Respondent data revealed that participant ideals and examples of ethical behaviors included lawfulness, nonviolence, integrity, and honesty.

Overall, 48% of participants reflected that their behaviors as intelligence operatives were ethical. However, 40% of participants stated that this was only "sometimes" or "maybe" true. Seven percent (7%) of the response data indicated that the participants felt they exhibited unethical behavior, and 3% of participants exhibited uncertainty about the ethics of their behavior.

4.2.2 Informed Ethical Decisions

For questions B-4 through B-6 of the interview, participants were asked to describe existing communication channels, mechanisms, and resources available to aid during ethical decision making while serving in the intelligence community. Participants were also prompted to describe the adequacy of existing resources. Participants were then invited to assess whether they possessed enough information to make informed ethical decisions while serving as intelligence operatives.

Seventeen percent (17%) of respondents were unaware or unsure of existing communication channels designated for ethical discussions. Further, 16% of respondents revealed that they felt partially prepared to make ethical decisions in their roles as intelligence operatives.

4.2.3 The Effects of Unethical Behaviour

In questions B-7 through B-10 of the interview, participants were asked to provide examples of unethical behaviors in the context of the intelligence community. The participants were also prompted to consider why intelligence operatives would commit unethical behavior in their course of duty. Participants were then invited to critically examine whether intelligence community policies relate to ethical decisions and behavior. Lastly, participants were asked to speculate about how individual divergences from intelligence community directives impact the intelligence community as a whole.

The behaviors the participants discussed included the mishandling or divulgence of classified data (9%) and acts of espionage against the United States (6%). Participants hypothesized that unethical behavior in the intelligence community derived from moral disagreement with intelligence mission objectives (6%), financial motivation (5%), and influential fear or threats of harm (3%).

4.3 In-Depth Thematic Interviews

A subgroup of 10 participants agreed to engage in an in-depth interview. The interview drew from the initial questionnaire data and consisted of 10 focus questions surrounding thematic influential criteria.

The codes of Part B-1 and B-2 were categorized into two groups representing ethics and ethical behaviors to illustrate how individual behaviors (ethical decisions) were influenced by intelligence operations. Ten significant statements emerged from the interviews: five statements derived from the group comprised of intelligence operatives and the other five statements originated from the group comprised of operational managers.

- Group of Intelligence Operatives (micro)
    - Regarding information compartmentalization and targeting: “I thought we should have held off a little bit more to wait to action (a target) because it (the intelligence) was really kind of hearsay; I didn’t see the factual data to back it up” (Interview 2).
    - Regarding compliance with or commitment of unethical actions: “We are not required compliance with or commitment of unethical actions when it comes to policy being practiced. I think it’s really subjective and based on the context of your work. The demands for information and the conflicts that can happen when, whoever your community partners are, need a thing. And so, I think sometimes it (ethics) can get muddled” (Interview 4).
    - Regarding subordination during ethical conflict: “For me, I had to know who to be subordinate to, that’s not a really clear answer, but I think maybe it kind of shows an example of how complicated it is. I think we’re expected to be subordinate to policy. That’s something that I always felt safe with someone I had to face. Conflict, ethical conflicts. I could always say, ‘Well, um, you know, the USSID or directive says that this is what I do

and that's the ultimate authority.' Different people are okay with saying 'no' to people that they directly report to, and some people aren't, so it probably varies" (Interview 2).

- Regarding availability of sufficient data to issue targeting: "I left government work because of this specific thing. Um, because I think we're just expected to understand that human rights are violated as part of the job. It's a necessary evil. I specifically have worked with people in my last unit that were involved in gross violations of human rights in Afghanistan and made jokes about it probably to compartmentalize their own complicity" (Interview 4).

- Regarding availability of sufficient data to issue targeting: "I don't trust it. The short answer is no. I don't trust that. That's why I left. I think it's complicated because it means that the people have to pay the price. I think the people that are impacted the most are people who are, um, collateral. Like the term collateral damage is citizens who don't have anything to do with the situation. And it's our lower enlisted, um, workers, military members who don't have any power and are not given the right tools to make the best decisions have trauma, impacts based on the decisions that they made there, that they had to make or are ordered to make, um, and they also get the penalty. The disciplinary penalties more heavily" (Interview 4).

- Group of Operational Managers (meso)

  - Regarding subordination during ethical conflict: "Depending on the mission and the scope of the unit that you're associated with" (Interview 5).

  - Regarding transforming to fit a skewed ethical model: "From a legal standard, that was skewed post 9/11 with the introduction of the Patriot Act and the other legislative efforts that have kind of modified what that means. And there's always that tradeoff between privacy and security that intelligence operators are expected to maintain that line. And it's not always clear exactly what that line is, what that tradeoff is between security and individual rights. So, I do feel that it's skewed, but it's not well defined what that model should or does look like" (Interview 5).

  - Regarding being informed about legal and ethical parameters of intelligence operations: "Legal mostly and somewhat ethical, uh,

parameters. But mostly that was in line to preserve the confidentiality and integrity of the program, not necessarily the ethical parameters. So, some institutions do have ethics hotlines, so to speak, people can report disagreements to. However, those aren't always, um, ever used or commonly practiced. In fact, in some places, the illusion or disagreement, um, that you would participate in such activities would be frowned upon. And that would, um, lead to, I guess, restriction from program access potentially" (Interview 10).

- Regarding importance placed upon a code of conduct or code of ethics: "A lot of the ideas of code of conduct, are presented for different types of missions and intelligence operations can be ambiguous. There can be a lack of clarity of how that applies within specifically the intelligence community. So, there was generally an importance placed on the code of conduct. However, it wasn't always clear how that code of conduct would apply within intelligence operations, specifically, as opposed to more traditional, military, or forward operating assignments" (Interview 6).

- Regarding transforming to fit a skewed ethical model: "It's allowed me to think about stuff that I never really thought of before with regards to ethics. I think intelligence agents are transformed to fit a skewed ethical model on that. Yes, but did it forced me to realign my ethics to support a mission. I would say no" (Interview 1).

In all, the participant interview responses coalesced around three topical clusters, reflecting significant associations between the ethics of the (a) mission, (b) operative, and (c) leadership.

4.4 Summary of Findings

The research offered nine main avenues of understanding the phenomenon: (a) the perception of the current state of ethics in the U.S. intelligence community; (b) the ethical boundaries that define NSA intelligence operations; (c) an understanding of how individual operative behaviors (ethical decisioning) are influenced by intelligence operations; (d) the points of divergence between intelligence operative behavior and intelligence community policies and directives; (e) the perceived impact to the larger intelligence community that results from intelligence operatives' ethical deviations; (f) the significance and multidimensional advantages of communication in intelligence operations; (g) the evaluation of the need for an effective, accessible ethical communication mechanism; (h) the formulation and generation of the Transactional

Ethics Communication Framework (TECF) that facilitates dialogue for ethical decision making incorporating ethics, leadership, and organizational congruence; and (i) the premise that the TECF provides an accessible and effective means for intelligence operatives to communicate and disambiguate operational ethical concerns.

The demographic profile analysis of direct-line managers and intelligence operatives produced several significant findings. A prominent omittance of intelligence agency affiliation (71%) perhaps reflects the clandestine nature of intelligence work. Participant time served suggests that being an intelligence operative is not a sustainable role; the majority of direct-line managers and intelligence operatives (85%) transitioned from the profession after serving 7–15 years. The participant deployment time findings indicate that the majority of direct-line managers and intelligence operatives (74%) served at least one year in a deployed capacity. Since deployment occupies a significant facet of intelligence collection, guidelines and directives surrounding ethical behavior while abroad could be clearly communicated to potentially retain staff.

Participants exhibited a dualistic experience concerning the role of ethical behaviors in intelligence operations. Forty-eight percent of participants indicated that their behaviors as intelligence operatives were ethical; however, 40% stated that this was only “sometimes” or “maybe” true. A small portion of respondents (7%) indicated that they exhibited unethical behavior while operating within the intelligence community. With regard to ethical decision making in intelligence operations, 17% of participants indicated a lack of knowledge surrounding the existence or adequacy of mechanisms to communicate ethical dilemmas. Further, 16% of respondents stated that they felt unprepared to make ethical decisions in their roles as intelligence operatives.

Participants provided examples of unethical behavior with a mostly negative sentiment (.88 confidence) using some of the following descriptors: divulgence of classified data, committing acts of espionage against the United States, serious crimes, and lying, which they attributed to moral disagreement with the intelligence mission objectives, financial motivation, influential fear or threats of harm, and alcohol.

For those engaging in the in-depth interview, the overall consensus was that the questions forced them to think critically about the existence or actuality of ethical frameworks within operational intelligence and their own behaviors within those.

Statistical and thematic participant interview analysis uncovered the foundational characteristics of a new conceptual model that could better describe the relationship

between intelligence collection and ethical behavior in alignment with the mission, operative, and leadership.

5. Discussion

The discussion of the research covers two primary domains: a comparison of the results to the literature and the construction of an ethical framework that practitioners can use to create consistent policies surrounding intelligence operative ethical behavior.

5.1 Comparison Between Results and Literature

The scholarly and gray literature indicated that U.S. Department of Defense military intelligence operations lack a consistent framework for regulating ethical behavior from the top down (Barrett, 2012; Giles, 2019). Confirming this notion, the research findings indicated that only 6% of participants perceived that existing communication channels, mechanisms, and resources were available to support ethical decision making while serving in the intelligence community. Further, only 5% of participants claimed that the existing mechanisms were adequate. This correspondence supports the notion that ethical behaviors within intelligence operations remain insufficiently governed.

The literature review covered the ethical dilemmas common to intelligence operations—including privacy violations (Mackie, 1977; Phythian, 2013), surveillance (Phythian & Omand, 2012), whistleblowing (Lindblöm, 2007; Rawls, 1971), and torture (Bybee Memos)—that complicate the ethical principles of universal human rights (Erskine, 2004; Phythian, 2013), just intelligence (Bellaby, 2012), and the rule of double effect (Christopher, 1994). In alignment with these findings, the participants verified the tradeoffs that occur between national security and individual rights during the divulgence of classified data, acts of espionage against the United States, serious crimes, and lying. The participants identified financial remuneration, fear of personal harm, and alcohol as the primary determinants of unethical behavior.

The literature review also covered the authentic, situational, and shared/collaborative leadership styles that shape ethical culture in the workforce. The scholarship on authentic leadership supported the notion that an operative's willingness to execute a given order derives from their personal ethics and self-awareness (Chan, 2005; Northouse, 2013). Those findings supported the participants' perceptions that personal values, identity, and self-regulation when making or following leadership directives contribute to ethical behavior at work. The review of situational leadership focused on dynamic leadership traits that adjust to employee experiences (Hersey & Blanchard,

1996; Northouse, 2013). The literature on situational leadership intersected with the participants' observations that ethical behaviors and decisions were subjective and depended on the context of the operation (e.g., unit assignment, geolocation, mission objective, etc.). The literature on shared/collaborative leadership challenged the hierarchical organizational structure of the military and intelligence communities (Pearce et al., 2014). The participants confirmed the totemic structure of the military, the practice of information compartmentalization, and the authoritative military chain of command, which run contrary to the collaborative leadership style and its promise of heightened organizational justice.

The literature on organizational congruence contextualized an operative's willingness or unwillingness to complete an assigned task (Williams, 1993, 2002). Organizational congruence refers to individual alignment with organizational values, which contributes to individual decision-making processes and ethical behavior. The participant responses indicated that 48% achieved congruence with intelligence community values while 7% felt adamant incongruence. As a whole, the intelligence operatives claimed to transform their behavior to fit a skewed ethical model during their tenure of service in the intelligence community.

Overall, the participants articulated a need for effective communication to guide ethically ambiguous circumstances and decision-making processes, provide reporting criteria and guidance, offer nonrepudiation assurance if decisions were made erroneously based on partial information, and institute a nonattributable reporting capability. Overall, data indicated the need for such a communication mechanism to sidestep individual responsibility for operational decisions that concern ethics ("taking it upon oneself to decide what is right and what is wrong").

5.2 The Transactional Ethics Communication Framework (TECF)

Due to the absence of a unified framework for guiding ethical decisions, as noted in the literature review and the research findings, the research contributes a communication framework for the intelligence community and stakeholder groups to the field. The framework derives from the following defensible theoretical statements that emerged from the findings:

- The research findings built an understanding of how intelligence operations influence individual operative behaviors through ethical decisioning. Tasks, orders, and directives all validated an observed authoritative influence and

assumed legal agency alignment with accepted knowledge-compartmentalization practices.

- Ethical boundaries were defined within NSA intelligence operations through programmatic context to protect sources and methods.

- The divergence between intelligence operative agent behavior and intelligence community conduct policies surfaced in the forms of resignation, exposure behaviors, internal moral conflict, and organizational incongruence.

- Individual intelligence agent ethical deviation produced an observed negative impact on the greater intelligence community in the form of repudiation (e.g., program or access exclusion, degradation of access, or compeer scrutiny).

These observations grew from evidentiary data that surfaced in existing and applied theories concerning ethics, leadership, and congruence, as well as primary ethnographic research. The research activates this new knowledge through the generation of a conceptual model that more distinctly maps intelligence operations within ethical parameters and can be leveraged in the intelligence community to inform operative decision making during events of ethical conflict.

5.2.1 TECF Components

The participant response data analysis also shaped components of the communication mechanism that could contribute to ethical decisioning that arises during intelligence operations. The participant findings unearthed the need for the following fundamental components:

- redundant, required, and universal communication to educate intelligence operatives on available communication mechanisms and inclusive accessibility modalities, regardless of service circumstances (e.g., deployed or strategic) or agency employment type (e.g., contractor, military, or civilian);

- nondiscretionary prescriptive policy directive language to mitigate interpretations of acceptable mission practices;

- the creation, adoption, and enforcement of policy directives that aim to prevent mission-related unethical behavior;

- the creation, adoption, and enforcement of policy directives that provide safeguards and amnesty for operatives who enact their right to use the proposed communication mechanism;
- defined and cited mission-agnostic policy directives instituting ethical behavior practices in intelligence work, including how to recognize unethical behavior and escalate concerns;

- a top-down modeled behavior approach to use the proposed ethical communication mechanism to complement mandatory interactive training; and

- a timely, reliable, and confidential communication mechanism.

5.2.2 TECF Purpose

The goal of the ethical communication framework is to function as a system of exchanged messages (communication construct) that aids in disambiguating tasks and orders for those serving in the intelligence community. The framework enables operatives to pause, inquire about the circumstances surrounding an ethical decision, or raise an ethical matter for committee consideration to prevent individuals from engaging in unethical practices.

5.2.3 TECF Approach

Offering a programmatic implementation approach, this communication framework leverages operational safeguards to ensure continued participation. The research recommends that the ethical communication mechanism be implemented via digital methods (software as a service platform, software enabled devices, or infrastructure as code) to provide universally accessible, integrated, discretionary, data redundant, movement, and storage capabilities (initial contact phase). The digital structure is designed to facilitate information exchanges and ethical conflict resolution.

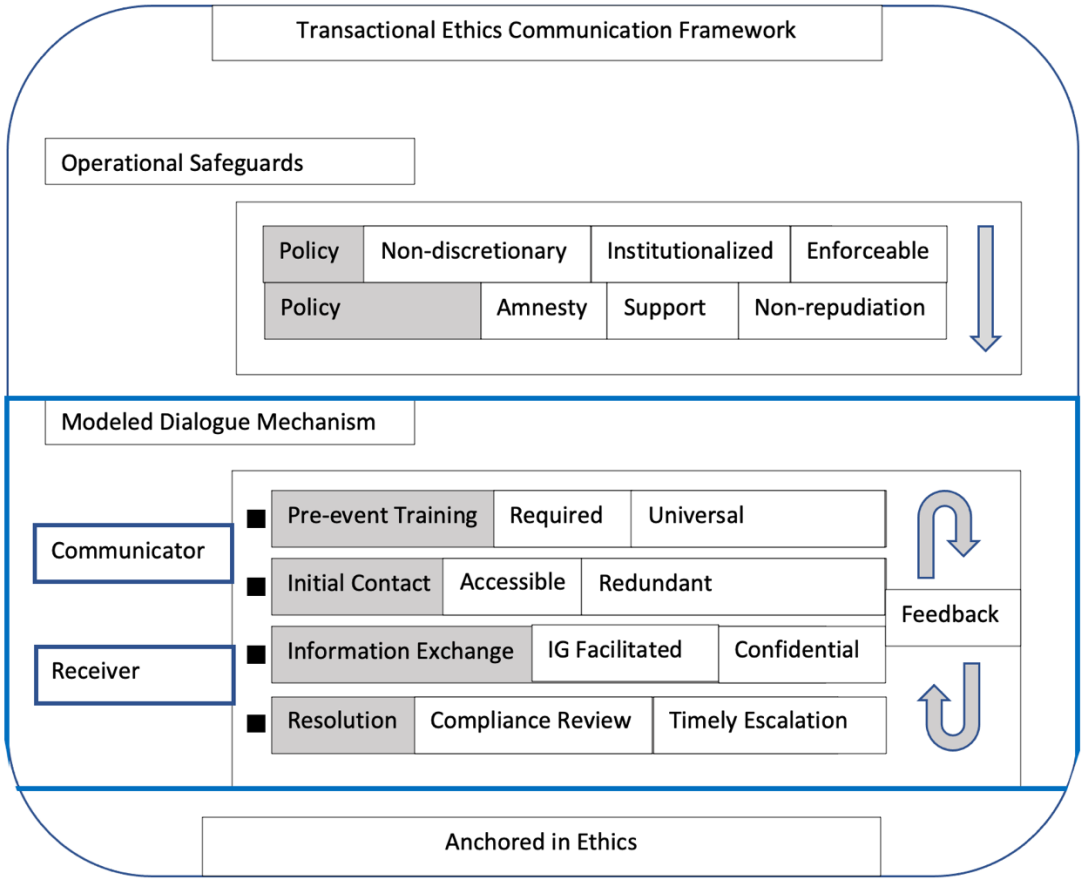
The TECF comprises four main phases of a total communication process: pre-event, initial contact, information exchange, and resolution. Within the modeled dialogue mechanism, the presence of a communicator and a receiver are required. These parties communicate via message exchanges to ensure that intelligence operational methods fall within standardized ethical parameters.

The communicator is the intelligence operative experiencing the ethical dilemma or facing an ethical decision point. The communicator participates in the pre-event, initial

contact, and information exchange phases. During the pre-event phase, education of intelligence agency personnel would take place. Education could occur via multi-echelon socialization efforts and mandatory interactive training in which the trainees would achieve proficiency in utilizing the mechanism.

The receiver's role is fulfilled by IG ethic officers (or similar) and an independent compliance review committee sponsored by internal audit or legal departments. The receiving parties offer timely and confidential message reviews during the information exchange and resolution phases. The framework positions intelligence leadership to provide overt, sincere support and advocacy during all phases of the communication cycle. In the TECF (see Figure 4), the communication exchange involves an ongoing, circular process. This feedback loop ensures that the framework is assessed and evaluated for continued effectiveness.

FIGURE 4
Transactional Ethics Communication Framework (TECF)



Source: Cole, 2022

5.2.4 TECF Implementation

The research covers the implementation of the TECF to ensure that the guidance remains relevant and sustainable. An implementation checklist operationalizes the TECF during three main stages: (a) implementation planning, (b) establishment and execution of TECF tasks, and (c) the identification of implementation support elements needed for successful launch and sustainability.

The implementation checklist can assist singular or joint intelligence entities in operationalizing the TECF by providing a reference during planning and implementation phases. The checklist serves as a guide or starting point to ensure basic components are considered when launching the framework. Depending upon the operating environment, some of the outlined variables within the checklist may or may not apply. The implementation checklist reflects three main segments: (a) TECF implementation planning, (b) establishment and execution of TECF tasks, and (c) the identification of TECF implementation support elements needed for successful launch and sustainability. Other considerations not cited in the implementation checklist may serve as influential factors to enhance the communication framework utility.

Appendix N in the dissertation document provides a robust checklist that covers the three phases of implementation. The planning phase involves successful TECF launch factors, including organizational change and utilization of existing communication mechanisms and constructs to leverage and advance existing knowledge and behavioral norms. During the execution phase, the agency-appointed business or operational unit responsible for actualizing the TECF implementation would nominate a subordinate joint force to coordinate the organization, equipment, and preparation for the implementation phase. During the last phase, the identification of support elements becomes crucial to implementation success and sustaining the operation of the TECF.

5.2.5 TECF Governance

The research recommends that the TECF receive adequate oversight and governance from an appropriate, dedicated entity that is guided by evaluative metrics during the formative, process, and outcome stages of implementation. Programmatic governance of the TECF may be conducted by internal audit resources or allocated compliance teams. The evaluative metrics of an operational communications framework could include formative, process, or outcome evaluations, depending on an organization's available resources (e.g., staff, expertise, budget, etc.), program maturity, and organizational tenure. To ensure standardization and implementation adherence, meaningful diagnostics must coexist with sustainable quality assurance practices.

5.2.6 TECF Summary

The TECF model is designed to introduce informational exchange concepts and define principal functional communication components to guide dialogic engagement among intelligence operatives and leadership to raise and disambiguate ethical decision points pertinent to operational mission objectives. It is expected that the TECF will promote methodical and ethical decision making among members of the intelligence community, reduce immoral conduct, prevent policy deviance, and increase recusals. Through streamlined implementation and adequate governance, the TECF may bring behavioral transparency to all participating branches of government, which could systematically reduce abuses.

Few systematic applications of operational intelligence ethics have been proposed; as a result, no domestic model or framework for individual intelligence accountability have evolved. However, if ethics are not launched to the forefront of operational behaviors within national defense environments, the disparity between human rights and technologically advanced capabilities will remain.

6. Conclusion

The present research inaugurated a unique contribution to the field of ethics within the intelligence community. Pertinent limitations to the research were discussed to provide realistic scope and manage investigative expectations. The validity and reliability of the research methodology were also adjudicated using credible evaluation criteria.

The literature review and research findings illustrated the need for a framework to guide intelligence operatives in making significant ethical decisions each day in an ethically tenuous field. The qualitative research findings yielded an enriched and intimate understanding of the congruence between clandestine operational behaviors, thought processes, leadership styles, and rationale as they relate to ethics.

The research uncovered nine main findings:

1. the perception of the current state of ethics in the U.S. intelligence community;
2. the ethical boundaries that are presently defined for NSA intelligence operations;

3. an understanding of how individual operative behaviors (ethical decisioning) are influenced by intelligence operations;

4. the points of divergence between intelligence operative behavior and intelligence community policies and directives;

5. the perceived impact to the larger intelligence community resultant from ethical deviation by intelligence operatives;

6. the significance and multidimensional advantages of communication in intelligence operations;

7. the evaluation of need for an effective, accessible ethical communication mechanism;

8. the formulation and generation of the TECF that facilitates dialogue for ethical decision making and that incorporates ethics, leadership, and organizational congruence; and

9. the premise that the TECF provides an accessible and effective means for intelligence operatives to communicate and disambiguate operational, ethical concerns.

The findings of this research can improve the practice of prioritizing ethics in intelligence operations to protect agents who face risks due to their personal involvement in ethical decisions and formalize ethical minimums that should govern behaviors in the line of intelligence work. As such, the research paves the way for (a) improved ethical oversight, (b) acceptable and explicit operational standards, and (c) a functional ethical framework that opens the gateway for dialogic ethical analysis among intelligence operatives and officers.

Through the development of the TECF, the present research contributes significant knowledge in the field of applied ethics. The transactional ethics communication conceptual framework serves as a tool that illustrates the interdependent nature and significance of ethics, leadership, and organizational congruence in guiding ethical decision-making practices within the intelligence community.

6.1 Recommendations for Future Research

The research also opens new avenues for further research by inviting scholars to address, among other topics, organizational culture and ethics in intelligence communities across geopolitical borders. The following recommendations for future research are proposed:

1. Conduct a retrospective analysis of intelligence policies circa 2020 as compared to modernized policies of a future state to evaluate the impact of ethical centrality upon mission completion and succession rates in support of national defense intelligence missions. This comparative linear regression analysis would be meaningful in validating the correlation between ethical behavior and mission success variables in ethics advocacy as a core intelligence community governance strategy.

2. Conduct an associative analysis of organizational edge data (e.g., positional application rates, social media content, and collegiate internships) to identify how public sentiment, support, and confidence are impacted by overt ethical policy implementation. This type of correlative analysis could inform projective engagement estimates for community-based intelligence agency partnership programs (e.g., university and academic laboratories and industry sector partnerships).

3. Conduct an exploratory analysis to determine interrelationships among ethical business practices within the intelligence community along with organizational human resource performance and employee behaviors (e.g., talent acquisition, attrition, employee performance, tenure, and absenteeism). This type of analysis would be valuable in diagnosing the interdependencies among an organizational culture anchored in ethics, business continuity, and prosperity.

4. Conduct a vignette of analyses to better understand how ethics are interpreted and implemented across geopolitical boundaries. This analysis would be valuable in illuminating how ethics are understood and enacted within various cultural contexts in support of varying singular and collective defense missions (e.g., country specific ministries of defense and the North Atlantic Treaty Organization).

6.2 Significance

This research is considered significant as it addresses the critical philosophical problems that face the individuals who protect U.S. national security. Through the theoretical literature review and phenomenological research, the research illuminates the intersections among ethics, leadership, congruency, and intelligence operations at a critical juncture when advanced technologies shift the boundaries between privacy and surveillance.

The present research also contributed significant knowledge in the field of applied ethics through the development of the TECF. The model introduces informational exchange concepts and defines principal functional communication components to guide conversational engagement among intelligence operatives and leadership to raise and disambiguate ethical decision points pertinent to operational mission objectives. The TECF illustrates the interdependent nature and significance of ethics, leadership, and organizational congruence to develop a future communication framework that could be operationalized in intelligence community ethical decision-making practices.

As the field of applied ethics matures, the adoption of ethics in business process designs, critical decision-making models, and organizational culture is projected to increase. The conversation surrounding ethics in the modern intelligence world continues, but perhaps will be challenged by the research findings in pragmatic ways. Intelligence practices can remain congruent with organizational and behavioral standards, and this expectation can be institutionalized via the incorporation of ethical frameworks.

References

1. Anderson, K. (2015). *A code of ethics and professional conduct for NSA intelligence professionals*. Air War College. https://apps.dtic.mil/sti/citations/ADA620280

2. Andregg, M. (2014). Breaking laws of god and men: When is this allowed for intelligence professionals? *Strategic Monitor*,*16*(3–4), 49–59.

3. Andregg, M. (2016) Ethical implications of the Snowden revelations. *The International Journal of Intelligence, Security, and Public Affairs*, *18*(2), 110–131, https://doi.org/10.1080/23800992.2016.1196942

4. Aristotle, & Sachs, J. (2002). *Nicomachean ethics* (J. Sachs, Trans.). Focus.

5. Augustine. (1993). *Confessions* (F. J. Sheed, Trans.). Hackett. (Original work published 1942)

6. Augustine. Hill, E., In Rotelle, J. E., & Augustinian Heritage Institute, (2021). *The Trinity*.

7. Barrett, C. (2012). *Finding the "right way": Toward an army institutional ethic* (Carlisle Papers). Strategic Studies Institute. https://apps.dtic.mil/sti/pdfs/ADA569665.pdf

8. Beauchamp, T. L., & Bowie, N. E. (1988). *Ethical theory and business* (3rd ed.). Prentice-Hall.

9. Bellaby, R. (2012, February). What's the harm? The ethics of intelligence collection. *Intelligence & National Security, 27*(1), 93–117. https://doi.org/10.1080/02684527.2012.621600

10. Bellaby, R. W. (2016). Justifying cyber-intelligence. *Journal of Military Ethics, 15*(4), 299–319. https://doi.org/10.1080/15027570.2017.1284463

11. Berkovich, I. (2014). Between person and person: Dialogical pedagogy in authentic leadership development. *Academy of Management Learning & Education*, *13*(2), 245–264. https://doi.org/10.5465/amle.2012.0367

12. Braun, H. E., De Bom, E., & Astorri, P. (Eds.). (2022). *A companion to the Spanish scholastics*. Brill.

13. Caza, A., & Jackson, B. (2011). Authentic leadership. In A. Bryman., D. Collinson, K. Grint, B. Jackson, & M. Uhl-Bien (Eds.), *Sage handbook of leadership* (pp. 350–362). Sage.

14. Chan, A. (2005). Authentic leadership development: Emergent themes and future directions. In W. L. Gardner, B. J. Avolio, & F.O. Walumbwa (Eds.), *Authentic leadership theory and Practice: Origins, effects and development* (pp. 227–252). Elsevier.

15. Christopher, P. (1994). *The ethics of war and peace.* Prentice-Hall.

16. Cogan, C. (2004). Hunters not gatherers: Intelligence in the twenty-first century. *Intelligence and National Security, 19*(2), 304–321. https://doi.org/10.1080/0268452042000302010

17. Crosby, B. C., & Bryson, J. M. (2005). A leadership framework for cross-sector collaboration. *Public Management Review*, *7*(2), 177–201. https://doi.org/10.1080/14719030500090519

18. Dimmock, M., & Fisher, A. (2017). *Ethics for A-level*. Open Book.

19. Elders, L. (2019). *The ethics of St. Thomas Aquinas: Happiness, natural law, and the virtues*. The Catholic University of America Press.

20. Erskine, T. (2004). 'As rays of light to the human soul'? Moral agents and intelligence gathering. *Intelligence and National Security, 19*(2), 359–381. https://doi.org/10.1080/0268452042000302047

21. Esposito, M., & Williams, L. (2010). *Moving beyond human and organizational incongruence.* HAL Archives-Ouvertes. http://hal.grenoble-em.com/hal-00542258/document

22. Friman, H. (2007). Innovation, change and experimentation: A new model for addressing organizational challenges in military intelligence. *American Intelligence Journal, 25*(1), 29–37.

23. Giles, K. (2019). *Command decision: Ethical leadership in the information environment*. Strategic Studies Institute. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1934&context=monographs

24. Godfrey, E. D., Jr. (1978). Ethics and intelligence. *Foreign Affairs, 56*(4), 867–875. https://doi.org/10.2307/20039997.

25. Govinfo. (n.d.). *Accountability and oversight.* Retrieved August 22, 2021, from https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int018.html

26. Graeff, C. L. (1983). The situational leadership theory: A critical view. *The Academy of Management Review*, *8*(2), 285–291. https://doi.org/10.2307/257756

27. Herman, M. (2004). Ethics and intelligence after September 2001*. Intelligence and National Security, 19*(2), 342–358. https://doi.org/10.1080/0268452042000302038

28. Hersey, P., & Blanchard, K. H. (1996). Life cycle theory of leadership. *Training Development Journal, 23*(5), 26–34.

29. Huxham, C. (2003). Theorizing collaboration practice. *Public Management Review, 5*(3), 401–423. https://doi.org/10.1080/1471903032000146964

30. Keller, J. W., & Foster, D. M. (2012). Presidential leadership style and the political use of force. *Political Psychology, 33*(5), 581–598. https://doi.org/10.2307/23324176

31. Kumar, M., & Santoro, D. (2017). A justification of whistleblowing. *Philosophy & Social Criticism*, *43*(7), 669–684. https://doi.org/10.1177%2F0191453717708469

32. Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* Sage.

33. Lindblöm, L. (2007). Dissolving the moral dilemma of whistleblowing. *Journal of Business Ethics, 76*, 413–426. https://doi.org/10.1007/s10551-006-9291-2

34. Luthans, F., & Avolio, B. J. (2003). *Authentic leadership: A positive development approach. Positive organizational scholarships*. Berrett-Koehler.

35. Luthans, F., Baack, D., & Taylor, L. (1987). Organizational commitment: Analysis of antecedents. *Human Relations, 40*(4), 219–237. https://doi.org/10.1177/001872678704000403

36. Mackie, J. (1977). *Ethics: Inventing right and wrong.* Penguin.

37. Meglino, B., Ravlin, E., & Adkins, C. (1989). A work values approach to corporate culture: A field test of the value congruence process and its relationship to individual outcomes. *Journal of Applied Psychology, 74*(3), 424–432. https://doi.org/10.1037/0021-9010.74.3.424

38. The National Counterintelligence and Security Center. (n.d.). *Law*. Retrieved March 17, 2022, from https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-law

39. Northouse, P. G. (2013). *Leadership: Theory and practice* (6th ed.). Sage.

40. Pearce, C. L., & Conger, J. A. (2003). *Shared leadership: Reframing the hows and whys of leadership.* Sage.

41. Pearce, C. L., Wassenaar, C. L., & Manz, C. C. (2014). Is shared leadership the key to responsible leadership? *Academy of Management Perspectives, 28*(3), 275–288. https://doi.org/10.5465/amp.2014.0017

42. Pfaff, T., & Tiel, J. (2004). The ethics of espionage. *Journal of Military Ethics*, 3(1), 1–15. https://doi.org/10.1080/15027570310004447

43. Phythian, M., & Omand, D. (2012). Ethics and intelligence: A debate. *International Journal of Intelligence and Counterintelligence, 26*(1), 38–63. https://doi.org/10.1080/08850607.2012.705186

44. Rawls, J. (1971). *Theory of justice.* Harvard University Press.

45. Ronn, K. V. (2016). Intelligence ethics: A critical review and future perspectives. *International Journal of Intelligence and Counterintelligence, 29*(4), 760–784. https://doi.org/10.1080/08850607.2016.1177399

46. Rutkauskas, V. A., & Stasytyte, V. (2013). Leadership intelligence: How to get there? *Procedia - Social and Behavioral Sciences*, *75*, 52–61, https://doi.org/10.1016/j.sbspro.2013.04.007.

47. Schwandt, T. A., & Halpern, E. S. (1988). Constructing an audit trail. In T. A. Schwandt & E. S. Halpern (Eds.), *Applied social research methods: Linking auditing and metaevaluation* (pp. 71–103). Sage.

48. Smith, D. (2005). *Institutional ethnography: A sociology for people*. Alta Mira Press.

49. Thompson, T. J. (2018). A psycho-social motivational theory of mass leaking. *International Journal of Intelligence and Counterintelligence*, *31*(1), 116–125. https://doi.org/10.1080/08850607.2017.1374800

50. Tornau, C. (2020). Saint Augustine. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy.* https://plato.stanford.edu/archives/sum2020/entries/augustine/

51. U.S. Department of Defense. (2010). *National Security Agency/Central Security Service* (Directive No. 5100.20). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510020p.pdf

52. U.S. Department of Justice, Office of Legal Counsel. (2002). *Memorandum for Alberto R. Gonzalez, Counsel to the President.* https://www.justice.gov/olc/file/886061/download

53. Van Wart, M. (2013). Lessons from leadership theory and the contemporary challenges of leaders. *Public Administration Review, 73*(4), 553–565. https://doi.org/10.1111/puar.12069

54. Velasquez, M. G. (2006). *Business ethics: Concepts and cases*. Prentice Hall.

55. Wang, D., Waldman, D. A., & Zhang, Z. (2014). A meta-analysis of shared leadership and team effectiveness. *Journal of Applied Psychology, 99*(2), 181–198. https://doi.org/10.1037/a0034531

56. Williams, L. C. (1993). *The congruence of people and organizations: Healing dysfunction from the inside out.* Quorum Books.

57. Williams, L. C. (2002). *Creating the congruent workplace: Challenges for people and their organizations.* Quorum Books.