



CYBER INTELLIGENCE: Preparing Today's Talent for Tomorrow's Threats

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
CYBER INTELLIGENCE TASK FORCE
SEPTEMBER 2015



ACKNOWLEDGEMENTS

CHAIRMAN

Ambassador John Negroponte

STAFF

Ambassador Joseph R. DeTrani, *President*

Chuck Alsup, *Vice President of Policy*

Dave White, *Senior Policy Advisor and Resident Fellow*

Ryan Pretzer, *Policy and Public Relations Manager*

English Edwards, *Marketing and Communications Manager*

William Cullin, *Fellow*

Noel Hardesty, *Cyber Training & Education Intern*

CYBER COUNCIL CO-CHAIRS

Terry Roberts, *Founder, CyberSync, Inc.*

Ned Deets, *Director, Software Solutions Division,
Software Engineering Institute*



CYBER INTELLIGENCE TASK FORCE

Writing Team

Dr. Randy Borum, *Professor and Coordinator for Strategy and Intelligence Studies, School of Information, USF*

Dr. Ronald Sanders, *Vice President and Fellow* Booz | Allen | Hamilton

CYBER INTELLIGENCE TASK FORCE

Editing Team


Ron Carback, *Defense Intelligence Officer for Cyber, Defense Intelligence Agency*

John Felker, *Director of Operations, National Cybersecurity and Communications Integration Center, DHS*

Bob Gourley, *Partner, Cognition; Publisher, ThreatBrief.com*

Geoff Hancock, *CEO, Advanced Cybersecurity Group*

EDITORIAL REVIEW

Joe Mazzafrò 

COPY EDITORS

Joey Dahl, *INSA Intern*

Christina Ma, *INSA Intern*

Jessica Di Paolo, *INSA Intern*

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.



EXECUTIVE SUMMARY

Cyber intelligence – assessing an adversary’s capabilities, intentions, and activities in the cyber domain – should support and inform the entirety of an organization’s network operations, including offensive and defensive processes. Though essential to an organization’s cyber activities, cyber intelligence as a professional discipline is relatively emergent, particularly its unique tradecraft – a blend of technical knowledge (e.g., network operations, communications, and perhaps digital forensics or malware reverse engineering) and classic analytic skills (e.g., hypothesis and alternative testing). We believe that it is time for this nascent but increasingly critical intelligence discipline to have its own professional development blueprint. This paper is largely dedicated to examining how such a blueprint may take shape, to include the following foundational elements:

- **A common body of knowledge** that establishes a shared framework of terminology, domains of knowledge, and first principles of practice;
- **A competency-based framework** that would inform upon which areas a cyber intelligence analyst should be knowledgeable, encompassing technical, analytic, informatics, contextual domain and communication/organizational competencies;
- **A dual-track development model** that would emphasize the training of technical and analytic competencies differently, depending on the analyst’s background and experience, the proficiency level required to meet his/her responsibilities, and whether he/she is operating at a strategic, operational or tactical level;
- **A training and education program** that tracks the skill sets and proficiency levels required of the cyber intelligence analyst at the entry level, the specialized or retrained expert level, and senior executive level; and
- **Prototypical career paths** that provide a sequential list of positions or roles, qualifications, critical development experiences, skill sets to be accrued or strengthened, and important success factors one could anticipate in their career progression as a cyber intelligence analyst.

While there has been a proliferation of formal and informal education and training initiatives to prepare analysts to provide cyber intelligence-related support to organizations in the public, private and academic sectors, the quality and usefulness of these initiatives varies widely, as few focus on cyber intelligence as a distinct, unique academic discipline. This may very well change over time, and leveraging the good work already done by the National Security Agency (NSA) and Department of Homeland Security (DHS) through their National Centers for Academic Excellence in Information Assurance/Cyber Defense program offers an opportunity to accelerate the process by including knowledge units and focus areas dedicated to cyber intelligence. Related continuing education initiatives could then easily be developed so that comprehensive training and education standards would be available to guide establishment of entry-level, mid-career, and senior-level professional education and development.

INTRODUCTION

Targeted by an increasingly persistent and complex array of cyber threats, organizations across the public and private sectors must strive to get ahead of the threat curve. To do so, organizations are turning to cyber intelligence. This emerging discipline requires a blend of technical expertise and classic analytic tradecraft; however, little consensus has formed around a training and education model to prepare individuals and teams to perform this critical role. This paper identifies some of the core competencies critical to its successful performance and offers a preliminary training and education framework.

Cyber intelligence is defined here as the products and processes across the intelligence cycle of assessing the capabilities, intentions, and activities – technical and otherwise – of potential adversaries and competitors in the cyber domain (with cyber counterintelligence as a sub-discipline). For purposes of this paper, the category of adversaries includes individuals and organizations using the cyber domain¹ for criminal and related fraudulent activities. The term *cyber intelligence* is used for two reasons. First, in national security and defense organizations, cyberspace is often treated as a designated domain², not dissimilar from maritime, land, air, or space. In that context, domains often specify the point of reference in intelligence collection and analysis (e.g. maritime intelligence). Second, intelligence pertains to actionable knowledge derived from processed, or analyzed, data and information. Intelligence should be distinguished from raw threat data, such as strings of code, and unprocessed threat information, such as feeds from the U.S. Computer Emergency Readiness Team (US CERT). Intelligence functions for cybersecurity include collecting, processing, analyzing, contextualizing and reporting threat information to a supported decision maker so that it can be used effectively³.

Intelligence is essential to an effective cybersecurity mission. NATO recognizes “Intelligence and Counter-Intelligence” as one of five designated mandates of national cybersecurity⁴; similarly, the 2014 U.S. National Intelligence Strategy identifies cyber intelligence as one of the Intelligence Community’s four mission objectives (alongside counterterrorism and counterproliferation)⁵ and the U.S. Department of Homeland Security (DHS) has identified “threat analyst /counterintelligence analyst” as one of several mission-critical jobs and tasks. According to the 2012 report by the DHS Task Force on Cyber Skills:

Threat Analyst /Counterintelligence Analysts deploy deep and current knowledge of the attack surface, its most vulnerable and high value targets, and how its technical vulnerabilities may be exploited; maintain up to the minute situational awareness on what malicious actors are using and targeting; and develop techniques and program custom tools to detect local changes, identify suspect interactions, and watch for and respond to what the malicious actors are doing. More advanced teams also are able to understand the attackers’ motivation, language, organization, and social behaviors, as well as group the threat actors logically to create effective “cyber” profiles of groups, actors, and campaigns, thereby helping organizations become more proactive in their security posture and defense⁶.



The training paths to become a qualified cyber-intelligence analyst are inconsistent and nonexistent in some cases.

The need to develop a robust cyber intelligence capability is not limited to law enforcement, national/homeland security and intelligence agencies or military organizations. Commercial and other quasi-public entities (e.g., public utility companies, financial institutions, etc.) are realizing that they too must have a similar capability if they are to secure their own networks and data. While the intelligence tradecraft has been around for years, the discipline of cyber intelligence is continuing to evolve and mature, and so too are the training and education requirements necessary to prepare individuals for the discipline.

Cybersecurity education and training programs have proliferated throughout the U.S. in response to the growing hazards of malicious cyber activity^{7,8,9,10,11,12}, yet virtually

none of those programs provide systematic training in intelligence collection, analysis and management. In addition, it is not clear whether these programs have been informed systematically by the needs of the U.S. Intelligence Community and law enforcement organizations (both US and international) to understand foreign national and transnational cyber threat capabilities and intentions. As a result, a recent review of academic cybersecurity programs in the U.S. concluded that “[t]he training paths to become a qualified cyber-intelligence analyst are inconsistent or nonexistent in some cases.¹³” Currently, there are only about seven schools in the U.S. known to offer a specific course in cyber intelligence, and only a couple that offer a specialization or concentration within a related master’s degree program¹⁴.

A COMMON BODY OF KNOWLEDGE

With few specified career paths or systematic curricula in cyber intelligence, the current array of roles, skills, preparation and standards among professionals engaged in cyber intelligence activity is fuzzy and varied. As a discipline of study and practice, cyber intelligence is in its early stages of maturity. However, the foundation of knowledge in its two parent disciplines – cybersecurity and intelligence studies – is more fully developed. Drawing on the knowledge base, educational programs and career descriptions of those more mature disciplines will accelerate the professionalization of cyber intelligence analysis.

As a foundation for cyber intelligence training and education standards, the field of cyber intelligence would benefit from a Common Body of Knowledge (CBK), which establishes both a taxonomy and a “peer-developed compendium of what a competent professional in the field must know”^{15,16}. In essence, by employing common ontology, domains of knowledge, skills, techniques, and first principles of practice, professionals in the field can better communicate, learn from each other and advance knowledge and practice in the field based on a shared, collective understanding.

Just as importantly, the CBK also can serve as a foundation for establishing academic curricula and programs to ensure that graduates meet entry-level, intermediate, and advanced workforce expectations. Numerous disciplines have used the CBK approach to define their current state of knowledge and practice and to anchor discussions about

what knowledge still needs to be developed and how these might impact the future of the field^{17,18,19, 20, 21, 22, 23, 24, 25, 26, 27}. While a CBK is not the final word on the foundations of any discipline, having a shared language and common points of reference facilitates further inquiry and debate.

The National Institute for Standards and Technology (NIST) and other U.S. government agencies have teamed with the scientific and professional communities such as the National Research Council to identify cybersecurity workforce requirements and standards. Those efforts offer a starting point for structuring the relevant specialized domains of knowledge specifically required for cyber intelligence.

NIST launched one of the first efforts to outline industry standards and best practices in response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*²⁸. NIST developed a voluntary, risk-based cybersecurity framework through collaboration between government and the private sector that uses a common language to address and manage cybersecurity risk. The core functions outlined in the framework include the following, and cyber intelligence plays a key role in each:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

As a companion to that effort, NIST led one of the most comprehensive analyses of cybersecurity skills ever undertaken. The result – the National Cybersecurity Workforce (NCW) Framework²⁹ – offers great promise as a basis for developing cyber intelligence training and education requirements. The NCW Framework consists of 31 specialty areas organized into seven categories, within which cyber intelligence is treated more as a component set of professional cybersecurity requirements than a distinct discipline³⁰. Functions that we would include in our definition of cyber intelligence are within the *Analyze* category. However, there are as yet no KSAs – knowledge, skills and abilities – provided in the framework corresponding to the *Analyze* category because the NCW working group deemed them to be too sensitive and/or classified.

This mind set is unfortunate. Breaking through this inclination to treat cyber intelligence as an inherently governmental, “classified” (that is, national security-related) discipline is essential to establishing a CBK and maximizing its subsequent benefits to the public and private sectors. In point of fact, the *Analyze* category really only describes a set of general functions that may be essential to classified cyber intelligence, but that also are applicable across other sectors and industries. *Analyze* encompasses four designated specialty areas – Threat Analysis, All Source Intelligence, Exploitation Analysis and Targets – comprised of activities for the “highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence³¹,” as demonstrated in Figure 1.

ANALYZE

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Threat Analysis

Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Exploitation Analysis

Analyzes collected information to identify vulnerabilities and potential for exploitation.

All Source Intelligence

Analyzes threat information from multiple sources, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Targets

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Figure 1: NCW Framework category – Analyze

Researchers at Carnegie Mellon University’s Software Engineering Institute³², recognizing the dearth of training and education opportunities for cyber intelligence analysts, conducted a survey of cyber intelligence programs across the public and private sectors in 2012 as part of the Cyber Intelligence Tradecraft Project (CITP), one goal of which was to “define the core competencies and skills that make up a successful cyber intelligence analyst.” Unlike the NCW Framework, the CITP (Figure 2) considers cyber intelligence a distinct discipline whose core competencies – “teachable skills” – include:

- Critical Thinking
- Data Collection & Examination
- Communication & Collaboration
- Computing Fundamentals
- Information Security
- Technical Exploitation

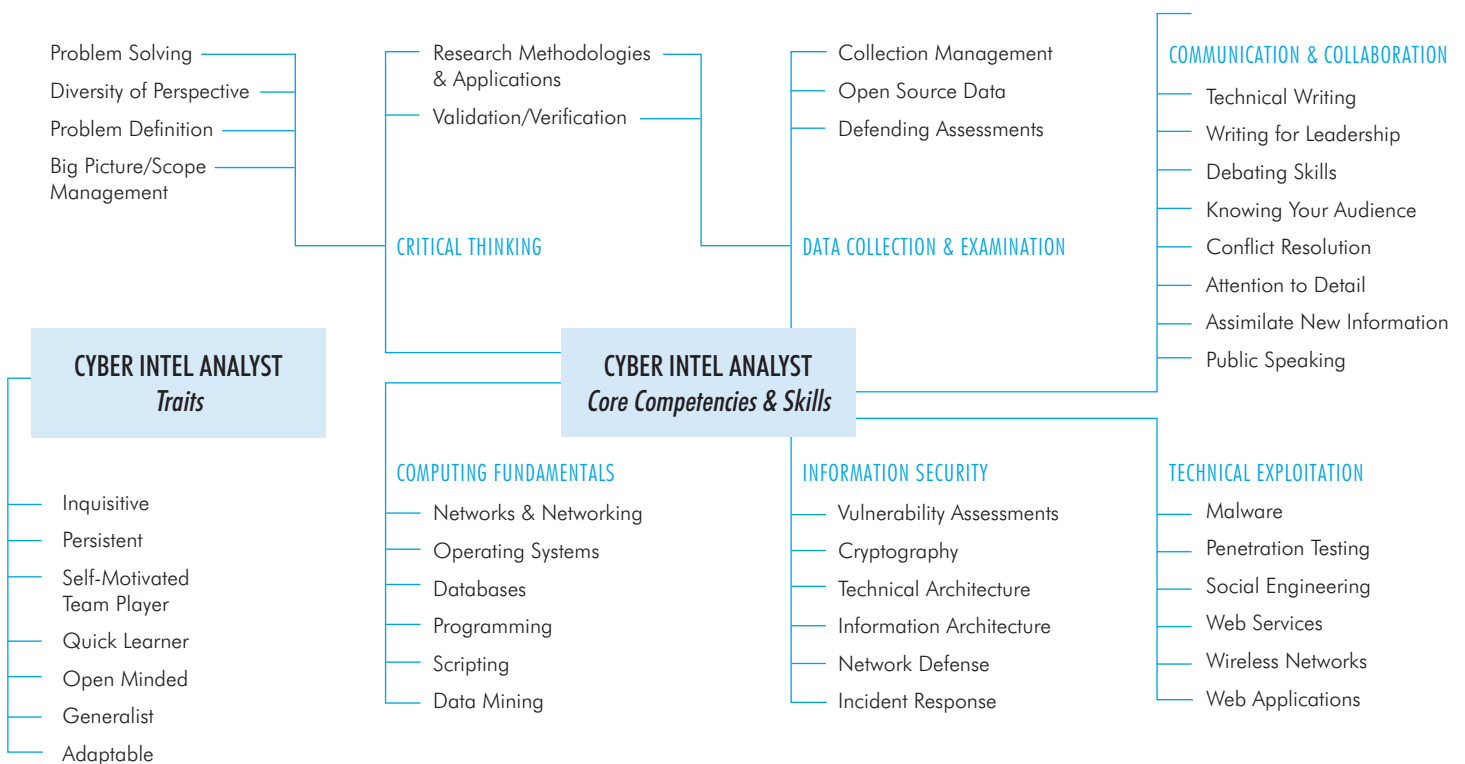


Figure 2: The CITP Core Competencies & Skills

The CITP study explicitly includes and clusters both analytic and technical domains, what some might call the “soft” and “hard” skills required for effective cyber intelligence. In contrast, while the NCW Framework does refer to some relevant cyber intelligence functions, it does not disaggregate the component foundations of analytic tradecraft. Understanding the discipline and professional practice of cyber intelligence requires that analytic and technical domains not only be included, but that they be treated as integrated equals.

Because cyber intelligence is as much or more of an analytic discipline than a purely technical one, professionals in the field must be capable of conducting research, developing and evaluating hypotheses, acquiring and managing new knowledge, generating and analyzing courses of inquiry (that is, collection) and action, formulating and solving complex problems, expressing clearly reasoned opinions, and communicating effectively in writing, oral presentation, and visual display^{33, 34, 35, 36} – in addition to understanding computing and information security fundamentals and technical exploitation (though to a lesser extent than specialists).

A COMPETENCY-BASED FRAMEWORK

Integrating elements from all three models (NIST, NCW, and CITP), it is possible to construct a competency-based knowledge framework for cyber intelligence and to parse those models into levels that distinguish between knowledge competencies (awareness and understanding) and proficiencies (skills and abilities). The five categories of competencies would include the following:

- **Technical Competencies:** The technical foundation for understanding the hardware and software of information and communications technology, especially as they relate to cybersecurity, including the operation and underlying mechanisms of workstations, networks, and operating systems; the mechanisms of technical (e.g., malware) and human (e.g., social engineering) vulnerabilities and exploitations; and applied principles and tools of information security, including risk assessment/management, intrusion detection, cryptography, network defense, incident response and recovery.
- **Analytic Competencies:** The social-scientific basis for complex analysis of data and information from a variety of sources, including foundations of strategy, systems thinking, reasoning and logic, problem solving, and decision making. Emphasis is placed on hypothesis generation and testing, and formulating, selecting, and applying appropriate qualitative and/or quantitative analytic methodologies, including collection strategies and methods. This includes recognition and application of ethical and professional/tradecraft standards in choosing and communicating about those methods. When applying analytic competencies to cyber intelligence it is important for the analyst to understand and consider the culture, leadership, behavior, and background of adversaries as well as consumers.

- **Knowledge Management (Informatics³⁷) Competencies:** The knowledge management and information science basis for planning and organizing information collection, developing and applying tools to gather and support complex data and information analysis from heterogeneous sources, information visualization, and understanding, utilizing, and evaluating various information storage and retrieval systems.
- **Contextual Domain Competencies:** The sector-specific, national/regional, psychosocial, and/or sociocultural foundations for analyzing complex problems; identifying key actors and roles; assessing perceptions, interests and intentions; sense-making; drawing inferences from actions and behaviors; and discerning situational influences. Foreign language capability and regional/cultural competence (at the strategic, operational, and/or tactical level) may also be included as a domain competency.
- **Communication and Organizational Competencies:** These competencies emphasize clear expression of opinions and reasoning, along with effective communication of one’s ideas in writing, oral presentation, and visual display. It also comprises the project management skills necessary to plan, organize, evaluate, motivate, mobilize and control resources, processes and outcomes to achieve specific goals.

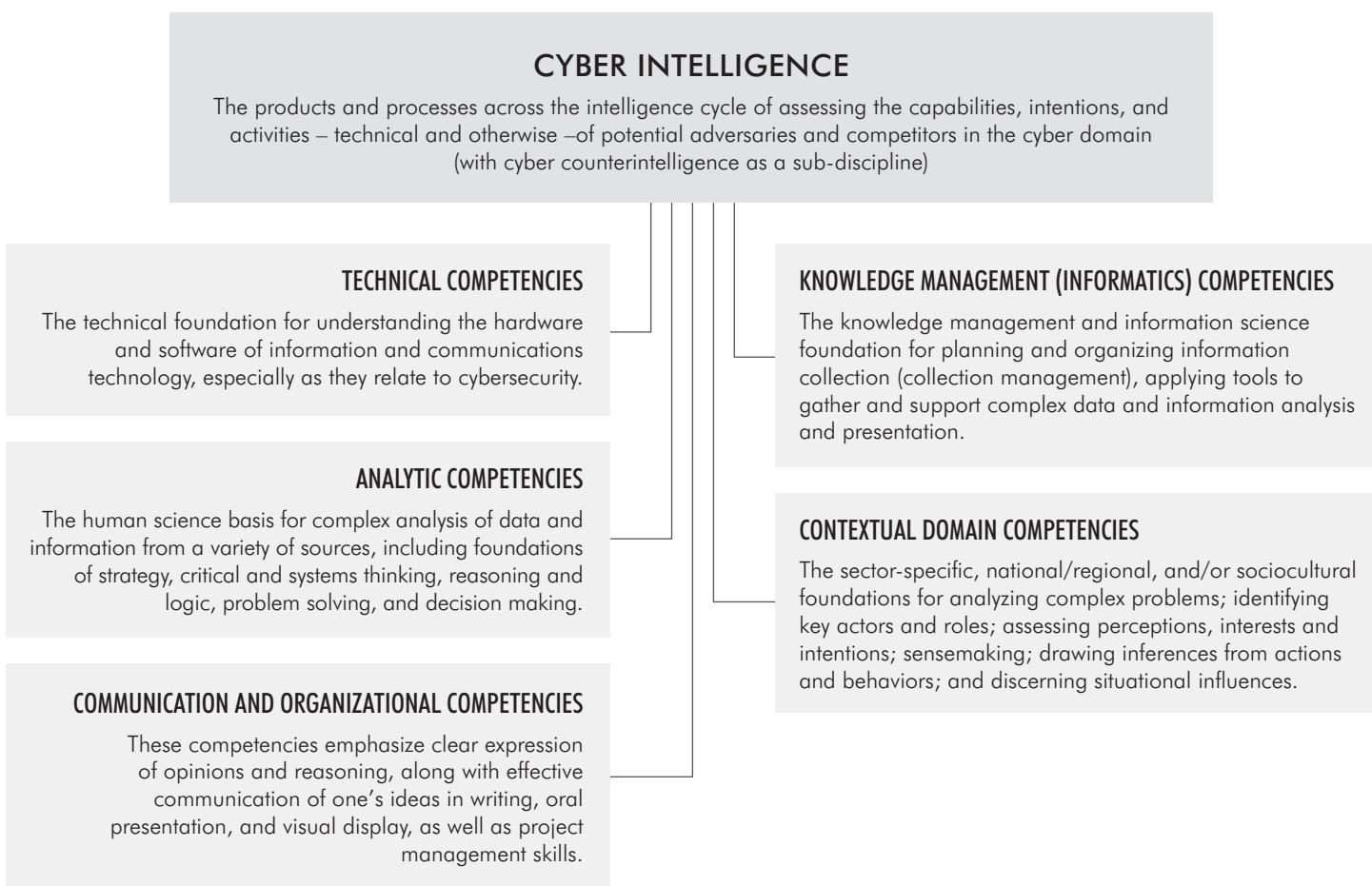


Figure 3: The Five Competencies of Cyber Intelligence

A DUAL-TRACK DEVELOPMENT MODEL: INTEGRATING THE ANALYTIC-TECHNICAL SKILL SETS

A competency-based framework would inform the areas in which a cyber intelligence analyst should be knowledgeable, but it also stands to reason that not every analyst should be expected to demonstrate expertise in all of them. The requisite depth of knowledge will vary for different cyber intelligence professionals – particularly as roles and responsibilities emphasize the technical and analytic competencies differently. For instance, some analysts may require only a rudimentary understanding of cryptography’s terms and basic concepts, whereas a truly proficient cryptographer would be able to independently apply those concepts and mathematical algorithms to create an authentication protocol. Arriving at a balance of analytic and technical skills is an imperative of effective cyber intelligence, and consequently of any training and education framework.

As noted earlier, few integrated and specialized training opportunities exist in cyber intelligence. Thus, the current workforce is composed primarily of people who come from a background of education or experience either in intelligence or in technical computer/systems security, with some degree of “cross training” between the disciplines. People with a technical/computer science background and experience will pick up some intelligence concepts, terminology and tradecraft in the course of their work, just as individuals with a nontechnical intelligence analytic background will learn some cybersecurity concepts, terminology and technical skills.

However, that “cross-training” cannot be unsystematic. The technical and analytic knowledge, skills, and abilities represent broad classes of competencies in cyber intelligence; it is the integration of these “hard” and “soft” competencies that distinguishes cyber intelligence from other cyber specialty areas. Thus, a “dual-track” training and development model – with one track for technically trained cybersecurity professionals who wish to specialize in intelligence (Technical/Analytic) and another for the classically trained intelligence analysts who wish to specialize in the cyber domain (Analytic/Technical) – is a good first step. Both tracks might be grounded on a common body of knowledge, but with each branching to develop distinct roles, required skills, preparation and practices.

The analytic-technical division of emphasis may depend upon where the cyber intelligence professional is operating. The INSA Cyber Intelligence Task Force uses a three-tiered structure to describe the strategic, operational and tactical levels at which actionable knowledge about a cyber threat influences decisions and activities within an enterprise (Appendix A). Those levels are distinguished by the intended consumer, decision requirements, timeframe, adversary characterization, collection scope and methods, and other factors.

It is imperative for both public and private enterprises to have the capacity to collect, analyze, and act upon cyber intelligence at all three levels. This requires a range of professionals, from tactical-level technicians to strategically focused C-Suite executives, each schooled in the tradecraft associated with their level:

- **The entry-level analyst**, who must be equipped to perform basic cybersecurity and related cyber intelligence functions.
- **The cyber intelligence professional**, who has specialized (or retrained) in cyber intelligence, and must perform at a full-performance, expert, or senior-expert level.
- **The senior executive**, who is responsible for assuring the organization's strategic mission and must make decisions about the value of its assets and the resources allocated to protect them. This includes, *but is not limited to*, the CIO, CTO, or CISO.

At the tactical level where incident response occurs, the imperative may be to employ personnel who come with a stronger technical background and to train and grow their analytic capabilities. At the strategic level, however, it is of greater value to employ the person with stronger analytic expertise, while seeking to improve their technical training. The analytic-technical spectrum of training and expertise across the cyber intelligence levels is important to keep in mind, not only for discerning which skills are important, but also understanding the level and type of knowledge, skills, abilities, and attributes the analyst should possess.

This is not to say we should flatly prescribe more technical training to analysts and more analytic skills work to technical professionals, but rather thoughtfully consider where and how to employ their relative expertise. In each case, greater training and education is required in both analytic and technical areas. As a nation, we must seek to effectively develop and employ the right person for the right role while improving learning in both areas.

A TRAINING AND EDUCATION PROGRAM

With a competency-based framework established, it is possible to begin developing a training and education program that tracks the hypothetical career progression of a cyber intelligence analyst from entry level to full-performance professional, and from there to the enterprise executive level. Each level has its own unique set of competencies and proficiencies, and accordingly its own training and education requirements and modalities.

ENTRY-LEVEL ANALYST

The entry-level analyst must be equipped to demonstrate basic cyber intelligence competencies acquired mainly through a balance of technical and analytic training when entering the workforce. Such training could be dual tracked by weighting content more heavily toward either the technical or the analytic, as appropriate (arriving at, in essence, the technical analyst vs. the analytic technician). Track content and focus also could vary based upon near-term organizational roles and expectations.

When Hutchins, Pirolli and Card³⁸ conducted a Cognitive Task Analysis (CTA) for the practice of intelligence analysis (not explicitly cyber related), a pattern emerged:

During this bootstrapping phase of our CTA effort, we learned that there are several career paths for intelligence analysts. These career paths can be categorized as either having more of a *technology emphasis* where the focus is on systems, equipment, and managing the personnel who operate and maintain this equipment or an *analytical emphasis* where the focus and experience is on performing long-range analysis.

If a young person today wanted to prepare for a position as an entry-level cyber intelligence analyst, he or she would likely need to pursue a traditional major (e.g., computer science or intelligence studies), with a minor in the other, complementary track, perhaps even complemented by coursework in a foreign language or regional studies. Currently, a graduate of such a hybrid, self-defined program might struggle to find a clearly delineated career path in a given organization. However, demand for cyber intelligence analysts will only further drive the development of specialized, systematic cyber intelligence training and education programs, as well as more clearly identifiable educational and career opportunities for aspiring professionals.

Numerous formal education and training alternatives exist to prepare the entry-level cyber intelligence analyst, though these programs rarely focus specifically on cyber intelligence as an academic specialty that blends technical and analytic elements. That may change over time, and one way to accelerate that maturation may be through the National Security Agency (NSA)/Department of Homeland Security (DHS) Centers for Academic Excellence in Information Assurance and Cyber Defense (CAE IA/CD) program.

While not an accreditation program per se, the CAE IA/CD program establishes guidelines for curricula in information assurance and cybersecurity, with colleges and universities that conform to these guidelines certified as CAE institutions. Those standards are organized around focus areas and knowledge units (KU). Applicant institutions have the option of applying for one or more of 17 “focus area” designations for their programs, with each focus having its own subset of core and optional KUs that must be met. At present, none of CAE’s 17 focus areas deal with cyber intelligence as we have defined it, but the structure for doing so exists. To that end, NSA and DHS should develop “Cyber Intelligence” as an 18th focus area within the CAE IA/CD program, and add two optional knowledge units to the current list of 51: one for “Intelligence Analysis” (to cover analytic competencies) and another for “Knowledge Management” (to cover the Informatics competencies). Both new units would require a definition, a list of topics, and list of outcomes, which are outlined below as a starting point for further development:

Proposed KU: Intelligence Analysis

DEFINITION

The intent of this knowledge unit is to provide students with sufficient understanding of strategy, critical and systems thinking, intelligence research, decision making, hypothesis generation and testing, and intelligence analytic methodologies and tradecraft such that they can identify, analyze and communicate about the capabilities, intentions, and activities of a potential adversary or competitor in the cyber domain.

TOPICS

- Foundations of strategy
- Critical and systems thinking
- Problem definition, scope management and problem solving
- Judgment and decision making
- Hypothesis generation and testing
- Qualitative and/or quantitative analytic methodologies
- Structured intelligence analytic techniques
- Analytic communication
- Ethics and standards in intelligence analysis

OUTCOMES

Students will be able to:

- Use technologies, methods and tradecraft to retrieve, aggregate, and organize information and to develop and evaluate new knowledge.
- Analyze data and apply information to an organization’s mission and strategic objectives by generating and analyzing courses of action.
- Express clearly reasoned opinions and communicate effectively in writing, oral presentation, and visual display.
- Recognize and apply ethical and professional standards in choosing and communicating about their analytic methodology.

Proposed KU: Knowledge Management

DEFINITION

The intent of this Knowledge Unit is to provide students with the ability to plan and organize information collection (collection management), develop and apply tools to gather and support complex data and information analysis from heterogeneous sources, adapt how data are visually presented to maximize understanding, and to understand, use and evaluate information storage and retrieval systems.

TOPICS

- Foundations of informatics
- Information needs and information seeking
- Information access and retrieval
- Advanced search strategies
- Knowledge evaluation and organization
- Collection management
- Data and information analysis tools
- Information analytics
- Data visualization

OUTCOMES

Students will be able to:

- Plan and organize information collection by developing a collection management plan.
- Demonstrate advanced use of search engines and to use specialized tools for data and information analysis.
- Adapt the presentation of data (including in visual form) to maximize understanding for the audience/decision maker.

These two new KUs would be combined with the following existing units to form the new focus area in cyber intelligence. The focus area definition would be “KUs necessary to impart the skills and abilities for assessing, analyzing and communicating the capabilities, intentions, and activities – technical and otherwise – of potential adversaries and competitors in the cyber domain.”

- 1.1 Basic Data Analysis
- 1.4 Cyber Threats
- 1.5 IA Fundamentals
- 2.5 Probability and Statistics
- 3.35 Overview of Cyber Operations
- 3.41 Security Risk Analysis
- 3.7 Data Administration
- Intelligence Analysis
- Knowledge Management

CONTINUING EDUCATION AND RESPECIALIZATION

In many fields, an undergraduate or even a graduate degree is insufficient to stay current, even when augmented by on-the-job experience and learning. Such is the case in a discipline based on a dynamic, rapidly growing body of knowledge and practice, and cybersecurity may be among the most extreme examples in this regard. People actively working in the cybersecurity field require ongoing professional education if they hope to stay current. In 2000, the half-life of knowledge obsolescence in computer science and computer engineering was estimated at about 2.5 years³⁹. Given the accelerating pace of change in technology and rapidly evolving cyber threat vectors, that half-life is likely to be considerably lower now.

The knowledge, skills and abilities (KSAs) and even domains of knowledge needed for entry-level practice in cyber intelligence will likely change substantially over time. Moreover, as the field of cyber intelligence matures and evolves from today’s *ad hoc* cross-training model to a more deliberate dual-track approach, and eventually perhaps to a fully integrated education and training framework, nonsupervisory cybersecurity professionals at the full-performance level and above will need to understand continuing professional education requirements. This will be necessary both to maintain and to enhance their proficiency, and in some cases to respecialize in cyber intelligence, from basic tradecraft to the leadership and management of cyber intelligence analysts and organizations. Plans for an enhanced cybersecurity workforce should include the present professional cadre performing cyber intelligence functions so that they have opportunities to stay up to date with their technical and analytic skills training.

Continuing education and respecialization for cyber intelligence may be less concentrated in traditional institutions of higher education and rely more heavily on commercial and nonprofit organizations that specialize in providing continuing professional education; the SANS Institute is a preeminent example. Professional education extends beyond technical training but its focus typically is on competency-based application and practice rather than purely theoretical, as often is the case in a traditional, discipline-based academic program. This is a space where many professional certification training offerings seek to operate, though there is currently no certification for cyber intelligence as described here. In the future, having courses and programs of professional education in cyber intelligence will be necessary to keep practitioners current and to make the cyber intelligence function more accessible to a broader range of organizations. This is an imperative for both private industry and the government.

EXECUTIVE LEVEL TRAINING

Managing an organization's cybersecurity posture can no longer be confined to the chief information officer (CIO), the chief information security officer (CISO), and the deep recesses of an organization's network operations center. The CEO, COO and other C-suite executives must acknowledge and appreciate the strategic risks associated with cybersecurity, just as they do other risks to the organization, from its financial viability to its physical infrastructure. Some organizations, recognizing the existential threat that cyber attacks pose to their viability, have established a new senior position to integrate the management of those interdisciplinary risks in a single point of executive accountability: the chief risk officer (CRO). Cyber intelligence enables CROs, CISOs, and other C-Suite executives not only with information to implement preventive and defensive measures on networks and systems, but also help convey the potential implications in the boardroom.

Risk management executives need to be educated about cybersecurity so that they can make better informed strategic decisions, especially in the aftermath of a data breach, electronic espionage, or other cyber disruption. Admittedly, CEOs rarely have the technical background or time to



Bridging the communication gap between technical cybersecurity personnel and executive decision makers should be a high-priority objective.

review and weigh the merits of each cybersecurity measure undertaken to counter a threat or respond to an attack. These executives do not need to develop a new repertoire of technical skills, but rather must appreciate the nontechnical implications of the threat, including the potential impact to business operations, reputation and financial well-being. In addition, executives need support in understanding threat actors' intentions, doctrine, and operations; these factors may have vital implications for enterprise mission and business models for which these executives are responsible.

Thus, while it is imperative for strategic- and operational-level cyber intelligence analysts to have the ear of senior leaders, those senior leaders must also be able to discern the strategic implications of the intelligence they receive. Bridging the communication gap between technical cybersecurity personnel and executive decision makers should be a high-priority objective. Standing up internal cyber intelligence units is one bridge. Another, more sustainable bridge is needed in executive education, however. Educational institutions should consider adding a course in "strategic" information management and cybersecurity to their MBA curricula, especially in executive MBA programs. Shorter, more intense cybersecurity learning experiences for C-suite executives also should be considered. Agencies in the U.S. Intelligence Community and the Department of Defense are required to use military-style "war games" and scenario-based exercises for incident-response planning. Many organizations in the private sector have adopted this kind of training as well, and found it to be particularly effective in helping senior executives comprehend, manage, and experience the consequences of cybersecurity threats and attacks in a safe and risk-free environment.

PROTOTYPICAL CAREER PATHS

The tiered training program of the entry-level analyst, retrained/specialized professional and senior executive can inform a cyber intelligence professional about his or her career progression, but certainly much more is needed. The broad range of competencies cyber intelligence entails opens for these professionals a myriad of possible career paths that can be rewarding and allow him or her to contribute meaningfully to an organization's cyber defense mission.

The development of prototypical career paths, which can be guided by the CBK and competency-based framework (and curriculum models derived from it), as well as the NCW Framework, would indicate a key maturation of the discipline. A career path is simply a trajectory or progression one follows over the course of employment in a particular field. Career "pathing" can be done formally or informally, though detailed career paths typically include five areas⁴⁰: sequential list of positions or roles; qualifications; critical developmental experiences; competencies that are accrued, strengthened, or required; and important career success factors. Some organizations, most notably the Intelligence Community and the contractors that support them – the 'tip of the spear' when it comes to cyber intelligence – have already begun this process to best utilize and retain trained personnel.

Certainly, cyber intelligence has many characteristics of an emerging profession. Two recent studies have examined these issues as they pertain to the field of cybersecurity. In 2012, the National Initiative for Cybersecurity Education (NICE) examined the current best practices for implementing professionalization and concluded that available evidence supported a staged model for the emergence/development of a new profession⁴¹:

- **Stage 1:** Full time occupation identified
- **Stage 2:** Formal training and educational programs provided
- **Stage 3:** Professional association established
- **Stage 4:** Code of ethics established
- **Stage 5:** Support of law provided

In 2012 and early 2013, the U.S. National Research Council formed the Committee on Professionalizing the Nation's Cybersecurity Workforce⁴². The committee concluded, "[c]ybersecurity is a broad field, and professionalization is something that can be undertaken for specific occupations within the field and not the field as a whole." The committee believed that a specific cybersecurity occupation should have well-defined characteristics (e.g., stable KSAs, designated roles and responsibilities, defined career paths and ethical standards) before any actions were taken toward professionalization. Judged by these benchmarks – a capability maturity model of sorts – cyber intelligence is well along this path, but not yet there. In fact, many of the hallmarks of professionalization coincide with the achievement of a more developed training and education framework, including:

- availability of initial certificate, undergraduate or graduate educational programs;
- skill development, to include apprenticeships, internships, and/or residency programs;
- professional credentialing, with or without formal education or training;
- professional associations; and
- agreed-upon ethical standards (particularly critical given the access given, and trust placed, in the cybersecurity professional).

RECOMMENDATIONS

To help cyber intelligence arrive at these hallmarks of professionalization, the following are proposed to help shape the discipline for the future:

1. A Common Body of Knowledge (CBK) should be developed and validated for the field of cyber intelligence to establish a shared framework of terminology, domains of knowledge, and first principles of practice, so that professionals in the field can communicate with each other and advance knowledge based on a shared understanding, and so educational institutions can teach them. This should include domains of knowledge, the importance of each knowledge element, and the level of knowledge that is necessary for entry-level proficiency. The competency clusters outlined in this paper offer a good start in this regard.
2. Based on that validated CBK, a curriculum framework should be developed for cyber intelligence education. This effort could perhaps be led by NIST as a corollary to its NCW Framework or by NSA and DHS as part of the CAE IA/CD program. Certainly, the incorporation of cyber intelligence explicitly as an 18th focus area within the CAE IA/CD program, as well as optional knowledge units addressing analytic competencies and informatics competencies, would heighten recognition of the discipline and foster the development of specialized cyber intelligence training at colleges and universities across the country.
3. Further, the dual-track (technical-analytic and analytic-technical) and integrated models for cyber intelligence education and training should be refined, further developed, and used to design new programs and learning outcomes. Additional attention will need to be given to roles, skills, preparation, and standards within each track, and how they articulate with the cyber intelligence CBK. Walker⁴³ and Smith and Tillman's⁴⁴ core curriculum concepts provide a starting point:
 - **Content:** Content comprises the topics and themes for instruction. (What should be taught?)
 - **Scope/Purpose:** Scope concerns the question of content coverage and type and ideally corresponds to the level of mastery that a course is intended to develop. (How much should students know?)
 - **Organization:** Curricular organization pertains to how the content is clustered and sequenced at the course and program levels. (How is the content organized for delivery?)

CONCLUSION

Cyber intelligence, though essential to an organization's cyber defense mission, is remarkably underdeveloped as an academic discipline and profession. While several coinciding efforts have sought to establish educational standards and workforce competencies for other cybersecurity professions, less attention has been paid to the knowledge and skills required to prepare individuals and teams to perform cyber intelligence, which requires a blend of technical expertise and classic analytic tradecraft. It is the integration of these "hard" and "soft" skill sets that fundamentally distinguishes cyber intelligence from other cyber specialty areas. By identifying five clusters of competencies – Technical, Analytic, Knowledge Management (Informatics), Contextual Domain, and Communication and Organizational – we have laid out a potential framework to help inform comprehensive and widely applicable cyber intelligence training and education curricula for higher education and workforce respecialization. From there, a professional development blueprint for cyber intelligence, including a tiered training and education program and prototypical career paths, can better emerge.

Ideally, one or more professional organizations associated with the intelligence and/or cybersecurity sectors can support and endorse this competency-based framework to facilitate broad adoption. The framework, as well as its underlying CBK, must be validated, which could be accomplished in a number of ways. A survey of cyber intelligence practitioners, educators and thought leaders to vet and validate the CBK would be an appropriate next phase. Consideration could then be given to the issue of credentialing for curricula and for cyber intelligence professionals, which would demonstrate another leap forward. With standardized training guidelines and professional credentialing, the discipline would have progressed significantly toward certification. The credential could be sponsored and managed by an existing organization with an established reputation for respected certifications in information security and cyber defense. This in itself may accelerate cyber intelligence's integration into cybersecurity and broader cyber education and practice.

The integration of cyber intelligence into cybersecurity education at all levels is indeed most appropriate and desirable. Cyber intelligence is not only a distinct discipline, but a general function for any cybersecurity or cyber defense mission. Training and education courses in cybersecurity and information assurance should explicitly address cyber intelligence in discussions of threat assessment and risk management, and encourage the use of a risk-based, intelligence-driven approach to information and network security. We believe the elements presented in this paper make such an objective not only feasible, but achievable in the near future.

APPENDIX A: OPERATIONAL LEVELS OF CYBER INTELLIGENCE

STRATEGIC CYBER INTELLIGENCE

- Produced for senior executive leadership; C-Suite and equivalent in both private and public sectors.
- Used to inform organizational/national strategy and policy development that will direct enterprise over the long term (3+ years).
- Collected broadly within sector to which organization belongs and likely includes complementary sectors.
- Focused broadly on threat vectors and adversaries and on contextual political, economic, and social trends. Includes understanding of state and non-state threat actors' interests, policies, doctrines, and concepts of operations.
- Generally nontechnical in nature, focused on trend analysis across and between sectors, stated and unstated objectives of state and non-state actors, and other strategic indicators.

OPERATIONAL CYBER INTELLIGENCE

- Produced for executive managers in IT and security such as the CIO and CISO, as well as other management team members (e.g., public affairs, human resources, legal)
- Used to inform risk-based decisions about resource allocation and activity to maintain business continuity and prevent disruption.
- Collected with an emphasis on enterprises' operations, to include partners, suppliers, competitors, customers and other trusted relationships.
- Focus on targeted, opportunistic, and persistent threat vectors that pose greatest risk to business continuity.
- Blends technical and nontechnical collection to explore and prioritize threats, the mechanisms and signatures of potential attacks, and organizational vulnerabilities.

TACTICAL CYBER INTELLIGENCE

- Produced for incident response teams.
- Used to restore operations quickly and collect cyber forensic evidence following a cyber attack or intrusion.
- Collected with internal emphasis on organization, including personnel, assets and networks.
- Focused on understanding and analyzing an adversary's use of technical/logical tactics, techniques and procedures (TTP) to target the organization.
- Generally more technical in nature (e.g., exploits and malware, delivery mechanisms, technical/logical artifacts of an attack)

ENDNOTES

- ¹Ludwick, Melissa, Jay McAllister, Andrew D. Mellinger, Kathryn Ambrose Sereno, and Troy Townsend. Cyber "Intelligence Tradecraft Project: Summary of Key Findings." Software Engineering Institute, Carnegie Mellon University, 2013.
- ²Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* (2010): 97-108.
- ³Hurley, Matthew M. *For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance*. Air Univ Maxwell AFB, AL Air Force Research Institute, 2012.
- ⁴Klimburg, Alexander (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn, 2012.
- ⁵Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States of America*. Washington, DC: Office of the Director of National Intelligence, 2014.
- ⁶Homeland Security Advisory Council. *CyberSkills Task Force Report*. Washington, DC: Department of Homeland Security, 2012, pp. 7-8.
- ⁷Chao, Han-Chieh, Sherazi Zeadally, and Gregorio Martinez. "Securing Cyberspace in the 21st Century." *Computer* 46, no. 4 (2013): 0022-23.
- ⁸Marks, Paul. "Cybersecurity guru: Hunt for the next generation of hackers." *New Scientist* 213, no. 2854 (2012): 29.
- ⁹Gavas, Efstratios, Nasir Memon, and Douglas Britton. "Winning Cybersecurity One Challenge at a Time." *Security & Privacy, IEEE* 10, no. 4 (2012): 75-79.
- ¹⁰Andreasson, Kim, ed. *Cybersecurity: Public Sector Threats and Responses*. Vol. 165. CRC Press, 2012.
- ¹¹Chabinsky, Steven R. "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line." *J. Nat'l Sec. L. & Pol'y* 4 (2010): 27.
- ¹²Stevens, Tim. "Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World." *Contemporary Security Policy* 34, no. 1 (2013): 254-256.
- ¹³Ludwick, Melissa, Troy Townsend, Joan P. Downing (September, 2013). *White Paper – CITP Training and Education*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh: PA. p. 11.
- ¹⁴The following schools are known to offer a course in "Cyber Intelligence": American Military University, California State University at San Bernardino, Eastern Michigan University (undergraduate), George Washington University, James Madison University (undergraduate), Mercyhurst University, and National Intelligence University. The University of South Florida offers a Graduate Certificate in Cyber Intelligence and formal Cyber Intelligence concentrations in both the MS in Cybersecurity and the MS in Intelligence Studies, and Utica College offers an MS in Cybersecurity with an Intelligence Concentration. At least two schools have programs that link—but not necessarily integrate—cybersecurity and intelligence studies: University of Detroit Mercy has a five year combined program to receive a bachelor's degree in information systems and a master's degree in intelligence analysis, but they are distinct degree programs. Embry-Riddle Aeronautical University offers a Bachelor of Science in Cyber Intelligence and Security that combines cybersecurity and intelligence-related coursework, but not a course in cyber intelligence specifically.
- ¹⁵Bandara, Wasana, Paul Hamon, and Michael Rosemann. "Professionalizing Business Process Management: Towards a Body of Knowledge for BPM." In *Business Process Management Workshops*, pp. 759-774. Springer Berlin Heidelberg, 2011, 760.
- ¹⁶Becker, R.E., Montgomery, L.E.: *A profession defined: Association management's body of knowledge*. *Association Management* 47, 221 (1995).
- ¹⁷Abdolmohammadi, Mohammad J., Priscilla Burnaby, and Susan Hass. "A review of prior common body of knowledge (CBOK) studies in internal auditing and an overview of the global CBOK 2006." *Managerial Auditing Journal* 21.8 (2006): 811-821.
- ¹⁸Bandara, Wasana, Paul Hamon, and Michael Rosemann. "Professionalizing Business Process Management: Towards a Common Body of Knowledge for BPM." *8th International Conference on Business Process Management*. 2010.
- ¹⁹Beckers, Kristian, and Maritta Heisel. "A Usability Evaluation of the NESSoS Common Body of Knowledge." *Availability, Reliability and Security (ARES)*, 2013 Eighth International Conference on. IEEE, 2013.
- ²⁰Bishop, Matt, and Sophie Engle. "The software assurance CBK and university curricula." *Proceedings of the 10th Colloquium for Information Systems Security Education*. 2006.
- ²¹Burnaby, Priscilla, and Susan Hass. "A summary of the global Common Body of Knowledge 2006 (CBOK) study in internal auditing." *Managerial Auditing Journal* 24.9 (2009): 813-834.
- ²²Crowley, Ed. "Information system security curricula development." *Proceedings of the 4th conference on Information Technology Curriculum*. ACM, 2003.
- ²³Knapp, Kenneth J., et al. "The Common Body of Knowledge: A Framework to Promote Relevant Information Security Research." *Journal of Digital Forensics, Security, and Law* 2.1 (2007): 9-34.
- ²⁴Pearson, Thomas D. "Education for Professionalism: A Common Body of Knowledge for Appraisers." *Appraisal Journal* 57.1 (1989).
- ²⁵Roy, Robert H., and James H. MacNeill. *Horizons for a profession: The common body of knowledge for certified public accountants*. American Institute of Certified Public Accountants, 1967.
- ²⁶Shoemaker, Daniel, et al. "A Comparison of the Software Assurance Common Body of Knowledge to Common Curricular Standards." *Software Engineering Education & Training*, 2007. CSEET'07. 20th Conference on. IEEE, 2007.
- ²⁷Theoharidou, Marianthi, and Dimitris Gritzalis. "Common body of knowledge for information security." *Security & Privacy, IEEE* 5.2 (2007): 64-67.
- ²⁸E.O. 13636 was issued on February 12, 2013, and established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."
- ²⁹See: *Interactive National Cybersecurity Workforce Framework* at <http://niccs.us-cert.gov/training/tc/framework/overview>
- ³⁰The Framework is meant to define professional requirements in cybersecurity, much as other professions, such as medicine and law, have done. See: <http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework>
- ³¹See Note 29
- ³²See Note 11
- ³³Marrin, Stephen. 2011. *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. New York, N.Y.: Routledge.
- ³⁴Breckenridge, James G. "Designing effective teaching and learning environments for a new generation of analysts." *International Journal of Intelligence and Counterintelligence* 23.2 (2010): 307-323.
- ³⁵Moore, David T. *Critical thinking and intelligence analysis*. No. 14. Government Printing Office, 2010.
- ³⁶Treverton, Gregory F., and C. Bryan Gabbard. *Assessing the tradecraft of intelligence analysis*. Rand Corporation, 2008.
- ³⁷The term "informatics" is used broadly here to refer to the study and practice of applying data, information and knowledge to improve problem solving and decision making.
- ³⁸Hutchins, Susan G., Peter L. Pirolli, and Stuart K. Card. *A new perspective on use of the critical decision method with intelligence analysts*. Naval Postgraduate School Monterey CA Dept of Information Sciences, 2004.
- ³⁹Wulf, William. *The Urgency of Engineering Education Re- form*, Excerpts from the LITEE 2002 distinguished Lecture, Auburn University, AL March 22, 2002 in *Journal of SMET Education*, July-December 2002.
- ⁴⁰Carter, Gary W., Kevin W. Cook, and David W. Dorsey. *Career paths: charting courses to success for organizations and their employees*. Vol. 32. Wiley, 2011.
- ⁴¹National Initiative For Cybersecurity Education (September, 2012). *Best Practices For Implementing Professionalization*. White Paper, Draft Version 1.0, Washington, DC: National Initiative For Cybersecurity Education.
- ⁴²National Research Council. *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. Washington, DC: The National Academies Press, 2013. Note that one of this paper's co-authors was a member of that Panel.
- ⁴³Smith, Patricia L., and Tillman J. Ragan. *Instructional design*. Upper Saddle River, New Jersey: Merrill, 1999.
- ⁴⁴Walker, D.F. *Fundamentals of Curriculum*. Harcourt Brace Jovanovich, 1990. Concepts described in Marsh, note 35.

ABOUT THE INSA CYBER INTELLIGENCE TASK FORCE

The INSA Cyber Intelligence Task Force consists of individuals from government, the private sector and academia with an interest in promoting the discipline of cyber intelligence as an emerging yet essential component of cybersecurity practices. The Task Force is chaired by John Felker, director of operations for the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security and Geoff Hancock, CEO of Advanced Cybersecurity Group. Since 2011, the Task Force has published white papers on the strategic, operational and tactical value of cyber intelligence to organizations from the public, private, nonprofit and academic sectors.

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions. As a nonprofit, nonpartisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities. INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.



INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

BUILDING A STRONGER INTELLIGENCE COMMUNITY
901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org