An Exploratory Analysis on Cybersecurity Ecosystem using NICE Framework

Information Technology and Decision Sciences

November 8, 2018

Dan J. Kim, Ph.D.

University of North Texas

Introduction

- Cybersecurity has become the biggest fear for many company chiefs, eclipsing regulation and the economy (Cowley 2018)

- Estimated more than 1.5 million unfilled positions by 2020 for Cybersecurity in U.S. (Zadelhoff 2017)

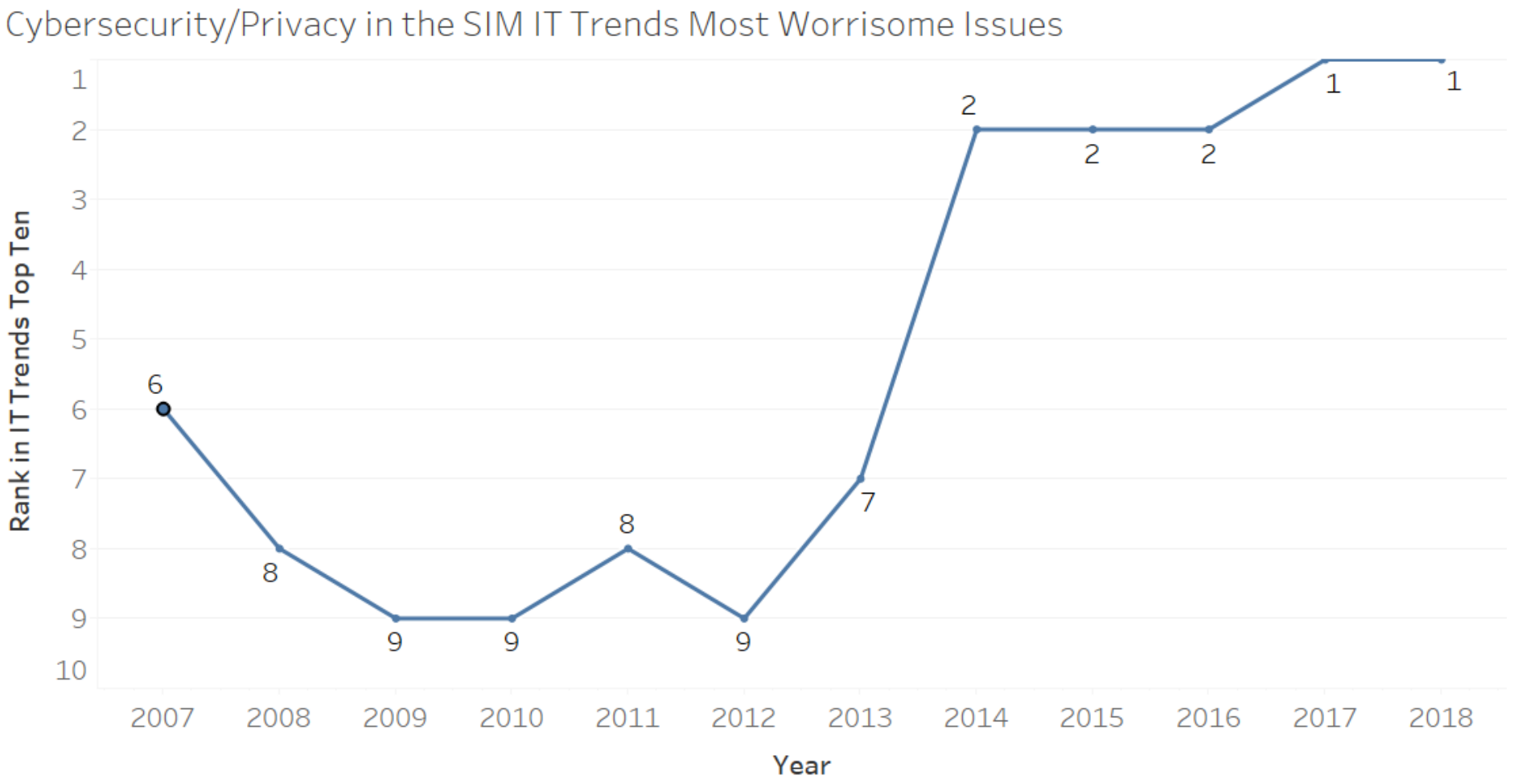
Table 3: Top-Ten Personal and Organizational IT Management Issues, 2017

IT Management Issues	Most Important to their Organizations *(2016 Rank)*	Most Important or Worrisome to IT Leaders *(2016 Rank)*
Security/Cybersecurity/Privacy	**1** *(2)*	**1** *(1)*
Alignment of IT and/with the Business	**2** *(1)*	**4** *(3)*
Data Analytics/Data Management	**3** (a)	**7** (a)
Compliance and Regulations (e.g., HIPAA, SarBox, SAS70, PCI, etc.)	**4** *(12)*	**5** *(11)*
Cost Reduction/Cost Controls (IT)	**5** *(6)*	**20** *(13)*
Cost Reduction/Cost Controls (Business)	**6** *(7)*	**39** *(36)*
Innovation	**7** *(3)*	**10** *(7)*
Digital Transformation	**8** (a)	**19** (a)
Agility/Flexibility (Business)	**9** *(5)*	**27** *(22)*
Agility/Flexibility (IT)	**10** *(4)*	**6** *(8)*
Credibility of IT/Perception of IT Leadership	**21** *(19)*	**2** *(4)*
IT Talent/Skill Shortage/Retention	**17** *(15)*	**3** *(2)*
Business Continuity	**18** *(11)*	**8** *(5)*
Improving IT Communications and Relationships with the Business	**20** *(18)*	**9** *(10)*

(a) Item introduced this year.

n = most senior IT leader in 769 unique organizations

Most Worrisome IT Issue



UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

Table 6: Top-Ten Most Difficult to Find and Most Important Technical Skills, 2017

Technical Skill or Capability	Percentage Selecting	
	Most Difficult to Find *(% Selecting)*	Most Important to Organization *(% Selecting)*
Security / Cybersecurity	**1** *(52.2%)*	**1** *(50.6%)*
Analytics / Business Intelligence / Big Data / Data Scientist	**2** *(41.7%)*	**2** *(36.0%)*
Analyst --- Business (a)	**3** *(23.3%)*	**3** *(31.0%)*
Functional Area Knowledge	**4** *(20.9%)*	**4** *(21.6%)*
Architecture / Architect --- Application / Solution (b)	**5** *(18.0%)*	**5** *(19.9%)*
Cloud	**6** *(17.4%)*	**8** *(19.1%)*
ERP (Enterprise resource planning)	**7** *(16.9%)*	**5** *(19.9%)*
Architecture / Architect --- Data / Information (c)	**8** *(15.9%)*	**10** *(15.3%)*
Architecture / Architect --- Enterprise (d)	**9** *(15.3%)*	**13** *(11.7%)*
Software Packages / COTS (e.g., ERP, CRM, DBMS, etc.) (e)	**10** *(13.8%)*	**11** *(14.0%)*
Agile Software Development	**11** *(12.6%)*	**9** *(15.6%)*
IT Project Manager	**12** *(12.2%)*	**5** *(19.9%)*

(a) New item added in 2017. However, "Business Analysis" appeared on the list of soft skills in 2015 and was 4th on most difficult to find and 3rd on most important.

(b) In 2015, "Architecture / Architect --- Application /Solution" was "Application / Solution Architecture."

(c) In 2015, "Architecture / Architect --- Data / Information" was "Data / Information Architecture."

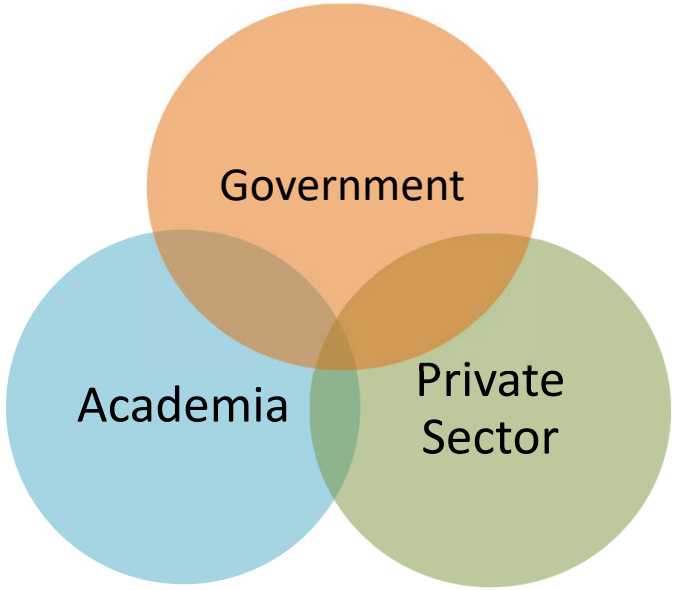
(d) In 2015, "Architecture / Architect --- Enterprise" was "Enterprise Architect."

(e) New item added in 2017.

n = most senior IT leader in 769 unique organizations

Issues and Initiatives

- Lack of skills and knowledge has been identified as the biggest barrier to successfully implement cyber defense.
- Substantial initiatives to increase Cybersecurity workforce in:
  - Government
  - Academia
  - Private Sector



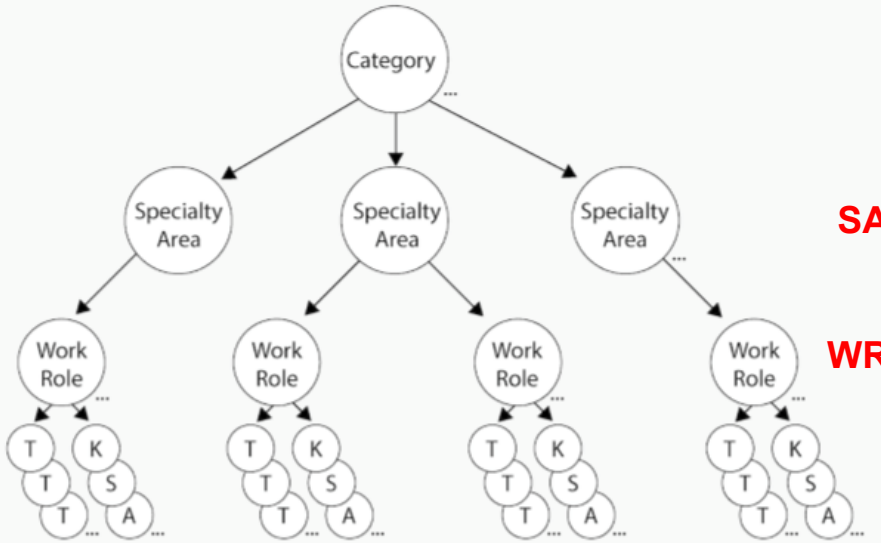
NICE Cybersecurity Workforce Framework

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role



C7

SA33

WR52

T1007 / K0630 / S0374 / A176

TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

CAE-CD 2019 Knowledge Units

Foundational CDE Knowledge Units

3

- Cybersecurity Foundations (CSF)
- Cybersecurity Principles (CSP)
- IT Systems Components (ISC)

Core Technical CDE Knowledge Units

5

- Basic Cryptography (BCY)
- Basic Networking (BNW)
- Basic Scripting and Programming (BSP)
- Network Defense (NDF)
- Operating Systems Concepts (OSC)

Core Non-Technical CDE Knowledge Units

5

- Cyber Threats (CTH)
- Cybersecurity Planning and Management (CPM)
- Policy, Legal, Ethics, and Compliance (PLE)
- Security Program Management (SPM)
- Security Risk Analysis (SRA)

Optional Knowledge Units

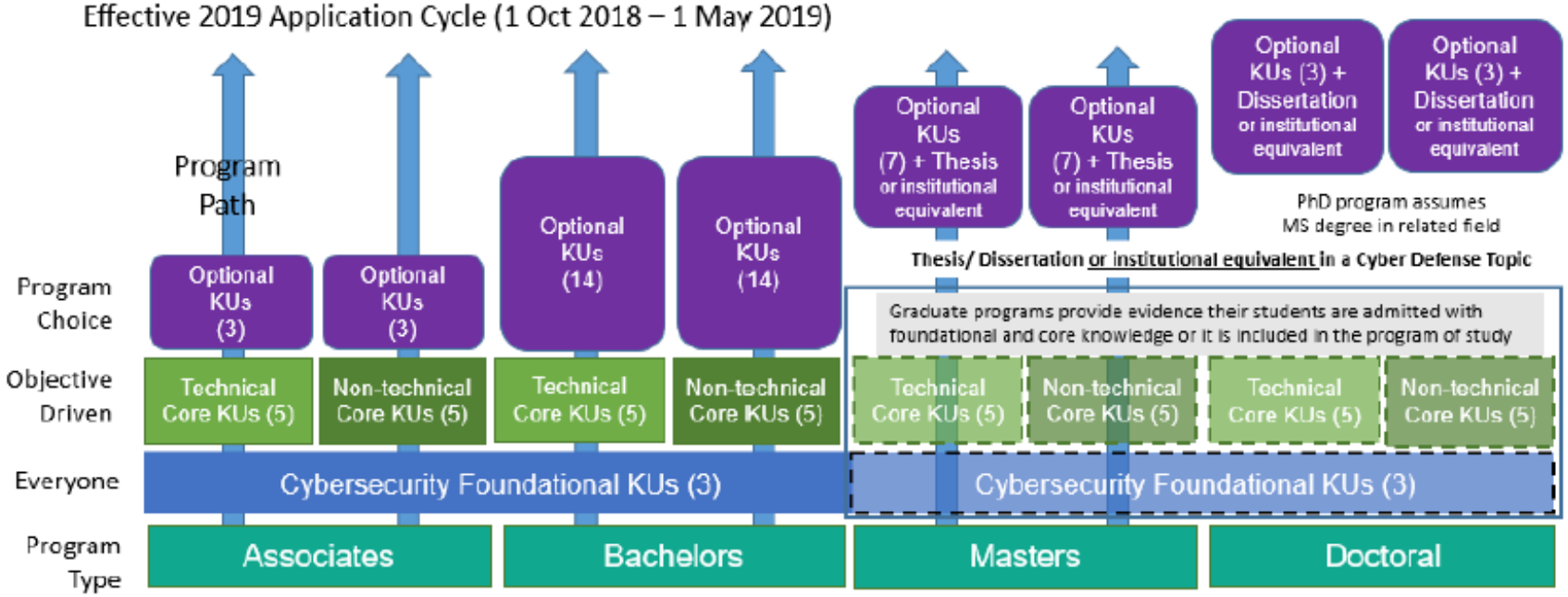
57

- Advanced Algorithms (AAL)
- Advanced Cryptography (ACR)
- Protocols (ANT)
- Algorithms (ALG)
- Analog Telecommunications (ATC)
- Basic Cyber Operations (BCO)
- Cloud Computing (CCO)
- Cyber Crime (CCR)
- Cybersecurity Ethics (CSE)
- Data Administration (DBA)
- Data Structures (DST)
- Database Management Systems (DMS)
- Databases (DAT)
- Device Forensics (DVF)
- Digital Communications (DCO)
- Digital Forensics (DFS)
- Embedded Systems (EBS)
- Forensic Accounting (FAC)
- Formal Methods (FMD)
- Fraud Prevention and Management (FPM)
- Hardware Reverse Engineering (HRE)
- Hardware/Firmware Security (HFS)
- Host Forensics (HOF)
- IA Architectures (IAA)
- IA Compliance (IAC)
- IA Standards (IAS)
- (IDR)
- Industrial Control Systems (ICS)
- Introduction to Theory of Computation (ITC)
- (IDS)
- Life-Cycle Security (LCS)
- Linux System Administration (LSA)
- Low Level Programming (LLP)
- Media Forensics (MEF)
- Mobile Technologies (MOT)
- Network Forensics (NWF)
- Network Security Administration (NSA)
- Network Technology and Protocols (NTP)
- Operating Systems Administration (OSA)
- Operating Systems Hardening (OSH)
- Operating Systems Theory (OST)
- Penetration Testing (PTT)
- Privacy (PRI)
- QA/Functional Testing (QAT)
- Radio Frequency Principles (RFP)
- Secure Programming Practices (SPP)
- Software Assurance (SAS)
- Software Reverse Engineering (SRE)
- Software Security Analysis (SSA)
- Supply Chain Security (SCS)
- Systems Certification and Accreditation (SCA)
- Systems Programming (SPG)
- Systems Security Engineering (SSE)
- Virtualization Technologies (VTT)
- Vulnerability Analysis (VLA)
- Web Application Security (WAS)
- Windows System Administration (WSA)
- Wireless Sensor Networks (WSN)

CAE-CDE Designation Requirements

Knowledge Unit Usage Notional Structure

Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) Designation Requirements,
Effective 2019 Application Cycle (1 Oct 2018 – 1 May 2019)



Knowledge Units (KUs):

Foundational: Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components

Technical Core: Basic Scripting and Programming; Basic Networking; Network Defense; Basic Cryptography; Operating Systems Concepts

Nontechnical Core: Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; Cybersecurity Planning and Management

SANS and GIAC Certifications in alignment with the **NICE Cyber Security Work Role Framework**
NIST Special Publication 800-181

SANS | GIAC
DEEPER KNOWLEDGE. ADVANCED SECURITY.

NICE Category: Highest Level Grouping

Specialty Area: Distinct areas of cyber security work

Work Role: Grouping level that maps to specific KSAs (Knowledge, Skills, and Abilities) and tasks within a specific job role. Dependent on size and type of organization, these work roles may go by different names.

SANS Training Course	GIAC Certification	Work Role Proficiency
Recommended SANS Course	Associated Recommended GIAC Certification	Level of Proficiency 1, 2, 3, 4
Recommended SANS Course	Associated Recommended GIAC Certification	Level of Proficiency 1, 2, 3, 4
Recommended SANS Course	Associated Recommended GIAC Certification	Level of Proficiency 1, 2, 3, 4

Other Mapped SANS Training and GIAC Certifications:
These courses and certifications map to the Specialty Area and Work Role but are not the top recommended courses and certifications.

https://www.giac.org/certifications/niceframework#using

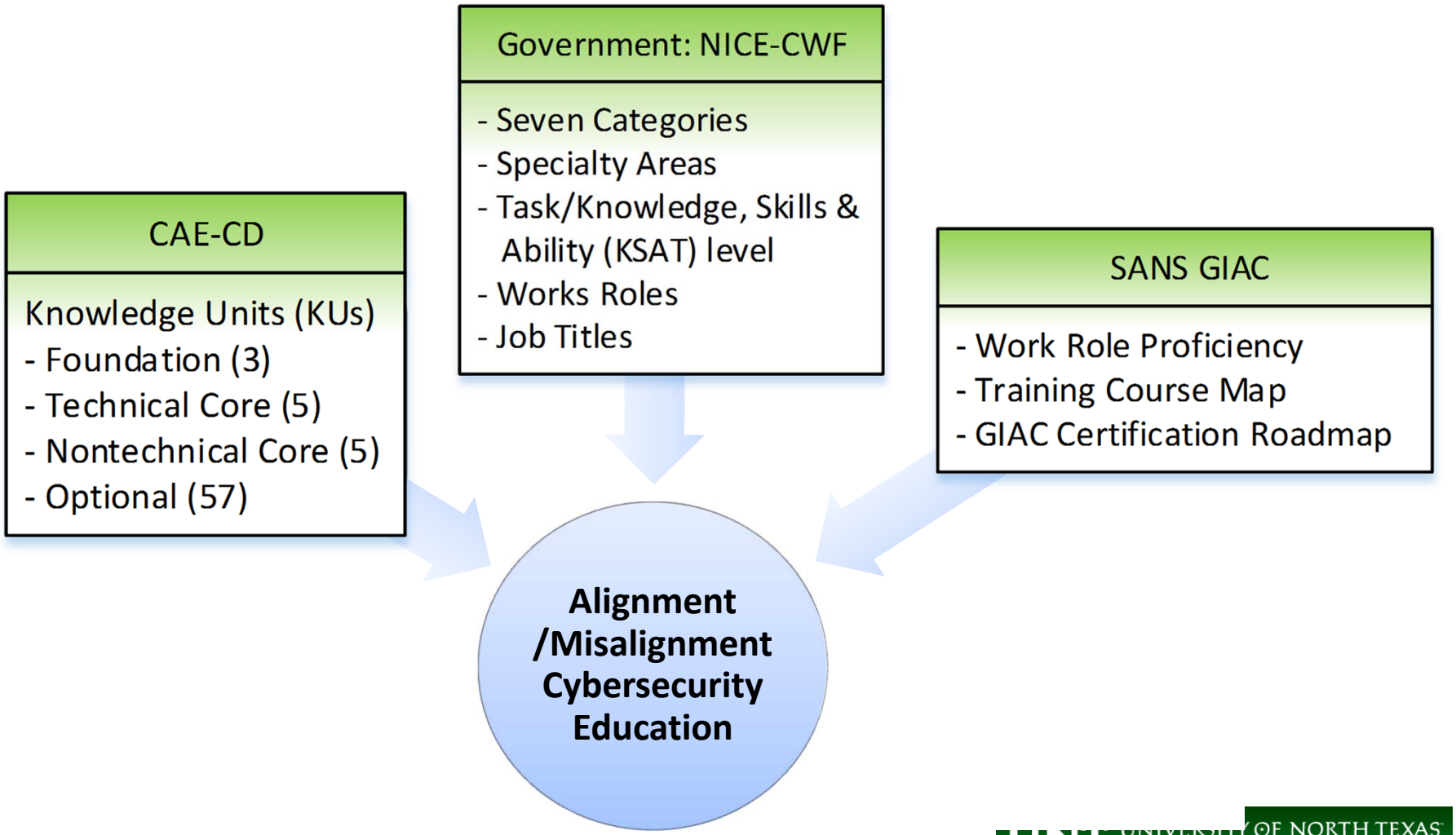
Some Issues

- Lack of transparency
  - No common language
  - Mismatch
  - Redundancy
  - Accountability
- No previous studies investigate these alignment/misalignment issues

Research Objective

- To investigate the alignment/misalignment issue within the cybersecurity ecosystem by
  - creating a knowledge alignment mapping framework
  - establishing inter-relationships using KSAT as mapping elements
- To serve our nation's cybersecurity workforce needs and to strengthen readiness

Knowledge Alignment Mapping Framework of Cybersecurity Education



Methodology

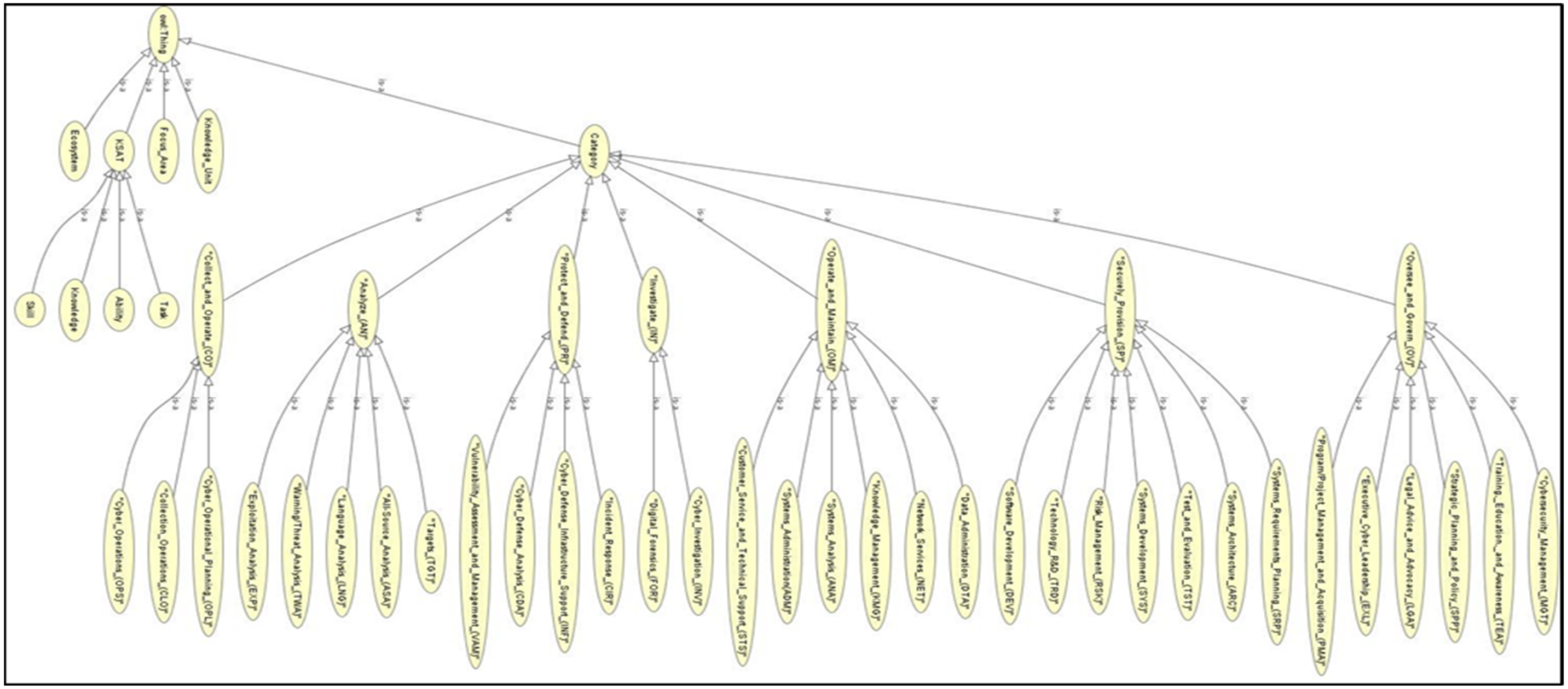
- Data Collection
  - Secondary Data
    - NICE Framework
    - CAE-CD KUs
    - SANS GIAC
  - Rationale
    - Commonly established set of taxonomy
    - Established guidelines from experts within their respective domains
    - Eliminates subjective interpretation

Methodology (Cont.)

- Ontological Network Analysis
  - Integrate pre-existing ontologies
  - Populate with preexisting data from various sources

- Ontology - modeling tool that organizes the concept at the level of knowledge and semantics, therefore domain ontology is often used to organize important entities, attributes, process and their relationship properly and effectively

Ontological Network Analysis



UNT UNIVERSITY OF NORTH TEXAS
Discover the power of ideas.

An Example of Analysis Results

Work Role	Knowledge (% out of 599)	Skill (% out of 370)	Ability (% out of 175)	Task (% out of 1003)	Cross Comparison
Authorizing Official	6.5%	0.5%	6.3%	0.4%	92.8%
Security Control Assessor	8.7%	18.4%	27.4%	2.1%	27.5%

	AN	CO	IN	OM	OV	PR	SP	Total
Advanced Network Tech & Protocol	5	7	6	39	17	15	22	58
Advanced Cryptography	2	3	2	27	3	6	9	33
Algorithms	0	1	2	14	0	2	6	16
Analog Telecommunications	3	4	1	26	9	10	13	36
Basic Data Analysis	1	3	4	28	2	1	4	32
Basic Scripting - Intro Program	2	4	7	17	5	6	15	31
Cloud Computing	6	5	3	45	24	18	31	74
Cyber Defense	10	13	40	52	43	68	58	158
KU Total	24	28	62	146	105	95	154	361
NICE Total	397	473	153	338	465	205	507	1990
Alignment	6%	6%	41%	43%	23%	46%	30%	18%

Expected Contributions

- Colleges and training vendors can create programs aligned to jobs.
- Students will graduate with knowledge and skills that employers need.
- It will be used as baseline sets for additional mapping studies for cybersecurity workforce and certifications
- It will be an important tool in building and maintaining an properly skilled workforce