Ph.D. in Cyber Operations Self-study Report

Mar 27, 2023

The Beacom College of Computer and Cyber Sciences

Contents

Part 1. Institutional History

1.1. Heritage: 1881 to 1982

Dakota State University (DSU) was established in 1881 as the first teacher education institution in Dakota Territory. Teacher education remained the primary mission of the institution through the 1950s. However, in response to the changing needs of South Dakota in the 1960s, the university began to expand its role to include degree programs in the liberal arts and business. In 1980, South Dakota welcomed a major new industry into the state: the banking and credit card industry. The success and growth of this new industry, as well as the success of other information oriented, computer-based industries in the state, prompted the states leadership to carefully examine the degree programs being offered at the public institutions of higher education within the state. After lengthy discussions, leaders in state government, the banking and information services industries, and the Board of Regents agreed to develop new degree programs at one institution and then to use the experience and knowledge from this development to expand programs throughout the state's public higher education system.

1.2. Mission Change: 1983 to 1984

In 1984, the Legislature of the State of South Dakota (South Dakota Codified Law §13-59-2.2) assigned Dakota State University the role and mission of developing technology-based degree programs in information systems, business, teacher education, and allied health care services at both the undergraduate and graduate levels.

The Legislature provided $2.6 million in additional operating funds to support a three-year mission change at DSU. During the initial phase of the transition, the academic programs of the institution were reviewed. Degree programs were phased out if they were duplicated at the other five regental institutions or if graduates would enter an over-supplied marketplace. New information systems programs, computer equipment, and facilities were approved for DSU. During the transition, special attention was given to ensure that all students in programs slated for phase out received a full opportunity to complete those programs. To ensure the continuation of education quality, when the number of students continuing in a program became very small, a special faculty mentoring program was developed.

The second phase of the transition began in August 1984, with the development of degree programs that integrated computers and information technologies into traditional academic subjects and added coursework specific to the computer and information systems areas. Existing faculty were retrained, and new faculty were hired. Programs to implement the research and service aspects of the new role and mission were started. This was a period of stress for the campus, but it was also a period of great exhilaration with faculty and staff invigorated and renewed by the need for innovation, adaptation, and change. Some faculty and staff were unable to adapt to the changing conditions and left the university, but those who stayed on for the ride were justly proud of their accomplishments.

Realizing that the innovative programs being developed at DSU were expensive, private industry and state government provided the university with additional financial resources. Consultants from state agencies and from national corporations also provided assistance and guidance that contributed greatly to the success of the mission change, amplifying the Mission Change: 1984 to Present.

There are three mission statements that direct DSU according to South Dakota Codified Law §13-59-2.2, South Dakota Board of Regents, and Dakota Student University.

1.2.1. Mission Statement by South Dakota Codified Law §13-59-2.2

The primary purpose of Dakota State University at Madison in Lake County is to provide instruction in computer management, computer information systems, electronic data processing, and other related

undergraduate and graduate programs. The secondary purpose is to offer two-year, one-year and short courses for application and operator training in the areas authorized by this section.

This authorization includes the preparation of elementary and secondary teachers with emphasis in computer and information processing.

Except for degree programs in existence during the 1983-84 academic year, the unique baccalaureate programs authorized for Dakota State University shall not be duplicated by the Board of Regents.

1.2.2. Mission Statement by South Dakota Board of Regents, Policy 1:10:5

The South Dakota Board of Regents regards the special focus universities of South Dakota as valuable contributors to the state's system of higher education. Special focus universities have a high concentration of degrees in a single field or set of related fields. Special focus universities offer master's and doctoral programs within their special focus area.

Universities operating within this sector are nationally recognized to promote research activities of their faculty, staff, and students. Dakota State University's research is propelling the workforce, economy, and student experience. The Board of Regents recognizes that special focus universities have unique characteristics and are critical to the success of the South Dakota system of higher education.

Students who attend Dakota State University pursue highly technical degrees with a broad focus in current and emerging computing and information technologies/cyber security that emphasize innovation, leadership, application, and research. DSU has the authority to credential certificates, associate degrees, baccalaureate degrees, master's degrees and doctoral degrees provided formal approval by the Board of Regents. The Board of Regents may authorize academic programs outside of the statutory mission as identified by the Regents due to workforce needs, strategic needs of the state, etc. All program requests must comply with BOR Policy 2:23 and 2:23:1.

1.2.3. DSU Institution Mission, Vision, & Values

DSU's mission is to prepare cyber-savvy graduates who are lifelong learners, problem solvers, innovators, and leaders to live lives of positive purpose and consequence.

Vision

Innovative, entrepreneurial, and resilient since 1881, DSU will continue to rise through short - and long-term success of our students and graduates, increased strength in applied research and athletics, and deep engagement with our stakeholders, in an environment infused with quality improvement.

Values

- Distinguished and effective teaching
- Integrity
- Clear communication
- Innovation
- Inclusion
- Quality

1.2.4. Strategic Plan *DSU ADVANCE 2027*

Dakota State University's strategic plan begins with its mission, vision, and values. These build a framework for the university goals. The strategic plan is built on our strengths and focuses our attention and commitment on the most pressing issues we are distinctively positioned to address. As an important

initiative, DSU continuously seeks to advance student success through highly engaged, high-impact educational practices.

The current Strategic Plan *DSU ADVANCE 2027*[1] is built on the previous "Excellent Through Innovation Strategic plan" in 2022 and will continue to evolve through 2027 and beyond. The Strategic Plan outline a path to more direct scholarship, research, intellectual property and economic development through solutions to all varieties of cyber threats to computing and information devices, networks and their users. Foundational goals defined in the Strategic Plan include:

- Ensure Financial Stability
- Strengthen Regional and National Relevance
- Enhance Ability to Recruit and Retain Talent
- Increase Student Enrollment
- Enhance Student Success
- Maintain Higher Learning Commission Accreditation
- Ensure Responsible Stewardship of State Resources
- Strengthen Risk Management Process

Five Pillars are identified in the Strategic Plan. These five Pillars include:

- Pillar 1: Increase Student Success
- Pillar 2: Improve Engagement, Governance, & Communication
- Pillar 3: Grow Scholarship, Research, Intellectual Property, & Economic Development
- Pillar 4: Elevate Athletics
- Pillar 5: Increase Sustainability & Resilience

Goals and milestones are further defined for each Pillar.

Mission and strategic plan alignment gave DSU its first graduate degree programs when we received authority from the South Dakota Board of Regents to offer a Master of Science degree in Information Systems (1998). A year later the Master program in Educational Technology was offered on our campus (1999). In 2004, DSU received authorization for its first doctoral program, offered in Information Systems. At the April 2014 Board meeting, DSU received authority to offer the D.Sc. in Cyber Security. On May 11, 2018, a request for transition from the existing Doctor of Science (DSc) degree program in Cyber Security to a new degree along with a name change from "Cyber Security" to "Cyber Operations" was submitted to the South Dakota Board of Regents. The South Dakota Board of Regents approved the request on May 23, 2018. DSU now offers four doctoral degrees, seven master's degrees, and ten graduate certificates. As the institution endeavors to articulate its mission in the fullest way, our degree programs are scrutinized each year to ensure they remain on the cutting edge relative to technology to enhance and support instruction and address work force demands.

DSU currently holds three prestigious designations from the National Security Agency (NSA) and the Department of Homeland Security (DHS) as National Centers of Academic Excellence (CAE) in Cyber Defense, Research, and Cyber Operations. DSU received its first CAE distinction in Information Assurance Education in 2004, one of 50 programs recognized. DSU was named as a National Center of Academic Excellence in Cyber Operations (CAE-CO) in 2012, one of the first four schools to receive the CAE-CO designation for the 2012-2013 academic year. There are currently 386 institutions with a

[1] DSU ADVANCE Strategic Plan 2022-27.

designation including CAE-CD, CAE-R, and CAE-CO from the National Security Agency. There are only 22 institutions which receive CAE-CO designations.

1.3. DSU Rising Initiative

In 2017, Dakota State University began a transformational five-year capital investment initiative called DSU Rising. The initiative was the result of a $30M donation from philanthropists Miles and Lisa Beacom and Denny T. Sanford. The donation would allow for the construction of an $18M, 40,000 square foot research and development building for the Madison Cyber Labs (MadLabs). The funds also provided for additional scholarships, new program development, hiring of more faculty and staff, and support the university's intent to bring 5G network capabilities to Madison, the region, state, and eventually the nation. In addition, South Dakota Governor Dennis Daugaard pledged $10M to Dakota State, monies from the research and development Future Fund. U.S. Senator Mike Rounds (R SD) had pledged to help Dakota State earn $20M in federal funds to advance DSU's cyber mission.

DSU intends to put South Dakota on the leading edge of cyber technologies with new economic development clusters creating high paying jobs and giving former students the ability to 'come home' to cutting edge companies and a growing regional economy. In 2021, Dakota State university and Sanford Health of Sioux Falls, SD have announced a CyberHealth Strategic Alliance between the two organizations that will drive cyberhealth innovation and research and create workforce and economic development opportunities for South Dakota.

1.4. DSU Rising II

The DSU Rising II project (2022) created a funding consortium to provide $90 Million to fund new components to the cyber research and education environment: a 100,000 square feet facility to house the expanded DSU Applied Research Lab in Sioux Falls, S.D., the support required to double the DSU cyber graduates, authority to expand DSU ARL Management and Security, to expand merit based Student Scholarships in cyber education, and to launch the Governor's Cyber Academy (a statewide K-12 cyber education program).

1.5. Student Demographics

Prior to the mission change in 1984 and like most state funded institutions, the majority of DSU students lived within a 50-mile radius of the campus. Most were traditional students coming to the institution directly from high school. Since the mission change, the DSU audience and student population has changed markedly. Immediately after the mission change, enrollment plunged a frightening 27.6 percent the first year, followed by another 12.6 percent decline the second year. But the new curriculum changes, combined with new institutional vigor, provided the institution with unprecedented enrollment growth and stability. The total headcount for Fall 2022 is 3,241, up one percent from 3,219 in Fall 2021, which was an increase from the Fall 2020 number of 3,186. The number of graduate students for Fall 2022 is 484, up 3.42% from Fall 2021. This number has seen steady and significant growth over the last 10 years.

1.6. Computing Environment

Students at DSU enjoy unique access to technology. DSU was not only the first institution in the region to provide 1:1 portable computing and a campus wide wireless network overlay, but one of the first in the nation to do so. In 2005 all students were provided fully functional portable computers (tablets) that included digital inking capabilities and voice to text translation. Currently, DSU are providing students with the latest Lenovo ThinkPad X1 Yoga, a 2-in-1 Laptop configured specifically for DSU academic programs. Similar computing tools allows for common computer imaging and software licenses used in classes. However, students may join the ubiquitous computing environment with devices of their own. Computing omnipresence builds on a long tradition of supporting data communication and networking

innovations. For degree programs emphasizing information assurance and security issues as well as digital design, additional lab facilities featuring computers with high end functions have been added to the campus technology infrastructure. DSU's leadership in using technology to support student learning also extends to the online environment when Dean of Arts and Sciences Dr. Eric Johnson delivered the first Internet enabled course in 1989.

Throughout its 142 years, Dakota State University has had a proud heritage of preparing graduates to meet the needs of a changing society. Since 1881, the university has provided challenging academic programs in one of the best educational environments in the state. The continuation of this tradition of service is of prime importance to the faculty, students, staff, and administration of Dakota State University.

1.7. Accreditation History

Dakota State University was granted accreditation by the Higher Learning Commission for a period of ten years in 1961 and accreditation has been continued after each comprehensive visit. The institution's most recent comprehensive visit, in October 2018, resulted in a positive review without any requirement for monitoring reports. Currently, DSU is participating in the Higher Learning Commissions Academic Quality Improvement Program (AQIP). Six AQIP Categories provide a framework for examination. The AQIP Categories are:

- Helping Students Learn
- Meeting Student and Other Key Stakeholder Needs
- Valuing Employees
- Knowledge Management and Resource Stewardship
- Planning and Leading
- Quality Overview

Each AQIP Category deals with a related group of key processes and encourages an organization to analyze, understand, and explore opportunities for improving these processes and the interrelationships among them.

The AQIP process works in tandem with our existing strategic planning and project review processes. It provides a framework that focuses on data analysis and the achievement of its published goals and objectives. The alternate accreditation review process is every ten years. With AQIP, our accreditation is reviewed yearly in cycles and culminates in a Reaffirmation of Accreditation at the end of a seven-year cycle.

Part 2. Trends in the Discipline

2.1. National and Regional Trends

Cybersecurity is a top priority at all levels of government (The White House, 2021). Cybercrime damages cost to the world estimated at $7 trillion USD in 2022 (Cybersecurity Ventures, 2022). The global cybercrime costs are expected to grow by 15 percent per year over the next three years, reaching $10.5 trillion USD by 2025 (Steve Morgan, 2020). "The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors (The White House, 2021)." The Ph.D. in Cyber Operations program at DSU aligns with the federal government's efforts to identify, deter, protect against, deter, and respond to cyberattacks and threat actors.

According to National Initiative for Cybersecurity Careers and Studies (NICCS), cyber operations "Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or

real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities (Petersen et al., 2020)." The cyber operations program "is a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises (Cyber Operations (CAE-CO) Program, 2023)."

Table 1 shows a list of cybersecurity Ph.D. programs in the nation. As shown in Table 1, most of the cybersecurity doctoral programs fall in traditional Ph.D. in Computer Science programs. DSU's Ph.D. in Cyber Operations program is a unique and highly specialized cybersecurity program. First, the program aligns with the NSA's cybersecurity strategy priorities. Second, the program's emphasis on low level programming including malware analysis, reverse engineering, and software exploitation forms the core of the cyber operations program at DSU. Third, the rich cybersecurity curriculums available at DSU pave pathways for students with various background to develop their specialties in cyber operations.

Table 1. Cybersecurity Ph.D. Programs[2]

School	Location	Link to Program Website
Arizona State University	Tempe, Arizona	Ph.D. in Computer Science – Cybersecurity
Carnegie Mellon University	Pittsburgh, Pennsylvania	Ph.D. in ECE: Mobility Research Center
Colorado School of Mines	Golden, Colorado	Doctor of Philosophy in Computer Science – Cyber Security
Indiana University Bloomington	Bloomington, Indiana	Ph.D. in Computer Science – Minor in Security Informatics
Indiana University Bloomington	Bloomington, Indiana	Ph.D. in Informatics – Security Informatics Track
Iowa State University	Ames, Iowa	Ph.D. in Computer Engineering with a focus on Information Assurance
Iowa State University	Ames, Iowa	Ph.D. in Computer Science with a focus on Information Assurance
Iowa State University	Ames, Iowa	Ph.D. in Math with a focus on Information Assurance
Mississippi State University	Mississippi State, Mississippi	Ph.D. Computer Science – Computer Security Concentration
Naval Postgraduate School	Monterey, California	Ph.D. in Computer Science (may elect Computer Systems and Security specialization)
Northeastern University	Boston, Massachusetts	Ph.D. in Information Assurance
Purdue University	West Lafayette, Indiana	Interdisciplinary Ph.D. Program in Information Security
Purdue University	West Lafayette, Indiana	Ph.D. in CS with an Info-Security Focus
Rochester Institute of Technology	Rochester, New York	Ph.D. in Computing and Information Sciences – Computing Security Focus
Sam Houston State University	Huntsville, Texas	Ph.D. in Digital and Cyber Forensic Science
Stevens Institute of Technology	Hoboken, New Jersey	Ph.D. program in Computer Science – Computer Security
The University of Tennessee	Knoxville, Tennessee	Ph.D. in Computer Engineering – Cybersecurity
The University of Tennessee	Knoxville, Tennessee	Ph.D. in Computer Science – Cybersecurity
University of Arizona	Tucson, Arizona	Ph.D. in MIS with Emphasis in Information Assurance
University of California-Davis	Davis, California	Ph.D. in Computer Science – Information Assurance Focus
University of Colorado Colorado Springs	Colorado Springs, Colorado	Ph.D. in Engineering – Concentration in Security
University of Idaho	Moscow, Idaho	Ph.D. in Computer Science – Information Assurance
University of Illinois at Urbana-Champaign	Champaign, Illinois	Juris Doctor Degree – Illinois Cyber Security Scholars Program
University of Missouri-Columbia	Columbia, Missouri	Ph.D. in Computer Science with a Focus in Information Assurance
University of North Carolina at Charlotte	Charlotte, North Carolina	Ph.D. in Computing and Information Systems
Virginia Tech	Blacksburg, Virginia	Ph.D. in Computer Science with Cybersecurity Track
Worcester Polytechnic Institute	Worcester, Massachusetts	Ph.D. in Computer Science – Cybersecurity Focus

[2] https://cybersecurityguide.org/programs/phd-in-cybersecurity/

2.2. Curriculum Implications

The National Initiative for Cybersecurity Careers and Studies identifies the roles, tasks, knowledges, skills, and abilities for cyber operations (National Initiative for Cybersecurity Careers and Studies, 2022). Table 2 and Table 3 include mappings from our curriculum to the desired knowledge and skills in cyber operations.

Table 2. Cyber Operations Knowledge Mapping

Knowledge	Course
K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.	INFA 723 - Cryptography and Network Security CSC 773 - Mobile Computing and Advanced Network Security CSC 841 - Cyber Operations II
K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	INFA 713 - Managing Security Risks
K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	CSC 840 - Cyber Operations I
K0004: Knowledge of cybersecurity and privacy principles.	INFA 723 - Cryptography and Network Security CSC 702 - Data Privacy
K0005: Knowledge of cyber threats and vulnerabilities.	INFA 735 - Offensive Security INFA 754 - Network Security Monitoring and Intrusion Detection
K0006: Knowledge of specific operational impacts of cybersecurity lapses.	CSC 840 - Cyber Operations I CSC 841 - Cyber Operations II
K0009: Knowledge of application vulnerabilities.	CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation
K0021: Knowledge of data backup and recovery.	INFA 713 - Managing Security Risks
K0051: Knowledge of low-level computer languages (e.g., assembly languages).	CSC 428 - Reverse Engineering CSC 844 - Advanced Reverse Engineering
K0109: Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	CSC 456 - Operating Systems
K0142: Knowledge of collection management processes, capabilities, and limitations.	INFA 713 - Managing Security Risks INFA 745 - Compliance and Audit
K0224: Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	CSC 328 - Operating Environments CSC 431 - UNIX/Linux Administration CSC 456 - Operating Systems
K0363: Knowledge of auditing and logging procedures (including server-based logging).	INFA 745 - Compliance and Audit
K0372: Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages).	CSC 705 - Design and Analysis of Algorithms CSC 712 - Data Structures
K0373: Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.	CSC 234 - Software Security CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation
K0375: Knowledge of wireless applications vulnerabilities.	INFA 751 - Wireless Security CSC 841 - Cyber Operations II
K0379: Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	CSC 321 - Information Security Management
K0403: Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	INFA 723 - Cryptography and Network Security
K0406: Knowledge of current software and methodologies for active defense and system hardening.	INFA 754 - Network Security Monitoring and Intrusion Detection
K0420: Knowledge of database theory.	CIS 484 - Database Management Systems CSC 714 - Database Systems
K0423: Knowledge of deconfliction reporting to include external organization interaction.	CSC 840 - Cyber Operations I
K0427: Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	INFA 723 - Cryptography and Network Security

K0428: Knowledge of encryption algorithms and tools for wireless local area networks (WLANs).	INFA 751 - Wireless Security
K0429: Knowledge of enterprise-wide information management.	CSC 437 - Survey of Enterprise Systems
K0430: Knowledge of evasion strategies and techniques.	CSC 421 - Web Software Security CSC 436 - Offensive Network Security CSC 439 - Threat Hunting and Incident Response INFA 735 - Offensive Security
K0433: Knowledge of forensic implications of operating system structure and operations.	INFA 721 - Computer Forensics
K0438: Knowledge of Global Systems for Mobile Communications (GSM) architecture.	CSC 420 - Cellular and Mobile Communications CSC 773 - Mobile Computing and Advanced Network Security CSC 841 - Cyber Operations II
K0440: Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.	CSC 438 - Defensive Network Security INFA 754 - Network Security Monitoring and Intrusion Detection
K0452: Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.	CSC 438 - Defensive Network Security INFA 754 - Network Security Monitoring and Intrusion Detection
K0468: Knowledge of internal and external partner reporting.	INFA 733 - Vendor Management
K0480: Knowledge of malware.	INFA 732 - Malware Analysis CSC 846 - Advanced Malware Analysis
K0481: Knowledge of methods and techniques used to detect various exploitation activities.	CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation
K0485: Knowledge of network administration.	CSC 431 - UNIX/Linux Administration INFA 754 - Network Security Monitoring and Intrusion Detection
K0486: Knowledge of network construction and topology.	CSC 285 - Networking I CSC 385 - Networking II INFA 754 - Network Security Monitoring and Intrusion Detection
K0516: Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	CSC 285 - Networking I CSC 385 - Networking II
K0528: Knowledge of satellite-based communication systems.	CSC 841 - Cyber Operations II
K0530: Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.	CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation
K0531: Knowledge of security implications of software configurations.	CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation
K0536: Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).	CSC 436 - Offensive Network Security INFA 735 - Offensive Security
K0560: Knowledge of the basic structure, architecture, and design of modern communication networks.	CSC 420 - Cellular and Mobile Communications CSC 773 - Mobile Communication and Advanced Network Security
K0565: Knowledge of the common networking and routing protocols (e.g., TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	CSC 285 - Networking I CSC 385 - Networking II
K0573: Knowledge of the fundamentals of digital forensics to extract actionable intelligence.	INFA 721 - Computer Forensics
K0608: Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).	CSC 328 - Operating Environment CSC 431 - UNIX/Linux Administration
K0609: Knowledge of virtual machine technologies.	CSC 437 - Survey of Enterprise Systems

Table 3. Cyber Operations Skill Mapping

Skill	Course
S0062: Skill in analyzing memory dumps to extract information.	CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation
S0182: Skill in analyzing target communications internals and externals collected from wireless LANs.	INFA751 - Wireless Security
S0183: Skill in analyzing terminal or environment collection data.	CSC 328 - Operating Environments
S0190: Skill in assessing current tools to identify needed improvements.	CSC 842 - Security Tool Development
S0192: Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.	INFA 754 - Network Security Monitoring and Intrusion Detection
S0202: Skill in data mining techniques (e.g., searching file systems) and analysis.	CSC 840 - Cyber Operations I
S0206: Skill in determining installed patches on various operating systems and identifying patch signatures.	CSC 328 - Operating Environments
S0221: Skill in extracting information from packet captures.	CSC 285 - Networking I CSC 385 - Networking II
S0236: Skill in identifying the devices that work at each level of protocol models.	CSC 285 - Networking I CSC 385 - Networking II
S0242: Skill in interpreting vulnerability scanner results to identify vulnerabilities.	INFA 732 - Malware Analysis CSC 846 - Advanced Malware Analysis
S0243: Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).	CSC 321 - Information Security Management
S0252: Skill in processing collected data for follow-on analysis.	CSC 285 - Networking I CSC 385 - Networking II
S0255: Skill in providing real-time, actionable geolocation information utilizing target infrastructures.	CSC 436 - Offensive Network Security INFA 735 - Offensive Security
S0257: Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).	CSC 328 - Operating Environments CSC 431 - UNIX/Linux Administration
S0266: Skill in relevant programming languages (e.g., C++, Python, etc.).	CSC 150 - Computer Science I CSC 250 - Computer Science II
S0267: Skill in remote command line and Graphic User Interface (GUI) tool usage.	CSC 328 - Operating Environments
S0270: Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.	CSC 428 - Reverse Engineering CSC 844 - Advanced Reverse Engineering
S0275: Skill in server administration.	CSC 431 - UNIX/Linux Administration CSC 437 - Survey of Enterprise Systems
S0276: Skill in survey, collection, and analysis of wireless LAN metadata.	INFA 751 - Wireless Security
S0281: Skill in technical writing.	CSC 803 - An Introduction to Research CSC 804 - Computer and Cyber Security Research Methodology CSC 807 - Computer and Cyber Security Research Design and Implementation CSC 808 - Mixed Research Methods for Computer and Cyber Sciences: Design and Implementation CSC 809 - Dissertation Preparation CSC 890 - Seminar: Research
S0282: Skill in testing and evaluating tools for implementation.	CSC 842 - Security Tool Development
S0293: Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.	INFA 735 - Offensive Security CSC 748 - Software Exploitation CSC 848 - Advanced Software Exploitation

S0295: Skill in using various open source data collection tools (online trade, DNS, mail, etc.).	CSC 328 - Operating Environments
S0298: Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.).	INFA 723 - Cryptography and Network Security
S0299: Skill in wireless network target analysis, templating, and geolocation.	INFA 751 - Wireless Security CSC 841 - Cyber Operations II
S0363: Skill to analyze and assess internal and external partner reporting.	INFA 733 - Vendor Management

As shown in Table 2 and Table 3, our curriculum provides and covers all the desired knowledge and skills in cyber operations.

Part 3. Academic Programs and Curriculum

3.1. Mission Statements for the Academic Programs being Reviewed

The Ph.D. in Cyber Operations is intended to be a technical program firmly grounded in computer science and will emphasize applied research in cyber security. Students enrolled in the program will become a vital resource for DSU researchers, as well as for regional and national employers. The program aims to produce graduates with a commanding knowledge of cyber security, of the applications and research in cyber security, and of supporting technology and innovation in computer science.

The program will provide a particular emphasis on technologies and techniques related to specialized cyber operations activities, including reverse engineering, malware analysis, and software exploitation. These technologies and techniques are critical to intelligence, military, and law enforcement organizations, as well as to employers in data-intensive industries.

3.2. Academic Degrees Offered within the Academic Programs

Students in the Ph.D. in Cyber Operations program must meet the following requirements in Table 4 to receive doctoral degrees in cyber operations.

Table 4. Degree Requirements

Ph.D. in Cyber Operations	Curriculum	Credit Hours	Percent	Assessment
Credit requirement	Cyber operation core courses	15 credits	25	Letter Grade
	Research core courses	9 credits	15	Letter Grade
	Residency requirement	3 credits	4	Satisfied
	Elective courses	15 credits	25	Letter Grade
	Dissertation credits	19 credits	31	Satisfied
	Total	61 credits	100	
Oral comprehensive exam		-	-	Pass/No Pass
Proposal defense		-	-	Pass/No Pass
Dissertation defense		-	-	Pass/No Pass

3.2.1. Credit Requirement

Total 61 credits are required to meet the degree requirements. These 61 credits include 15 core course credits, 9 research course credits, 15 elective course credits, 3 residency credits, and 19 dissertation credits. The specific core courses and research courses required in the program can be found in Table 5.

Students will be required to complete three on-site research seminars (CSC 890, one credit each, taken three separate times) in a face-to-face setting at the Madison, SD campus. These research seminars will be held annually and take place over multiple days. The research seminars are intended to acquaint students with contemporary cyber security research issues, allow students to report, present, and discuss articles

pertinent to cyber security research and provide students an opportunity to meet faculty, identify a dissertation advisor, present their dissertation proposal defense, as well as completing the final dissertation defense and oral comprehensive exam.

3.2.2. Oral Comprehensive Exam

Oral comprehensive examinations will be administered to all doctoral students who are pursuing the Ph.D. in Cyber Operations degree. Sitting for the oral exams signifies that a student has completed the Cyber Operations core curriculum including CSC 840, 841, 844, 846, and 848, or is in the final semester of completing the core courses. A student must successfully pass the oral comprehensive exam in order to defend his/her dissertation proposal.

The student will meet for 1 hour with faculty of the Cyber Operations PhD program in a private Zoom setting and will be asked five (5) questions. There will be 10 minutes allocated for each question. The questions posed to the student will be derived from the curriculum covered in the following classes: CSC 840, CSC 841, CSC 844, CSC 846, and CSC 848. CSC 841 and CSC 848 are offered in spring semester. Prior to the examination date the student will have the option to not take questions for CSC 841 or CSC 848. If a student has completed all five core courses, the student is expected to take questions in all five classes.

Oral comprehensive exams are generally scheduled and available in the 2nd week and 3rd week of the spring semester each year according to DSU's academic calendar. The oral exams are conducted via Zoom virtually. In the unfortunate case that a student may not be successful with the oral exam, the student can schedule to take the oral exam again in March during the CSC 890 Residency.

3.2.3. Proposal Defense

The purpose of the dissertation proposal defense is to assure that a student's plan of researching the proposed research question is complete and holds academic merit. Students work closely with their supervisory committees in determining the composition of the dissertation proposal and in writing the proposal.

The student must work closely with the dissertation chair to develop the proposal. Communications among the candidate, the dissertation chair, and the dissertation committee are essential to ensure the process goes smoothly. The major milestones in the proposal process are listed below:

- Research and proposal: the student must work closely with the dissertation chair to conduct research and develop the dissertation proposal.
- Submit proposal for committee review: dissertation committee needs minimum 3 weeks to review the proposal.
- Proposal review and committee recommendation: after review, the dissertation committee makes recommendation if a student is ready to defend the proposal.
- Schedule proposal defense: Graduate Office needs two weeks to schedule the proposal defense and makes announcement.
- Proposal defense: dissertation proposal defense is generally hosted in person during residency week in spring.
- Proposal revision: the student may be required to revise the proposal according to the recommendations from the dissertation committee. If so, a revision of the proposal needs to submit to the dissertation committee for final approval.

The proposal must be shared with the dissertation committee at least 5 weeks (3 weeks for dissertation committee review and 2 weeks for proposal scheduling) before conducting the proposal defense.

3.2.4. Dissertation Defense

A dissertation defense is an oral presentation and discussion of a dissertation study. The purpose is to share the results of the study and to demonstrate to the committee and the academic community that the author has done work of sufficient quality to receive the doctoral degree and is able to speak to it in open forum.

The candidate must work closely with the dissertation chair to develop the dissertation. Communications among the candidate, the dissertation chair, and the dissertation committee are essential to ensure the process goes smoothly. The major milestones in the dissertation process are listed below:

- Research and dissertation: the student must work closely with dissertation chair as proposed and post major updates to the committee.
- Submit dissertation for committee review: dissertation committee needs minimum 4 weeks to review the dissertation.
- Dissertation review and committee recommendation: after review, the dissertation committee makes recommendation if a student is ready to defense the dissertation.
- Schedule dissertation defense: Graduate Office needs two weeks to schedule dissertation defense and make announcement. The program coordinator will help schedule the dissertation defense.

The dissertation must be shared with the dissertation committee at least 6 weeks (4 weeks for dissertation committee review and 2 weeks for dissertation scheduling) before conducting the dissertation defense.

The program can be completed on a full-time or part-time basis, with classes offered in three academic terms: fall, spring, and summer. Minimum time to complete this program in 3 years. The program must be completed within 7 years of the semester of the student's admission.

3.3. Admission Requirements

Dakota State University has an annual applications cycle. Applications are due in mid-spring and selected applicants begin course work in the fall of the following academic year. The university seeks highly motivated masters prepared individuals with education and professional credentials that will enable them to be successful doctoral students. It is mandatory that students must have a bachelors or master's degree in computer science to apply. Only US residents and those holding a Permanent Resident Card are allowed to apply to this program.

1. Baccalaureate degree from an institution of higher education with full regional accreditation for that degree.
2. Minimum undergraduate grade point average of 3.0 on a 4.0 scale (or equivalent on an alternative grading system).
3. Master's degree completed at the time of application.
4. Baccalaureate and/or master's degree must be in Computer Science.

3.4. Curricular Options within the Academic Programs

3.4.1. Program Curriculum

Table 5 shows the specific courses required in the program. The program currently required 15 elective credits. Any 700 or 800 level course offering with a CSC, INFA or INFS can be used as an elective course.

Table 5. Program Curriculum

Pref.	Num.	Title	Prerequisite(s)	Cr. Hrs.
Core Courses (15 Credits)				
CSC	840	Cyber Operations I		3
CSC	841	Cyber Operations II	CSC 840	3
CSC	844	Advanced Reverse Engineering		3
CSC	846	Advanced Malware Analysis		3
CSC	848	Advanced Software Exploitation		3
Research Core (9 Credits)				
CSC	804	Computer and Cyber Science Research Methodology		3
CSC	807	Computer and Cyber Science Research Design and Implementation	CSC 804	3
CSC	890	Seminar: Research 1 credit each		3
On-Site Research Seminars (3 Credits)				
CSC	890	Seminar: Residency 1 credit each		3
Dissertation (19 Credits)				
CSC	809	Dissertation Preparation	CSC 807 or CSC 808	3
CSC	898D	Dissertation (1-16 credits)		16
Electives (15 Credits)				
Any 700 or 800 level course offering with a CSC, INFA or INFS prefix (subject to elective program approval).				
			Total number of hours required for degree	61

3.4.2. Course Rotation

Table 6 includes the course rotation schedule from Fall 2022 to Summer 2024.

Table 6. Course Rotation Schedule

Prefix/Number	FA 22	SP 23	SU 23	FA 23	SP 24	SU 24
CSC 705 - Design and Analysis of Computer Algorithms			X			X
CSC 710 - Structure and Design Programming Language						
CSC 712 - Data Structures			X			X
CSC 714 - Database Systems						
CSC 716 - Secure Software Engineering						
CSC 718 - Operating Systems & Parallel Programming	X			X		
CSC 720 - Theory of Computation		X			X	
CSC 722 - Machine Learning Fundamentals	X			X		
CSC 723 - Machine Learning for Cyber Security		X			X	
CSC 744 - Software Development Leadership						
CSC 748 - Software Exploitation	X	X		X	X	
CSC 773 - Mobile Communication and Advanced Network Security			X			X
CSC 786 - Cyber Problems	X	X		X	X	
CSC 791 - Independent Study: Collaboration Research			X			X
CSC 803 - An Introduction to Research	X			X		
CSC 804 - Computer and Cyber Security Research Methodology		X			X	
CSC 807 - Computer and Cyber Security Research Design and Implementation	X			X		
CSC 809 - Dissertation Preparation		X			X	
CSC 808 - Mixed Research Methods for Computer and Cyber Sciences: Design and Implementation		X			X	
CSC 840 - Cyber Operations I	X			X		
CSC 841 - Cyber Operations II		X			X	
CSC 842 - Security Tool Development			X			X
CSC 844 - Advanced Reverse Engineering			X			X
CSC 846 - Advanced Malware Analysis	X			X		

3.4.3. Plan of Study

Table 7 shows an example of 4-year plan of study.

Table 7. An Example of 4-year Plan of Study

						Year 1			Year 2			Year 3			Year 4		
Course			Cr.Hrs	Req.	Grade	FL	SP	SU	FL	SP	SU	FL	SP	SU	FL	SP	SU
Core Courses (15 credits)																	
CSC	840	Cyber Operations I	3	R		3											
CSC	841	Cyber Operations II	3	R			3										
CSC	844	Advanced Reverse Engineering	3	R				3									
CSC	846	Advanced Malware Analysis	3	R					3								
CSC	848	Advanced Software Exploitation	3	R						3							
Research Core (9 Credits)																	
CSC	804	Computer and Cyber Science Research Methodology	3	R						3							
CSC	807	Computer and Cyber Science Research Design and Implementation	3	R								3					
CSC	890	Research Seminar 1 credit each (3 credits required)	3	R					1			1			1		
On-Site Research Seminars (3 Credits)																	
CSC	890	Seminar 1 credit each (3 credits required)	3	R			1						1			1	
Dissertation (19 Credits)																	
CSC	809	Dissertation Preparation	3	R									3				
CSC	898D	Dissertation	16	R										4	6	6	
Elective (15 Credits)																	
CSC	748	Software Exploitation	3			3											
CSC	723	Machine Learning for Cybersecurity	3				3										
CSC	791	IS: Collab Cyber Sec Research	3									3					
INFA	735	Offensive Security	3						3								
INFA	754	Intrusion Detection	3								3						
Total Cr.Hrs			61			6	7	3	7	6	3	7	4	4	7	7	0
Overall Hours						6	13	16	23	29	32	39	43	47	54	61	61

3.5. Curriculum Management

3.5.1. Program Constituencies

The Ph.D. in Cyber Operations program constituencies include faculty, students, alumni, and industry representatives. The program faculty include Andrew Kramer, Bhaskar Rimal, Cody Welu, Kyle Cronin, Meikang Qiu, Michael Ham, Shawn Zwach, Stephen Krebsbach, Tom Halverson, Tyler Flaagan, and Yong Wang. Dr. Yong Wang is the program coordinator of the Ph.D. in Cyber Operations program. The Beacom College has a Cyber Security Industry Advisory Board (CSIAB). The advisory board currently includes 16 members from companies such as VantagePoint, Midco, SBS CyberSecurity, First Premier Bank in South Dakota. The advisor board meets two times each year.

3.5.2. Course Grades

Course Grades are used as an indirect measure of student attainment of specific program goals and objectives. DSU Program Guidelines require students to maintain a 3.0 GPA in the program, receive no grades below a C, and have no more than 2 grades of a C. If students do not maintain the required “B” average, they are placed on academic probation and given the opportunity to raise their GPA to 3.0 within the next nine credit hours. If students failed to meet any of the criteria of good academic standing, they are suspended from the program for two consecutive terms. Students may submit an early readmission petition to the Graduate Dean under extenuating circumstances.

3.5.3. Transfer Credits

Academic courses will be transferred as meeting graduation requirements if the courses parallel the scope and depth requirements for the degree or if the courses meet electives required for the degree.

The following minimum conditions must be met before graduate-level credit can be accepted:

- The institution from which credit is transferred is regionally accredited at the Master's level.
- The student must have been in good standing at the institution from where the credit is transferred.
- The grades in courses transferred are "B" or better.
- The transfer credits must have been completed no more than five years prior to commencement of the DSU graduate degree program.
- No more than 9 credits may be applied to another master’s degree. The program committee for each degree program may establish specific program level processes and criteria for course evaluation.

3.5.4. Advising

A two-tier approach to advising Ph.D. Cyber Operations students is employed. After hearing from the Graduate Dean on their acceptance to the program, graduate enrollment counselors will reach out to new students to coordinate student on-boarding activities including admissions, orientation, and academic advising. The graduate enrollment counselors support graduate students in every stage of their graduate program, helping to provide information, access resources, register for classes, alleviate administrative and technological barriers, and promote student success. Other key roles for graduate enrollment counselors include:

- Advising and assisting students with the development of their Plan of Study and recommending it to the respective program coordinator for approval.
- Completing course substitutions and credit transfer forms.
- Maintaining up-to-date, accurate and detailed documentation on student interactions, progress, and meetings.
- Recommending appropriate resources for students who need additional academic support to improve student success.
- Collaborating with appropriate departments (Registrar, Financial Aid, Cashier, Disabilities Services, Counseling Services, Veterans Services, etc.) to resolve individual student issues and ensure positive student experiences.

New doctoral students are also assigned a graduate faculty advisor. Program Coordinator Dr. Yong Wang serves as an academic advisor for each student upon entry to the Ph.D. in Cyber operations program. Other roles for graduate faculty advisors include:

- Discussing skill development and specializations

- Career planning
- Transitioning students to dissertation chair and committees
- Guide students through the program assessment process (comprehensive exams, dissertation)

Each student also has a dissertation advisor who helps the student with research and dissertation. A doctoral dissertation committee is formed when a student is ready to conduct proposal defense and dissertation defense. The committee includes Chair or Co-Chairs, plus minimum of one program representative and one Graduate Council representative:

- Program representative: The program representative is a DSU graduate faculty member or an affiliate graduate faculty member (as designated by the Graduate Council) in the student's program of study.
- Graduate Council representative: The Graduate Council representative is a DSU graduate faculty member who is outside the graduate student's program of study. The Graduate Council representative should possess sufficient familiarity with the student's research topic to review and comment on the manuscript. This committee member verifies that Graduate Council policies and procedures have been followed, ensures fair treatment of the graduate student, and ensures that the quality of the research is commensurate with the student's degree objectives.

All committee members must have the terminal degree for their field or approval from the Dean of Graduate Studies. The committee membership and the committee chairmanship are approved by the Dean of Graduate Studies, based on the recommendations of the student's academic advisor and the graduate program coordinator.

3.5.5. Hiatus Status

Continuous enrollment is defined as registering for at least one course per academic term. A student can take a hiatus for a term if taking no credit. A graduate student can take max two hiatus terms during plan of study.

3.5.6. Suspension

All graduate students are expected to maintain a Plan of Study grade point average of 3.0 (“B” average) throughout their graduate program. Failure to maintain the “B” average places the student on academic probation. Students on academic probation may register for an additional 9 credit hours of coursework and must raise their Plan of Study GPA to a 3.0 (“B” average) after completion of the 9 credits. If this is not accomplished, the student will be suspended from the program. A student who receives more than 6 credits of “C” or any grade lower than a “C” is suspended from the program.

Should it be necessary to suspend a graduate student for academic reasons, the student may apply for readmission to the Office of Graduate Studies after two semesters (summer is considered a semester term). The student must demonstrate an adequate reason for readmission.

A grievance procedure has been established for students wishing to contest probation or suspension. The Graduate Council will hear all grievances, following the procedure established in DSU Policy 03-30-00 Appealing Academic and Administrative Decisions.

Graduate students who have been officially suspended and who seek reinstatement shall submit a formal request for reinstatement, along with a supporting statement of explanation, to the Office of Graduate Studies. Requests shall be acted upon according to the established procedure for application to the program.

Students wishing to contest probation or suspension may appeal the decision, following the grievance procedure established by DSU: Appealing Academic and Administrative Decisions 03-30-00 http://www.dsu.edu/hr/policies/03-30-00.aspx. Graduate Council will hear all grievances. Students should consult the Office of Graduate Studies for details.

Students suspended for academic reasons may seek reinstatement after two academic terms by submitting a formal request for reinstatement, along with a supporting statement of explanation to the Office of Graduate Studies. The request shall be acted upon according to the established procedure for application to the program.

3.6. Program Modification

DSU received authority to offer the D.Sc. in Cyber Security at the April 2014 Board meeting. DSU proposed a change in the degree designation from the Doctor of Science (D.Sc.) to the Doctor of Philosophy (Ph.D.) in 2018. In addition to making the change from D.Sc. to Ph.D., DSU also requested a name change for the program from Cyber Security to Cyber Operations. Cyber security is the umbrella title for more specific areas such as cyber operations and cyber defense. The title, Ph.D. in Cyber Operations, aligns with our BS in Cyber Operations. The Board approved the change at the May 2018 meeting.

Another program modification was proposed and approved in Spring 2022. The major modification includes:

- CSC803 An Introduction to Cyber Security Research (3 credits) is eliminated from the research core. The research core now includes requirement of 3 credits CSC890 Seminar: Research (1 credit each). CSC890 Seminar: Research is offered in both Spring and Fall. Students are required to present approved research papers and participate in discussions in the seminar.
- CSC804 Computer and Cyber Science Research Methodology: minor course name modification due to the restructure of the research courses.
- CSC807 Computer and Cyber Science Research Design and Implementation: minor course name modification due to the restructure of the research courses.
- Create a new course CSC808 Mixed Research methods for Computer and Cyber Sciences: Design and Implementation (3 credits). This course presents mixed research methods including both quantitative and qualitative research methods commonly used in computer and cyber sciences research. Topics include (but not limited to) survey research, utilization of statistical software, qualitative research methods such as focus group discussions, case study, observation. The course includes a project component which help students in the computer and cyber science fields go through each step of the research process and apply the corresponding research methods in a selected research topic.
- Create a new course CSC890 Seminar: Research. CSC890 Seminar. This is a highly focused and topical course. The format includes student presentations and discussion of reports based on literature, practices, problems, and research. Seminars may be conducted over electronic media such as Internet and are at the upper division or graduate levels.
- CSC898D Dissertation and Electives: change dissertation credits from 22 to 16 and increase elective credits from 9 to 15. The changes provide students opportunities to take two more elective courses in cyber operations. This is especially important for the students who are admitted to the program from non-DSU schools. The cyber operations programs including the undergraduate and the graduate programs at DSU prepare students very well for doctoral studies. Allowing two more elective courses will be very beneficial for non-DSU students to utilize the existing curriculum in our cyber operations program. Further, as more graduate courses become

available at DSU, e.g., courses in Artificial Intelligence, allowing two more elective courses will also be very beneficial to the students who are admitted to the program from the DSU.

Part 4. Program Enrollments and Student Placement

4.1. Program Enrollments

In the fall of 2015, DSU received authorization from the SD Board of Regents and the Higher Learning Committee to offer a doctoral degree in Cyber Operations. In the spring of 2015, DSU accepted its first applications in the program. In the fall of 2015, we admitted our first students. Figure 1 shows the number of applications received each year since we have offered the program in 2015 (blue). The bars in orange represent the cumulative number of students in the Ph.D.in Cyber Operations program each year.

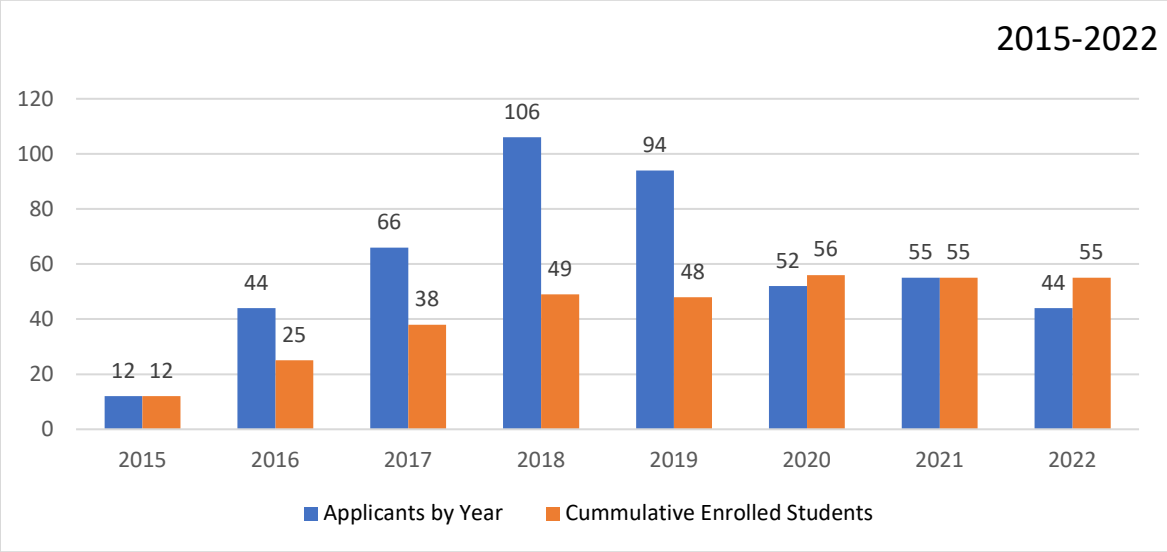

Figure 1. Application and Cumulative Enrollment of Cyber Operations Doctoral Students

In the first few years of availability, the program grew to attract a considerable number of applications (U.S. only). Our acceptances remained limited, however, due not only to our own capacity to support these doctoral students, but because many applicants lacked the technical background to thrive in the program. In 2019 DSU received permission from the SD Board of Regents and the Higher Learning Commission to offer a doctoral degree in Cyber Defense. The doctoral program in Cyber Defense addresses important technical aspects of cyber defense, yet infuses cyber defense leadership, ethics, and management concepts more suited to students with technical backgrounds other than the Computer Science B.S. and M.S. training preferred for candidates of the Cyber Operations doctoral program.

In 2020 applications to the more technical Cyber Operation doctoral program leveled, as did the cumulative enrollment in the program. Conversely, applications to the new Cyber Defense doctoral programs increased dramatically. At about the same time (2019), DSU received permission from the SD Board of Regents and the Higher Learning Commission to change the title of our doctoral degrees from Doctorate in Science (D.Sc.) to Doctoral in Philosophy which is more recognizable and consistent with degree programs in the Computer Science discipline.

4.2. Student Placements

A graduate from the program can choose a career path including professor, researcher for private industry firms, and researcher for government agencies. The following is a list of employers for graduates in our program:

- Accenture Federal Services, Arlington, VA
- Amazon, Seattle, WA
- Corelight, San Francisco, CA
- FullStory, Atlanta, Georgia
- Mandiant, Severn, MA
- Recorded Future, Somerville, MA
- Dakota State University, Madison, SD
- University of Alabama in Huntsville, Huntsville, AL

Part 5. Faculty Credentials

5.1. Program Faculty

A list of the faculty who teach in the Ph.D. in Cyber Operations programs at DSU and their credentials are included in Table 8. Current vitae for the faculty listed in Table 9 are included on the program review web site.

Table 8. Program Faculty

Faculty	Research Interests	Related Courses
Farhad Akhbardeh, Ph.D.	Naturel language processing, ML	CSC 722 - Machine Learning Fundamentals CSC723 - Machine Learning for Cyber Security
Kyle Cronin, D.Sc.	technology & education, cyber competitions, system administration, cellular/wireless technology, networking/virtualization/enterprise computing	CSC - 841 Cyber Operations II
Tyler Flaagan, Ph.D.	offensive security tools, techniques, and procedures	INFA 735 - Offensive Security
Michael Ham, D.Sc.	software reverse engineering, software security, BGP, networking secure protocol design	CSC 840 - Cyber Operations I CSC 846 - Advanced Malware Analysis
Andrew Kramer, MS	Software exploitation, reverse engineering	CSC 844 - Advanced Reverse Engineering CSC 848 - Advanced Software Exploitation
Meikang Qiu, Ph.D.	cyber security, big data analysis, AI, cloud computing, smarting computing, embedded systems, etc.	CSC 803 - An Introduction to Research CSC 808 - Mixed Research Methods for Computer & Cyber Sciences: Design and Implementation
Bhaskar Rimal, Ph.D.	IoT security, CPS security, critical infrastructure security (e.g., smart grid), wireless communications security (5G, 6G), intelligent transportation systems, cloud/edge computing/networking, ML and quantum computing	CSC 804 - Computer and Cyber Science Research Methodology CSC 807 - Computer and Cyber Science Research Design and Implementation
Varghese Vaidyan, Ph.D.	Software and hardware security, Side-channel Attacks, IoT Security, Fault Analysis, ML	CSC 809 - Dissertation Preparation
Yong Wang, Ph.D.	security and privacy in IoT, mobile devices, cloud, and cyberinfrastructure; network security in general	INFA 723 - Cryptography INFA 751 - Wireless Security CSC 773 - Mobile Communication and Advanced Network Security
Cody Welu, Ph.D.	network defense, threat hunting, intrusion detection, cyber security education	INFA 754 - Network Security Monitoring and Intrusion Detection
Shawn Zwach, MS	Malware analysis, networking	INFA 732 - Malware Analysis

5.2. Workload for Faculty Members Holding Professional Rank

The current faculty workload document of Dakota State University was effective May 1, 2021. While the standard workload is 30 workload units per academic year, reasonable time is allocated to faculty members who hold professorial rank and who actively engage in research, scholarship, or creative artistic activity or who actively pursue professional service activities related to their disciplines. Ordinarily, reasonable allocated time is equivalent of six workload units of instruction, or its equivalent per academic year and, if assigned, the faculty member must be actively engaged in productive scholarship. The institution may adjust this workload requirement to ensure faculty members have adequate time for research and scholarship or service or as deemed necessary by the institution.

The typical full time teaching load for tenured or tenure track faculty is 24 semester credit hours for each academic year (fall and spring). Faculty whose teaching load exceeds that requirement (and who are actively engaged in research, scholarship, or creative artistic activity and who actively pursue professional service activities related to their disciplines) may qualify for overload pay when the teaching load exceeds the 24-credit requirement in any given academic year. Faculty holding professorial rank but located off campus are required to provide service to the university, service to the discipline, and to actively engage in research, scholarship, or creative artistic activity.

Academic advising is recognized as part of a faculty member's teaching workload and generally will not exceed an assignment as primary adviser of more than 50 students for faculty members with professorial rank and more than 30 students for faculty members with lecturer rank. An unusually heavy advising load can be offset by a reduction in the faculty member's committee or other college assignments and/or a reduction in teaching load for faculty members holding lecturer rank.

5.3. Faculty development

In July 2018 Dakota State University established Center for Teaching and Learning (CTL) to serve as the university hub of teaching support and innovation. Prior to the establishment of the CTL, a single university committee was charged with identifying instructional development topics and implementing faculty workshops/events. That committee is now an advisory group to the CTL, which is directed by a senior faculty (1/2 time, by application) and includes an instructional design and technology specialist (full time) and clerical support. The CTL is also assisted by four faculty associates (one from each college) who are among the university's most accomplished instructors with strengths in course development, learner engagement, and assessment. The CTL faculty associates provide mentoring and consultation with individual faculty as their time permits. This Center for Teaching and Learning identifies, coordinates, and provides professional and academic development activities for faculty and staff. The CTL works with academic administrators and faculty to identify instructional priorities and develop programming to address those priorities.

The CTL not only supports teaching and learning traditional classroom environments but is especially focused on providing pedagogical and technology development in online environments. This support has included the creation of instructional aids, materials, and media that are accessible online to assist faculty in improving their teaching and student interaction skills. The CTL has also initiated peer review of all online courses using the state mandated Quality Assurance (rubric). For graduate students, the CTL provides expertise to support the goals of the university, including assisting in the production of quality thesis, dissertations, presentation, grant writing, and understanding of compliance issues. For undergraduates, engagement objectives include topics on mentored research, integrity (plagiarism, and copyright), and student service/government.

Funds for faculty research and travel:

- DSU supports a Faculty Research Initiative (FRI) intended to encourage and facilitate faculty research and creative activity. Year 2021's competition offered up to $3,000 for individual faculty or up to $5,000 for collaborative teams.
- The Supporting Talent for Research Trajectories (START) internal funding program was launched in 2018. This seed fund offers faculty support for preliminary work on research that will result in proposals for externally funded research grants.
- DSU also routinely sets aside significant funding for instructional and professional travel and for faculty training. Individual faculty can qualify for up to $1,200 for travel and training at qualifying events.
- Faculty sabbatical, by application and with a Dean's approval, faculty can apply for a one semester research sabbatical which is reviewed by the university promotion and tenure committee.

Part 6. Academic And Financial Support

6.1. Beacom College of Computer and Cyber Sciences

The Beacom College of Computer and Cyber Sciences office is the central point of support for all undergraduate and graduate students with majors within this college. The central office is located in the Beacom Institute of Technology Building. The office is also provided with several work study positions that are tasked with helping faculty whenever help is requested. Table 9 includes the staff in the Beacom College.

Table 9. The Beacom College

Name	Title
Patrick Engebretson	Dean
Tom Halverson	Associate Dean of Beacom Undergraduate Programs
Yong Wang	Associate Dean of Beacom Graduate Programs
Erin Kahler	Administrative Assistant II
Kathy Engbrecht	Retention Specialist
Eric Holm	Systems Architect

6.2. Graduate Programs and Research Support Services

The Office of Graduate Studies was established to promote and support graduate education at DSU. The Dean of Graduate Studies collaborates with and supports the functions and responsibilities of the Graduate Council and the graduate program committees within each college and serves as the advocate for graduate education and graduate student support at DSU. The Office of Graduate Studies staff is included in Table 10 below. The day-to-day operations and services provided by the Office of Graduate Studies are client centered. The office offers guidance and help to students from the first inquiry to graduation. This includes providing accurate and timely program information and maintaining the graduate programs website with current information for degree seeking students (http://www.dsu.edu/gradoffice/). The office also facilitates the recruitment of prospective students, the application process, assisting in setting up interactive audio video for remote sites in South Dakota and online for distance students. Other services provided by the Office of Graduate Studies include assisting with course scheduling and course rotations; making students aware of changes in schedules, rotations, and graduate policies; assisting with registration; supporting the assistantship committees; monitoring student progress toward graduation; and serving as a liaison among other support staff, faculty, and administrators.

Table 10. The Office of Graduate Studies

Name	Title
Mark Hawkes	Dean
Erin Blankespoor	Administrative Assistant
Abby Chowing	Graduate Enrollment Specialist
Brianna Mae Feldhaus	Graduate Enrollment Specialist
Jennifer Mees	Program Assistant II

On July 1, 2018, the new role of Vice President of Research and Economic Development was developed at DSU. This position was created to address unprecedented growth in student numbers, employee numbers, academic programs, research activity, to further formalize the research processes campus wide, and coordinate efforts between faculty and campus departments for increased efficiency. The university's awarded grant monies have been increasing substantially since 2018. The award total increased $2,396,866 in 2018 to $6,493,257 in 2019 and $5,923,216 in 2020. With the CyberHealth Strategic Alliance with Sanford Heath and the $90 million initiative to expand DSU's Applied Research Lab, these numbers will likely continue to grow. Table 11 includes the staff in the Research and Economic Development Office.

Table 11. Research and Economic Development Office

Name	Title
Ashley Podhradsky	Vice president for Research and Economic Development
Peter Hoesing	Associate Vice President for Research & Economic Development
Beth Delzer	Administrative Assistant

6.3. Library Resources and Services

Since Dakota State University received its current focused mission in the 1980s, the Mundt Library's mission has been to expand its collection of materials on computers, technology, and information systems. To that end, the Library has subscribed to an ever-widening number of databases and eBooks that support this emphasis. The physical and electronic collections continue to be built through faculty recommendations and requests, as well as from librarian selection based upon their knowledge of the curriculum and its needs. The journal collection is also based on faculty requests and is fine-tuned by means of an annual analysis of journal use. This analysis helps the Library focus its expenditures (and finite budget) on those journals that are regularly needed and used by the institution's students. The collections have been enriched with digital information. The Library subscribes to numerous online databases including the Association for Computing Machinery (ACM) Digital Library, ProQuest Research Library, ABI-Inform, IEEE, Lexis Nexis and over 100 others. Most of the material indexed in these databases includes direct access to the full text of the articles indexed. For those articles not available in full text, the Library provides speedy interlibrary loan service at no extra cost to all DSU students, faculty, and staff.

The Library holds an extensive collection of electronic books on computer security and information assurance, which are discoverable via the library catalog. In addition, the Library subscribes to Safari Tech Books Online, which provides access to 150 titles that provide hands on training in many areas of technology. The Library also provides access to LyndaCampus.com, which provides digital tutorials in almost every area of technology, marketing, education, and career planning. The Karl E. Mundt Library is also a member of several library consortiums and maintain borrowing and lending agreements with academic libraries across the country and around the world. As such, the Library can attain materials in

digital and/or physical formats for any scholarly need. The professional library staff is included in Table 12 below.

Table 12. Library Staff

Name	Title
Mary Francis	Interim Director of the Library
Ryan Burdge	Archivist
Michaela Clark	Library Associate -- Circulation & Interlibrary Loan
Ellen Hoff	Technical Services Librarian

6.4. Online@DSU Support Services

The Office of Online Education is responsible for program planning, marketing, program implementation and overall management of courses and programs offered by alternative delivery at Dakota State University. Working in partnership with the colleges and the institution's academic support areas, the Office of Online Education works to design and develop active and collaborative degree programs at a distance.

The Office of Online Education is staffed with the Director of Online Education, the State Authorization Coordinator, and an online admissions specialist shown in Table 13 below. This team serves the needs of students who are enrolled in the online and videoconferencing courses at DSU. The office is the mainstay of distance services to students, working with the administrative offices of DSU to provide these services. The staff also serves the Web needs of faculty, staff, and students at DSU. The office staff assists faculty in the design and implementation of courses delivered by various forms of technology. Table 13 includes the staff in the office of Online Education.

Table 13. Online@DSU Support Staff

Name	Title
Annette Miller	State Authorization Coordinator
Sarah Rasmussen	Director of Online Education
Andrea Derynck	Online Admissions Specialist

6.5. Information Technology Services Staff

DSU has a comprehensive technology infrastructure supporting universal (on and off campus) access to computing resources. The Information Technology Services staff listed in Table 14 below provides technology support to faculty, staff, and students.

Table 14. ITS Staff

Name	Title
Shawn Jaacks	Chief Information Officer
Brent Van Aartsen	Chief Technology Officer
Stephanie Baatz	Director of Support Services
Lora Ersland	Director of Administrative Services
Craig Miller	Technology Procurement & User Support
Tyler Steele	Manager of Multimedia Services

6.6. Administrative Support Staff

Current administrative staff will provide the academic support services to deliver academic programs at DSU. The administrative support personnel who are particularly critical to the delivery of the graduate programs are included in Table 15 below.

Table 15. Administrative Support Staff

Name	Title
Corey Braskamp	Director of Facilities Management
Kathy Callies	Registrar
Amy Crissinger	Vice President for Student Affairs and Enrollment Management
Amy Dockendorf	Controller
Denise Grayson	Director of Financial Aid
Sara Hare	Director of Budget & Grants Administration
Peter Hoesing	Director of Sponsored Programs
Kelli Koepsell	Director of Marketing and Communication
Javier Lopez	Food Service Manager
Jeanette McGreevy	Director of Institutional Effectiveness and Assessment
Laura Osborn	Director of Institutional Research
Deb Roach	Director of Career and Professional Development
Donna Fawbush	Events Coordinator/Interim Bookstore Director
Nicole Claussen	Director of International Programs Susan Slaughter Program Assistant II

6.7. Financial Support to the Students

Financial aid opportunities are expected to come from institutional and private sources. Financial aid policies and procedures for application, award, and distribution have already been developed to support the graduate programs at DSU. DSU has also certified alternative loan eligibility for enrolled graduate students (based on their educational costs) to regional and national lenders.

Part 7. Facilities and Equipment

With DSU's 1:1 portable computing environment requiring students to have a Windows or Mac laptop and its expansive secure wireless network, the need for dedicated computer labs is not as prevalent as it has been in the past. Classroom space on campus was significantly increased with the Fall 2017 opening of the Beacom College of Computer and Cyber Sciences, the first LEED version 4 building in South Dakota, and the renovations of East Hall in 2019 and 2021. Dedicated research facilities are available in the MadLabs. Students at DSU are given access to industry standard software and a virtual Information Assurance Lab to meet all their computing needs.

7.1. Information Assurance Lab

DSU’s Information Assurance (IA) Lab is a cloud-based solution to the problems of technology education. The IA Lab was designed and implemented in 2009 and its use has continually grown ever since with the additions of new classes plus growing enrollment. The IA Lab allows for an instructor to focus their time on creating and testing their lab. Once the lab is finalized, the lab administrator can copy unique instances of the lab to all students within the class. This process takes approximately 20 minutes total, depending on the size of the class. The lab can run any platform (Windows, MacOS, FreeBSD, or Linux), in addition to popular firewall and router distributions. These labs are all safely contained so that students are safe when practicing any cybersecurity concepts. Due to the self-service nature of lab implementation, it can be used for projects far beyond the classroom. The IA Lab hosts research projects for undergraduate and graduate students, in addition to housing research projects for faculty members. Due to the safe/secure nature of the lab, it also houses DSU’s High Performance Computing/Hadoop environment. The lab users vary from semester to semester, but largely include students from the

programs including Information Systems, Cyber Operations, Computer Science, Network Security Administration, etc.

7.2. MadLabs

On Jan. 31, 2018, Governor Dennis Daugaard signed House Bill 1057 into legislation which permit ted the demolition of DSU's Lowry Hall and construction of the Madison Cyber Labs, or MadLabs. The Madison Cyber Labs build on DSU's expanding capabilities and strengths to establish a hub of cybersecurity and cyber operations expertise, research, and economic development in South Dakota. As of February 2022, DSU faculty has established 16 MadLabs. Construction of $18 million, 40,000 square foot MadLabs building, located on the southwestern edge of campus, was completed in Fall 2019. It is the first research facility of its kind in the Upper Great Plains region.

There are five components to MadLabs' game-changing plan to reshape the cyber field in South Dakota, including 1) Resources: A winning combination of laboratory research space, state-of-the-art hardware and software, faculty expertise, and growing institutional relationships with a wide variety of public and private agencies; 2) People: Undergraduate and graduate students, faculty, researchers, interns, and other collaborators; 3) Programs: Nationally recognized cyber degrees from the associate to doctoral level, along with other professional development opportunities; 4) Research areas and institutes: Focus areas in defined interdisciplinary and multidisciplinary regions, that draw from every college on campus; 5) REED Connection: DSU is connected to the South Dakota Research, Education, and Economic Development Network (REED) via a 100 Gbps connection. Providing the campus with connectivity to Internet2, the Great Plains Network, and other research networks.

MadLabs® drives innovation and ideas from DSU into the South Dakota economy, the Great Plains, and the nation. At the same time, it draws new talent to the state and the region. The facility and its programs attract elite scholars, researchers, professionals, and partnerships with government, businesses, nonprofits, and other higher education institutions.

Researchers within MadLabs primarily focus on projects exploring and advancing technology application, information and quality assurance, business adverse event planning, economic growth, and policy improvement across multiple disciplines and fields. MadLabs' focus areas include cybersecurity, digital forensics, cyber defense, Artificial Intelligence (AI) and machine learning, reverse engineering, and malicious digital artifacts. MadLabs also fosters partnerships with the public and private sectors to cultivate ideas and transform their research to make a difference in the world. MadLabs currently includes 16 labs. PATRIOT Lab, Deep Red Labs, and VERONA Lab are three labs in the MadLabs.

Figure 2. DSU Madison Cyber Labs

7.3. MadLabs Research Environment and Network

The computing resources are available through the MadLabs Research Environment and Network (MADREN) at DSU. MADREN is an extensive technology infrastructure dedicated to cybersecurity research. The MADREN includes 10 Lenovo SR630s servers, each with dual Intel Xeon Gold 5118 Processors, for a total of 240 cores @ 2.3 GHz. This is supported by 2.56TB of TruDDR4 @ 2666MHz RAM available and a 126TB HPE Nimble Storage Adaptive Flash Array. These resources are accessible through virtualization via VMware Director. The MADREN also contains a large GPU cluster accessible through VMware View. It includes 5 Lenovo SR670s servers, each with dual Intel Xeon Gold 6242 Processors, for a total of 160 Cores @ 2.8 GHz each, and 1.92TB of TruDDR4 Performance+ RAM @ 2933MHz. The cluster has 40 NVIDIA Tesla T4 16GB cards, with 12,800 Turing Tensor Cores and 102,400 CUDA Cores. The total GPU capacity represents 324 teraFLOPS, 2.6 petaFLOPS, 5,200 TOPS (INT8), or 10,400 TOPS (INT4). All MADREN resources have access to Internet2, with a max data transfer of 100 Gbps.

Part 8. Assessment and Strategic Plan

8.1. Assessment

The assessment of the Ph.D. in Cyber Operations program is conducted through the Trojan Assessment Profile (TAP) (https://solutions.nuventive.com/).

Program Learning Outcomes (PLOs)

- Software reverse engineering: Be able to articulate the importance of software reverse engineering and successfully complete hands-on exercises and demonstrate a thorough understanding of the domain.
- Malware Analysis: Be able to utilize reverse engineering tools and procedures to conduct static and dynamic analysis on unknown binaries to understand their behavior and purpose
- Software Exploitation: Be able to use automated exploitation tools, understand manual exploitation process in a Windows and Linux environment, and create shell code using software exploitation techniques including but not limited to heap and RP exploitation.
- Cyber Operations: Be able to develop an in-depth understanding of cyber operations content focusing on mitigate cyber threats and anticipation of a cyber-attack.
- Communication: Be able to communicate and articulate technical information in an effective manner.

PLO Assessment Measures

- The results from the oral comprehensive exams, proposal defenses, and dissertation defenses are used to assess the PLOs directly. The target for oral comprehensive exams is 80% pass rate for the first attempt and 90% pass rate for the second attempt. The target for proposal defenses and dissertation defenses is 90% pass rate for the first attempt.
- Exit interview is conducted for each student completing dissertation defense.

Course Mapping to PLOs is shown in Table 16.

Table 16. Course Mapping to PLOs

PLO Outcome	CSC 840	CSC841	CSC844	CSC846	CSC848
Software reverse engineering			Developing		
Malware analysis				Developing	
Software exploitation					Developing

Cyber operations		Developing			
Communication	Developing	Developing	Developing	2	Developing

Among 6 students who took oral comprehensive exams in 2022, 1 student failed in software exploitation and planned to take the oral comprehensive exam in 2023. The rest of the students (83.3%) passed their oral comprehensive exams.

8.2. Strategic Plan

The Ph.D. Cyber Operation program will contribute to the following foundational goals as defined in the Strategic Plan *DSU ADVANCE 2027* (Table 17).

Table 17. DSU Strategic Plan Foundational Goals and the Ph.D. in Cyber Operations

Foundational Goal	Ph.D. in Cyber Operations
Strengthen Regional and National Relevance	A unique doctoral program specialized in cyber operations. Aligned with the federal government's efforts to identify, deter, protect against, deter, and respond to cyberattacks and threat actors. Collaborating with public/private sectors to resolve critical issues in cybersecurity.
Increase Student Enrollment	An online program with a residency requirement to engage and connect students across the nation. A community sharing same passion and mission in cyber operations. Dedicated faculty and staff who continuously enhancing the program to stay current with technology trends.
Enhance Student Success	Emphasis low level programming in malware analysis, reverse engineering, and software exploitation. Continuously improving curriculum to prepare students for cyber operations and research. Innovative artifacts from students' research and dissertation. Faculty-led research creating more research opportunities for students.
Maintain Higher Learning Commission Accreditation	Continuously conduct program assessment using Trojan Assessment Profile to ensure the program meets Higher Learning Commission Accreditation requirements.

The Ph.D. Cyber Operation program will strive to support two Pillars as identified in the Strategic Plan *DSU ADVANCE 2027* as shown in Table 18.

Table 18. DSU Strategic Plan Pillars and the Ph.D. in Cyber Operations

Pillar	Ph.D. in Cyber Operations
Pillar 1: Increase Student Success	Improve student preparedness for cyber operations and research and help students achieve their degree goals. Engage graduates from the Ph.D. in Cyber Operations to retain and assist current students. Build a community in cyber operations working together to address critical cyber security issues in the nation.
Pillar 2: Grow Scholarship, Research, Intellectual Property, & Economic Development	Promote scholarship through Ph.D. in Cyber Operations portfolio requirement. Participate in sponsored research internally and externally. Collaborate with DSU Research and Economic Development Office to create Intellectual Property.

REFERENCES

Cyber Operations (CAE-CO) program. (2023). National Security Agency/Central Security Service. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/Cyber-Operations/

Cybersecurity Ventures. (2022, August 10). *Cybercrime Damages To Cost The World $7 Trillion USD in 2022*. https://www.einnews.com/pr_news/585389499/cybercrime-damages-to-cost-the-world-7-trillion-usd-in-2022

National Initiative for Cybersecurity Careers and Studies. (2022). *Cyber Operations*. https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cyber-operations

Petersen, R., Santos, D., Wetzel, K., Smith, M., Witte, G., & others. (2020). *Workforce framework for cybersecurity (NICE framework)*.

Steve Morgan. (2020, November 13). *Cybercrime Costs. PHOTO: Cybercrime Magazine. Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

The White House. (2021, May 12). *Executive Order on Improving the Nation's Cybersecurity*. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/