Transdisciplinary Cybersecurity

Chair – Director of Cybersecurity Centers - Liebrock
Faculty:
Adjunct – Burnham, Pierson, Quist, Tietjen
CLASS – ChoGlueck, Dotson, Elliott, Kelly
Computer Science & Engineering – Jeffery, Liebrock, Mazumdar, Ramyaa, Shin, Soliman, Tong, Zheng
Electrical Engineering – El Osery, Shao, Teare
Business & Technology Management – Wang
Materials & Metallurgical Engineering - Majumdar
Mechanical Engineering – Ghosh, Lee

Degrees Offered: Master of Science, Professional Masters, and Doctor of Philosophy in Transdisciplinary Cybersecurity

Mission

Addressing many of the greatest challenges to society requires understanding and integration of the methods, theories, techniques, and perspectives of multiple disciplines to develop new approaches to solve complex, real-world challenges. The mission of the Transdisciplinary Cybersecurity graduate programs is to prepare students with a broad understanding of cybersecurity from the foundational documents that have guided the development of the discipline to the ethical, legal, and psychological challenges that cybersecurity professionals face. Students further engage in hands-on cybersecurity risk analysis, data analysis, and policy development. In addition, technical electives provide technical expertise that students will need to solve real-world challenges in cybersecurity.

These programs are designed to:

1. engage students with diverse backgrounds in cutting edge cybersecurity research and prepare them for high demand, high pay cybersecurity careers; and
2. enhance cybersecurity innovation leading to improvement in the cybersecurity stance of the state of New Mexico, the nation, and the world.

Graduate Programs

These programs are all available both on campus and via distance delivery. Any course not offered via distance delivery is explicitly marked as such. All courses must be taken for a letter grade to meet program requirements except for CYBS 590, CYBS 591, CYBS 595.

Educational Objectives

The transdisciplinary faculty for this program strives to improve the graduate program in transdisciplinary cybersecurity. Several years after graduation it is expected that our graduates will be:

- leaders who help address challenges to society requiring understanding and integration of the methods, theories, techniques, and perspectives of multiple disciplines; and
- lifelong learners who continue grow in their education and profession to use and/or develop new approaches to solve complex, real-world challenges.

Student Outcomes

Upon completion of a transdisciplinary cybersecurity degree program, students will be able to:

1. Communicate effectively both orally and in writing to a variety of audiences.
2. Analyze and evaluate the cybersecurity needs of an organization to conduct a cybersecurity risk assessment.
3. Design operational and strategic cybersecurity approaches and policies.
4. Understand and appreciate the legal, ethical, technical, and psychological environment impacting individuals and business organizations to determine the implications and risks associated with cybersecurity decisions.

In addition, upon completion of a Master of Science in Transdisciplinary Cybersecurity or Doctor of Philosophy in Transdisciplinary Cybersecurity degree, students will be able to:

5. Carry out research that demonstrates critical thinking by analyzing situations, integrating acquired knowledge, and developing solutions to real world cybersecurity challenges.

Core Courses

These courses are required for all programs (minimum of 18 credits at the 500-level; 3-4 credits for each course):

- CYBS 561 Foundations of Cybersecurity
- CYBS 502 Cybersecurity Ethics and Law
- CYBS 503 Cybersecurity Policy
- CYBS 504 Psychology of Cyber
- CYBS 509 Systems Decision and Risk Analysis
- CYBS 505 Data Science for Cyber

Technical Electives

- CYBS 541 Advanced Cryptography
- CYBS 554 Computer Network Security
- CYBS 557 Hardware-Based Network Security for the Internet of Things
- CYBS 563 Access Control and System Security
- CYBS 564 Secure Systems Administration
- CYBS 514 Computer Security and Incident Response
- CYBS 515 Reverse Engineering Malware
- CYBS 506 Cyber Physical System Security
- EE 560 Electronic Warfare
- EE 565 Position, Navigation and Timing

Other graduate cybersecurity courses may be substituted for the approved list only with prior written approval from their advisor and the program chair, which must be filed with the Center for Graduate Studies prior to taking the course.

Cybersecurity Area Courses

Graduate credits (CYBS 589) in the following cybersecurity areas: cybersecurity policy, psychology of cybersecurity, cybersecurity data science, or cybersecurity

technical electives.

Master of Science in Transdisciplinary Cybersecurity (MSTC)

The MSTC program requires a minimum of 30 graduate credits in cybersecurity including a research project.

Students in the MSTC program must take all of the required core courses listed above, a minimum three credits of technical electives from the approved list, and at least three additional credits in the following cybersecurity areas: cybersecurity policy, psychology of cybersecurity, cybersecurity data science, or cybersecurity technical electives; other cybersecurity courses may be substituted for the approved list only with prior written approval from the advisor and the program chair, which must be filed with the Center for Graduate Studies prior to taking the course.

Research projects may be either a thesis (6 credits) or an independent study (3 credits). A thesis is to be of a high quality to make a contribution to the discipline and should be submitted for publication. Students who complete an independent study must also complete an additional cybersecurity area course.

MSTC Degree Minimum Requirements Summary

- All core courses listed above (18 cr)
- 3 credits of technical electives
- 3 credits of cybersecurity area courses
- Research
    - 6 credits of thesis

    or
    - 3 credits of independent study and
    - 3 credits of cybersecurity area courses

Professional Master in Transdisciplinary Cybersecurity (PMTC)

The PMTC program requires a minimum of 30 graded graduate credits.

Students in the PMTC program must take all of the required core courses listed above, a minimum of six credits of technical electives from the approved list, and at least six additional credits in the following cybersecurity areas: cybersecurity policy, psychology of cybersecurity, cybersecurity data science, or cybersecurity technical electives; other cybersecurity courses may be substituted for the approved list only with prior written approval from the advisor and the program chair, which must be filed with the Center for Graduate Studies prior to taking the course.

PMTC Degree Minimum Requirements Summary

- All core courses listed above (18 cr)
- 6 credits of technical electives
- 6 credits of cybersecurity area courses

Accelerated Masters

The combined degrees of a MSTC or PMTC along with a BS in an aligned field may be achieved in five years. Students must complete all of the requirements of the associated BS and the MSTC or PMTC degrees. Students in the accelerated program may use up to nine 500-level or above credits toward both their BS and either MSTC or PMTC degrees.

Doctor of Philosophy in Transdisciplinary Cybersecurity

Students of exceptional ability, as demonstrated in previous courses, in a master's degree program, or in professional research experience, may pursue a program leading to the doctoral degree.

The prospective doctoral candidate in Transdisciplinary Cybersecurity should develop a strong background in the core of cybersecurity. Additionally, students must achieve a high level of competence in the field of specialization defined by their dissertation research. Additional information is found in the Graduate Program section of the catalog.

Research fields appropriate for the transdisciplinary cybersecurity candidate include attack and defense, communications security, computer security, cyberprivacy, cybersecurity data science, cybersecurity policy, cyberspace security, electronic warfare, enterprise-wide cybersecurity, forensics, incident response, information assurance, hardware security, network security, psychology of cybersecurity, reverse engineering, threat analysis, and vulnerability analysis. Transdisciplinary projects integrating theory, metrics, and methods from multiple disciplines are strongly encouraged.

PhD Degree Minimum Requirements Summary

- A minimum of 68 credits total.
- Up to 30 graded credit hours from an appropriate master’s degree, excluding research credits, may be included.
- 44 hours of graded coursework approved by the student’s advisory committee must include:
    - All core courses listed above (18 cr)
    - 9 credits of technical electives
    - 12 credits of cybersecurity area courses
    - Up to 12 graded research credits (CYBS 581) may be used toward the required graded coursework credits.
- Dissertation (24 credit hours): CYBS 595

Qualifying Examination

The paper critique is the program's qualifying examination. The critique is the first examination that a PhD student must pass within 24 months of enrolling in the program. The paper for critique must be agreed on by the doctoral committee. The student must conduct a successful written and public oral critique of a paper published in a high-quality professional journal on a cybersecurity topic. During the paper critique presentation, the student may be asked questions relating to background knowledge gained from taking regular coursework in cybersecurity subjects. The paper critique must be completed within 24 months of enrolling in the PhD program. The committee may determine that the

student has a pass, a conditional pass, or a fail on the critique. Students with an unconditional pass proceed to the dissertation proposal. Students with a conditional pass, will be required to overcome deficiencies, which may require additional courses, individual reading/research, and/or a subsequent critique before advancing to the dissertation proposal. Students who fail to pass the critique will be dismissed from the program. The committee will document the outcome of the critique and the reasons for its decision with a copy sent to the student, the program chair, and the Center for Graduate Studies.

Dissertation Proposal (Candidacy Exam)

The dissertation proposal is the program's candidacy examination, which cannot be done before the qualifying exam has been passed without condition or the conditions have been met. The student must write a research proposal and defend that proposal in a public oral defense at a minimum of two full semesters before the final dissertation defense. The proposal must include the rationale for the research, the preliminary research that has been done, and the plan for completion. The committee may determine that the student has a pass, a conditional pass, or a fail on the dissertation proposal. Students with an unconditional pass will be recommended for candidacy beginning in the subsequent semester, when they may register for dissertation credits. Students with a conditional pass, will be required to overcome deficiencies, which may require additional courses, individual reading/research, and/or a subsequent dissertation proposal before advancing to candidacy. Students who fail to pass the dissertation proposal will be dismissed from the program. The committee will document the outcome of the dissertation proposal and the reasons for its decision with a copy sent to the student, the program chair, and the Center for Graduate Studies.

Dissertation

Students may proceed with dissertation research after advancing to candidacy. Students must enroll in a minimum of 24 credits of dissertation (CYBS 595). Students should be aware that research typically takes significantly longer than two semesters and should plan accordingly. During dissertation registration, the student completes the research project approved by the committee via the dissertation proposal approval process. The dissertation is the documentation of research that advances the state of the science for transdisciplinary cybersecurity.

The student must write a dissertation and defend it in a public oral defense. The committee may determine that the student has a pass, a conditional pass, or a fail on the dissertation defense. Students with an unconditional pass will graduate with the doctoral degree. Students with a conditional pass, will be required to overcome deficiencies, which may require research and/or a subsequent public dissertation defense before graduation. Students who fail to pass the dissertation defense will be dismissed from the program. The committee will document the outcome of the dissertation defense and the reasons for its decision with a copy sent to the student, the program chair, and the Center for Graduate Studies.

Publication Requirement

Students are required to publish a minimum of three high-quality papers in reputable, refereed journals or conference proceedings. The journals and conferences selected must be approved in writing by the committee, which will be documented with a copy sent to the student, the program chair, and the Center for Graduate Studies. At least one paper must be published after the dissertation proposal defense; others may be published on work completed earlier in the program, but that work must be an integral part of the final dissertation.

Admission Requirements

Completion of a bachelor's degree in a relevant field (e.g., information technology, computer science, electrical engineering, mathematics, etc.) or the expectation of completing such a degree before the beginning of the first semester of graduate study. Students are expected to have competencies in mathematics equivalent to those required for completion of a B.S. degree at New Mexico Tech. Students who are deficient in mathematics will be required by their advisory committee to complete undergraduate coursework in the area of deficiency. Students should have an academic record that indicates a good potential for success in a graduate program. An undergraduate GPA of 3.0 or higher is used as a general guideline in New Mexico Tech's Graduate School.

Transdisciplinary Cybersecurity Courses:

The Transdisciplinary Cybersecurity Programs encourage students from other majors to take transdisciplinary cybersecurity courses. Students from other disciplines who are interested in taking these courses should inquire at the Cybersecurity Center's offices or contact any member of the program's faculty.

CYBS 500 Directed Research, cr to be arranged
Prerequisite: Graduate standing or consent of instructor and advisor

Offered both Spring and Fall semester. Credits cannot be applied towards the credit hours required for graduation. Research under the guidance of a CYBS faculty member.

CYBS 502 Cybersecurity Ethics and Law, 3 cr, 3 cl hrs
Prerequisite: Graduate standing or consent of instructor and advisor

A cybersecurity ethics and law course in which students learn standards of professional, ethical behavior in cybersecurity fields by examining case studies, ethical questions, and legal debates from the history of computing and cybersecurity.

CYBS 503 Cybersecurity Policy, 3 cr, 3 cl hrs
Prerequisite: CYBS 502 and Graduate standing or consent of instructor and advisor

A cybersecurity policy course that uses laws and standards to guide organizational policy development to secure information technology resources, without needlessly limiting technical responses, and analyzes both the outcomes of and processes for establishing those laws and standards.

CYBS 504 Psychology of Cyber, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

A psychology of cybersecurity course that addresses psychology issues from how humans respond to instructions and policies and to how differently hackers and defenders think.

CYBS 505 Data Science for Cyber, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

Data assembly, exploration, analysis, visualization, and inference. Python libraries such as NumPy, Pandas, and scikit-learn. Students are expected to explore problems related to cybersecurity threats, risks, and incidents that are important for businesses to become safer and less vulnerable to cyberattacks. Students must communicate and present their findings and results. Every student must complete at least one hands-on project. Prior knowledge of probability and statistics at the undergraduate level is assumed. Assumes experience with programming; experience with Python is recommended.

CYBS 509 Systems Decision and Risk Analysis, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

An advanced treatment on major topics involved in modern engineering decision-making and risk management: fundamental statistics/probability/economics theoretical prelims for decision theory; multicriteria decision-making and decision making under uncertainty; game theory and its applications; decision making processes and risk evaluation; and an introduction to Monte Carlo and Markov decision processes. Requires cybersecurity research paper. Prior knowledge of probability and statistics at the undergraduate level is assumed. (Shares lectures with EMGT 509.)

CYBS 506 Cyber Physical System Security, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

In this course we investigate security threats and countermeasures for cyber physical systems (CPS). Many of our critical infrastructure is built around CPS and as such they become targets for security attacks. The course will focus on attacks that target confidentiality, integrity and/or availability of CPS and how to mitigate them. Sample topics include but are not limited to network attacks, wireless/GPS exploitation, jamming and spoofing, and risk identification and management.

CYBS 514 Computer Security and Incident Response, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

This course covers what computer security incidents are and how to respond to an incident. Computer security incident case studies serve as the backbone of the course allowing students to analyze these case studies and determine how they were handled through process and technical analysis. Topics covered are data sources for incident detection and response, incident data analysis and incident remediation. Analysis areas covered are network event analysis, malware analysis and computer forensics for computer security incidents.

CYBS 515 Reverse Engineering Malware, 3 cr, 3 cl hrs

Prerequisite: CYBS 514 and Graduate standing or consent of instructor and advisor

Introduction to software reverse engineering of malicious software. Quick triage, static and dynamic analysis, string analysis, and deobfuscation analysis techniques. Intel x86 assembly, covering both 32 and 64-bit, Windows and Linux OS internals, will be discussed. Safe detonation using Cuckoo Sandbox, automated unpacking techniques. Detailed analysis and investigation of nation-state malware. Ghidra, FLARE VM, and other tools will be discussed.

CYBS 541 Advanced Cryptography, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

This course provides an overview of modern cryptographic theory and techniques, mainly focusing on their application into real systems. Topics include number theory, probability and information theory, computation complexity, symmetric and asymmetric cryptosystems, one-way functions, block and stream ciphers, Kerberos authentication systems, public key infrastructure (PKI), secure socket layer/transport layer security (SSL/TLS), and cryptographic protocols/applications in many real systems. **(Same as CSE 541.)**

CYBS 554 Computer Network Security, 3 cr, 3 cl hrs

Prerequisite: CYBS 561 with a grade of C or higher, or consent of instructor and advisor

This course will explore each layer of the internet protocol stack, focusing on security deficiencies, and remedies to those security deficiencies, and will involve extensive lab exercises using the DeterLab shared testbed (accessed via the Internet to enable distance education participants). It will study computer network security architecture and security mechanisms to protect against sophisticated adversarial attacks. This course reviews cryptographic primitives that underlie most network security mechanisms, then applies this understanding to network services proving authentication for data and transaction integrity and availability, and encryption for confidentiality. It also covers the integration of security services into network applications and utilities including secure mail, secure web services, secure wireless, and investigates system security issues such as for firewalls and intrusion detections systems. **(Same as CSE 554.)**

CYBS 557 Hardware-Based Network Security for the Internet of Things (IoT), 3 cr, 3 cl hrs

Prerequisite: CYBS 561 and CYBS 554, each with a grade of C or higher, or consent of instructor and advisor

This course will cover networking protocols, cryptography, and network security from the hardware implementation perspective. Topics include security

of ND, NAT, IPSEC and other specialized IPv6 protocols in support of IoT functionality. The focus will be on implementation of security policy enforcement mechanisms in IPv6 network protocols in a Field Programmable Gate Array (FPGA) platform to protect an IoT application against sophisticated adversaries. Lab exercises using a FPGA platform will enable investigation of hardware-based security technologies such as the use of Physically Unclonable Functions that are not otherwise accessible from software. **(Same as CSE 557.)**

CYBS 561 Foundations of Cybersecurity, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

This course will explore the ideas, literature, and worked examples that established the foundations of information security. The course introduces the concept of the Information Domain as the fundamental primitive that is the axis for introducing the policy requirements of Confidentially, Integrity and Availability that motivate the need for Information Security. The concept of the 225 reference monitor is the organizing principle for the course. The examination of foundational literature starts with appears and ideas that first appeared in the mid 1960's and spans the time of tremendous creativity up through the following four decades. **(Same as CSE 561.)**

CYBS 563 Access Control and System Security, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

Topics include theoretical foundations for access control, formal access control models, access control mechanisms, tools and techniques, information flow policy, trust management, security architectures, and current issues of advanced research in access control. In addition, the protection mechanisms of general-purpose operating systems, software systems, and web applications are discussed. **(Same as CSE 563.)**

CYBS 564 Secure Systems Administration, 3 cr, 3 cl hrs

Prerequisite: CYBS 561 and CYBS 554, each with a grade of C or higher, or consent of instructor and advisor

This course is primarily a Laboratory based course. The intention of the course is to give the students an experience of administering an IT system for a hypothetical business with the IT system experiencing increasingly aggressively sophisticated cyber-attacks. They are expected to build a business plan for the hypothetical business, a policy-based IT protection plan that they then implement on the host machines and networks in the laboratory. Simultaneously the adversary builds an exploitation plan that attempts to defeat the business's IT protection implementation and is able to achieve his/her exploitation objectives. The adversary has access to any/all exploit technology available, but there is a moderating factor of cost associated with the exploitation technology. The defenders have access to protection technology, but again there is a mitigating cost factor associated with the protection technology. The objective of the class is to experience and learn the capabilities an effectiveness of both defensive and exploitative technology with an appreciation of the need for policy and planning that directs, supports, and constrains the actions of both sets of actors. This course is not offered via Distance Education. **(Same as CSE 564.)**

CYBS 581 Directed Study, cr to be arranged

Prerequisite: Consent of graduate advisor

CYBS 589 Special Topics in Cybersecurity, 3 cr, 3 cl hrs

Prerequisite: Graduate standing or consent of instructor and advisor

Graduate special topics in computer science. For a list of offerings, please visit banweb.nmt.edu.

CYBS 590 Independent Study, cr to be arranged

Prerequisite: Consent of graduate advisor

Independent research supervised by a faculty member. It is expected that this work will culminate in a paper to be published, and an oral presentation is required.

CYBS 591 Thesis (MS Program), cr to be arranged

Prerequisite: Consent of graduate advisor

CYBS 595 Dissertation, cr to be arranged

Prerequisites: Documentation of successful completion of PhD candidacy exam and Academic Advisor recommendation for candidacy.

Faculty Research Interests

B. Burnham – Foundations of Cybersecurity, Policy
T. Dotson – Organizational High Reliability, User Experience Research Methods
T. Elliott – User Experience Research Methods, Psycolinguistics, Perception.
A. El Osery – Cyber Physical Systems
A. Ghosh - Health Systems, Health Sensing, and Health Monitoring for Naval and Weapons Systems
C. ChoGlueck - Ethics, Values and Norms Impact on Laws and Regulations, Science, Technology Policy
N. Kelly – Hacker Culture and History, Cybersecurity History
C. Jeffery – Program Execution Monitoring, Programming Language Support
K. Lee – Multi-Robot Systems
L. Liebrock – Cybersecurity, Cybersecurity Auditing, Enterprise-wide Forensics, Parallel Processing, Security Metrics, Threat Intelligence, Visualization, Well Posedness
B. Majumdar – Additive Manufacturing
S. Mazumdar – Data Management, Data Science, Information Privacy
L. Pierson – Network Security, Hardware Security Design, Formal Security Methods, Cryptographic Policy Enforcement Mechanisms
D. Quist – Malware, Reverse Engineering
R. Ramyaa – Artificial Intelligence
D. Shin – System Security, Software Engineering/Security, Usable Security
S. Shao – Secured Optical Links in Heterogeneous Wireless Networks
H. Soliman –Machine Learning
S. Teare - Encryption, Smart Instrumentation, Cyber Physical Systems
K. Tietjen – Incident Response and Digital Forensics, Threat Intelligence, Data Science Focused on Threat Detection and Response, Cyber Operations Process Engineering/Quality Management
J. Tong – Network Security
H. Wang – Risk Analysis, Agricultural Supply Chain, Financial Crime, Online Fraud
J. Zheng – Cybersecurity, Machine Learning, Mobile Computing, Networking, Smart Grids, Intelligent Manufacturing, Smart Agriculture