NATIONAL SECURITY STUDIES

Professional Studies Building, Room 449
201-200-2275

The National Security Studies Department (https://www.njcu.edu/academics/schools-colleges/college-professional-studies/departments/professional-security-studies/) focuses on a student-centered, scholar-practitioner approach to education. Its mission is to facilitate access, create opportunities and provide a supportive environment for achieving academic success, learning and appreciation of subject matter, professional and personal growth, and the acquisition and development of identified and marketable global and disciplinary competencies. The Department's vision is to create a diversified, current, innovative, successful and exemplary program that will integrate both theory and practice through the knowledge, skills, and abilities that will enable students to be globally competitive in the field and discipline of national security.

The National Security Studies Department is one of only a few departments in the country recognized as a Center of Academic Excellence (CAE) in both cybersecurity and intelligence. We have maintained our cybersecurity excellence award from the National Security Agency (NSA) for years at both the graduate and undergraduate levels. In 2019 the department was awarded a second CAE, in intelligence, from the Defense Intelligence Agency (DIA) and the Office of the Director of National Intelligence (ODNI). These awards help our students in the job market and demonstrate our ongoing ability to provide an award-winning education at an affordable price.

All faculty are current practitioners and have distinguished careers in the many and diverse fields of national security. For details on our faculty, please visit the department's faculty page (https://www.njcu.edu/academics/schools-colleges/college-professional-studies/departments/professional-security-studies/professional-security-studies-faculty/).

This National Security Studies degree program is designed for practicing security leaders, as well as those students who seek careers in national, corporate or information assurance/cyber security. All course work is offered on campus, at our satellite program at Wall, NJ, through our University Partnerships, at Middlesex County Community College, at Bergen County Community College, in web-enhanced format, and online. We are adding new locations across the state. For the latest info, please see the department's web page (https://www.njcu.edu/academics/schools-colleges/college-professional-studies/departments/professional-security-studies/).

All National Security Studies majors who qualify are be eligible for NJCU's Cooperative Education Program. A major objective of this program is to combine classroom education with practical experience, which provides a realistic, in-the-field environment for knowledge, skills, and abilities that supplement classroom learning. Students may earn up to 12 credits in Cooperative Education, with a maximum of 6 credits in any one experience.

Abdullah Al-hayajneh, Co-Chairperson
Assistant Professor of Cybersecurity

Michael Krantz, Co-Chairperson and Coordinator - Middlesex Campus
Professor of National Security Studies
Rutgers University, B.A., Seton Hall University, M.A., Ph.D.

Richard J. Cosgrove, Coordinator - Wall Campus
Associate Professor of National Security Studies
New Jersey City University, B.A.; Seton Hall University, M.A., Ed.S., Ed.D.

Kathleen Rennie (krennie@njcu.edu)
Associate Professor of Marketing
Rutgers University, B.A.; Seton Hall University, M.A., Ph.D.

Juste Codjo, DSc Program Coordinator
Assistant Professor of National Security Studies
Université d'Abomey-Calavi (Benin), B.A.; Webster University, M.A.; U.S. Army Command and General Staff College, Graduate Certificate; Kansas State University, Ph.D.

Kutub Thakur, Cyber Defense & Security Program Director
(kthakur@njcu.edu)

Assistant Professor of National Security Studies
New York Institute of Technology, B.S., University of Wisconsin - Platteville, M.S., M.P.M. Certificate; Pace University, Ph.D.

Laszlo Molnar, Graduate Program Coordinator
Associate Professor of National Security Studies
Budapest University of Economic Sciences (Hungary), M.A. & Ph.D.; Fletcher School of Law and Diplomacy, Tufts University & J. F. Kennedy School of Government, Harvard University - post-doctoral studies, special student and visiting scholar.

Michael Wiltsey
Associate Professor of National Security Studies
Monmouth University, B.A.; John Jay College of Criminal Justice, M.A.; Drexel University, Ph.D.

Abdullah Al-hayajneh (aalhayajneh@njcu.edu)
Assistant Professor of National Security Studies
Ahliyya Amman University, B.S.; New York Institute of Technology, M.S.; Capitol Technology University, Ph.D.

Jonathan Rosen
Assistant Professor of National Security Studies
Columbia University, Ph.D.

Various discipline-specific concentrations that will prepare students for multiple fields of employment or areas of additional undergraduate/graduate study are noted below. Course requirements for each concentration are explained in detail. The requirements for graduation, in addition to completion of the major area, are listed on "Undergraduate Degree Requirements (https://catalog.njcu.edu/undergraduate/undergraduate-degree-requirements/)."

- National Security Studies, B.S. (https://catalog.njcu.edu/undergraduate/professional-studies/security-studies/national-security-studies-bs/)
- National Security Studies, Minor (https://catalog.njcu.edu/undergraduate/professional-studies/security-studies/national-security-studies-minor/)
- Cyber Defense, Certificate (https://catalog.njcu.edu/undergraduate/professional-studies/security-studies/cyber-defense--certificate/)
- Cybersecurity, B.S. (https://catalog.njcu.edu/undergraduate/professional-studies/security-studies/cybersecurity-bs/)

- Information Security (INFOSEC) - Standard 4011, Certificate (https://catalog.njcu.edu/undergraduate/professional-studies/security-studies/information-security-certificate/)
- Military Science, Minor (https://catalog.njcu.edu/undergraduate/professional-studies/security-studies/military-science-minor/)

Professional Security (SECU)

SECU 1XX Professional Security Transfer Credit (0 Credits)

SECU 2XX Professional Security Transfer Credit (0 Credits)

SECU 150 Introduction to Security (3 Credits)
This introductory course provides an overview of the principles and problems of effective security enforcement. An analysis is made of the security officer's role in the organization served, the procedures and regulations which govern that role and the laws as they relate to the rights of citizens. The organization and administration of the security department are stressed.

SECU 151 Security Systems & Design (3 Credits)
Detailed examination into the administrative planning of security activities, requirements for their effective execution and the supportive equipment and physical layout design for maintaining an effective security system are conducted in this course.

SECU 152 Loss Prevention Technique (3 Credits)
This course stresses individual research in all aspects of loss prevention situations. Students are required to develop security systems that reflect new techniques and concepts. The case study method is employed.

SECU 153 Occupational Safety and Health (3 Credits)
Management and supervisory principles and basic concepts in occupational safety and health are introduced in this course.

SECU 154 Careers in Professional Security Studies (3 Credits)
Course focuses on the many and varied career opportunities in the field of professional security studies. In addition to researching and understanding the requirements for these positions, the application, interviewing process and the preparation of a professional resume and/or curriculum vita will be emphasized.
Pre-Requisite: Secu 150 Introduction To Security

SECU 155 Introduction to International Security (3 Credits)
This course introduces theories and problems in international security and applies them to current events. Topics include the causes and ethics of war, security policy decisions, balancing offense and defense, and threats from non-state actors, such as terrorists.

SECU 190 Microcomputers for the Professional (3 Credits)
This course uniquely affords undergraduate students to learn about microcomputers with colleagues in different professional majors or minors: business, fire science, health, nursing, criminal justice and security. Students can expect hands-on use of microcomputers in the on-campus labs. Topics include cybernetic literacy, ethics, electronic research, constructive, and cognitive development.
Pre-Requisite(s): INTD 120 Computer as a Tool

SECU 210 Introduction to Intelligence (3 Credits)
This course covers the history and evolution of intelligence, covering areas that include principles and processes, ethics, and how it is used in a national security setting. Students will develop knowledge of the use and practices of intelligence with respect to homeland and national security interests.
Pre-Requisite: SECU 150 Introduction to Security

SECU 214 Crime Scene Investigation (3 Credits)
This course will review basic and advanced procedures of crime scene investigation. Students will learn the procedures for documenting crime scenes. The course will also cover the proper search techniques, documentation, and collection of evidence. The course will also introduce students to fingerprint examination, bloodstain pattern analysis, and crime-scene reconstruction.

SECU 215 Behavioral Analysis and Criminal Profiling (3 Credits)
This course will explore a comprehensive approach to behavioral analysis and criminal profiling. It will examine the foundations and methods of profiling and application of such methods to the investigation of various crimes or threats. The course will also address the application of behavioral analysis to our understanding of terrorism.
Prerequisite: SECU 150 Introduction to Security

SECU 220 Current Security Problems (3 Credits)
This course analyzes special problem areas in national and industrial security. The focus is on security education and training, community relations, white collar crime, subversion and sabotage, civil disturbance, and emergency and disaster control.

SECU 221 Contemporary International Security Topics (3 Credits)
This course applies the theories and lessons from international security to new and emerging threats, risks, and sources of conflict and cooperation including terrorism, human security, climate changes, and cyberspace. Students learn security responses ranging from policy development to kinetic operations.
Pre-Requisite(s): SECU 155 Introduction to International Security

SECU 222 Computer Security I (3 Credits)
This introductory course focuses on the importance of information security and the impact technology has in the field of security. Specific areas of coverage include: history vs. current methodology, capabilities and limitations of communications; automated information systems (AIS); hardware; software; memory; media; networks; system operating environment and security policies.

SECU 224 Ethics in National Security (3 Credits)
This course examines how ethical standards apply to human relations and the specific implications for national Security professionals. It combines lectures, case studies, and discussions to critically analyze the impact of ethical behavior and conduct in support of national security objectives.
Pre-Requisite: SECU 150 Introduction to Security

SECU 226 Critical Thinking and Problem Solving for Professionals (3 Credits)
This course introduces students to the problem solving process, focusing on mastering the skills that enable them to make critical decisions in a variety of contexts. Operating in a collaborative environment that focuses on problem based learning: students establish and work within groups that will utilize strategies for identifying ROOT problems, generating alternatives or solutions, implementing a chosen solution, and evaluating the outcome. Students will discuss issues of group interaction as well as the importance of working within a group and as an individual.

SECU 250 Security Communication (3 Credits)
Effective communication about issues related to security with internal and external in a global society where information is shared instantaneously requires strategic planning and careful attention to messaging. Best practices are examined regarding proactive and reactive strategic communication, with an emphasis on communication research, objectives, programming and evaluation.
Pre-Requisite(s): SECU 150

SECU 280 Security Organization & Administration (3 Credits)
This course is designed as an introduction to the organization and administration of security functions within a corporation, company or municipality. Topics such as administrative procedures and corporate management philosophy are examined.

SECU 305 Special Topics in Professional Security Studies (3 Credits)
This course covers selected topics in Professional Security Studies that are of recent or current interest in the field. Topics are selected from the three major domains of this department to include National, Corporate or Information Assurance/Cyber Security.
Pre-Requisite(s): SECU 150

SECU 306 U.S. Security Interests East Asia (3 Credits)
Events in East Asia often grab headlines: North Korean nuclear weapons, Chinese hacking, tensions in Korea, Japan-China disputes, and rival claims across the Taiwan Strait. This course familiarizes students with one of the world's most dynamic regions, then harnesses that knowledge to assess U.S. security interests throughout East Asia.

SECU 309 Introduction to Computer & Network Security (3 Credits)
This course covers network security for the Cybersecurity Program. It will introduce network and internet terminology in information security,information assurance and related legal and ethical issues. The topics span various cybersecurity domains including TCP/IP general concepts, OS identification, scanning, web servers and wireless assets vulnerabilities, cryptography, and network protection.

SECU 310 Forensic Investigations (3 Credits)
This course provides an overview of forensic investigations that covers the three major domains in Professional Security Studies-National, Corporate and Information Assurance/Cyber Security . Students will be introduced to the various forensic investigations involved within these three areas.
Pre-Requisite(s): SECU 150 Introduction to Security

SECU 311 Bloodstain Pattern Analysis (3 Credits)
This course will explore the history of bloodstain pattern analysis in criminal investigations. Students will learn basic pattern interpretation and conduct experimentation to solidify their learning. Students will learn the methods for determining impact angles, direction of travel, as well as areas of convergence and origin of impact spatter patterns.

SECU 315 Big Data Analysis and Visualization in U.S. National Security (3 Credits)
The ability to collect, analyze, and produce visualizations of big data is a critical (and employable!) national security skill set. Using available datasets from the FBI, START/DHS, social media, and elsewhere, students will conduct and present policy relevant national security research using industry leading data visualization software.

SECU 321 Seminar on National Security (3 Credits)
National Security, the protection of American interests impacts many facets of our society. The role of the U.S. homeland security and intelligence communities are comprehensively investigated as they pertain to the interdisciplinary responsibilities of security professionals. This seminar is based on intensive study that supports other security courses with research.
Pre-Requisite(s): SECU 150

SECU 322 Computer Security II (3 Credits)
This intermediate course focuses on the importance of information security (INFOSEC) and the impact technology has in the field of security. Specific areas of coverage include: Operational Security (OPSEC), policy, roles and responsibilities, cryptography, transmission security, and components of the National Training Standard for Information System Security-(NSTISS). Components include: national policy, threats, countermeasures and risk management among others.
Pre-Requisite(s): SECU 222 Computer Science I

SECU 323 Risk Management (3 Credits)
Course focuses on the management and mitigation of risk in security settings. Critical incident response, risk assessment, and the development of security surveys, identifying risks and offering solutions will be emphasized and applied to the three major domains of national, corporate and cyber security within the security industry.
Pre-Requisite(s): CJS 150

SECU 324 Security Fraud (3 Credits)
Fraud in the security industry will be the focus of this course as it applies to national and corporate security organizations. This course will emphasize forensic accounting techniques and methods to identify fraud as well as prevention techniques. Those in traditional law enforcement, and business will benefit from the knowledge gained through this course.
Pre-Requisite(s): CJS 150 Introduction to Security

SECU 326 Public Speaking for Professionals (3 Credits)
Designed to help students improve oral communication, articulation and presentation skills. Emphasis is placed on identifying effective speech habits, techniques for improving speech; oral interpretation; effective speech planning and delivery; and interpersonal communication.

SECU 339 Cyber Incident Handling (3 Credits)
This course presents techniques for identifying vulnerabilities within computer systems and explains how to mitigate risks and damage. The content covers various aspects of contingency planning while highlighting effective strategies that minimize downtime in a computer system emergency. This course also demonstrates how to recover from losses after a breach, making it a valued resource in case of a network intrusion.

SECU 340 Ethical Hacking I (3 Credits)
This course immerse students into an interactive environment where they are shown how to scan, test, hack and secure their own Cyber systems. A self-contained lab gives each student in-depth knowledge and experience on how defenses work and then lead into attacking their own networks; no real network is harmed.
Pre-Requisite(s): SECU 222 or Permission of Instructor

SECU 345 Computer Forensics I (3 Credits)
Digital forensics are a standard component of today's investigation techniques for National, Corporate and Cyber Security. This course deals with the preservation, identification and reconstruction, extraction, documentation, reporting, acquisition, analysis, interpretation and reconstruction of computer data. Topics covered include evidence handling, chain of custody, collection, preservation, identification and recovery of computer data.
Pre-Requisite(s): SECU 222 or Permission of Instructor

SECU 350 Intelligence Analysis (3 Credits)
This course will provide students with the fundamental concepts of intelligence analysis, which will cover the intelligence process; defining the intelligence problem; an analysis approach to the target; the analytical spectrum; models and sources of intelligence; populating models; collection strategies; predictive analysis; organizational analysis; technology assessment and systems analysis and the analyst and the consumer/recipient of intelligence.
Pre-Requisite(s): SECU 150

SECU 380 Policy Development for the Security Professional (3 Credits)
This course examines policy making and the analytical process used to develop and implement them. This course studies the impact of policy decisions at various levels on the operations of Security organizations. Security policy is presented as the link between Security systems and people.
Pre-Requisite(s): SECU 150 Introduction to Security

SECU 398 Research Methods in Professional Security Studies (3 Credits)
Introduction and practice in the use of primary sources, including the basic methodologies and techniques of research design within the field of Professional Security Studies. Students will gain experience in the development of research proposals and in the use and verification of different types of empirical evidence. Consistent with the environment of Professional Security in the 21st Century, use of electronic databases, computers and technology are emphasized throughout.
Pre-Requisite: SECU 150 Introduction to Security

SECU 400 Cybersecurity and Event Management (3 Credits)
The Cybersecurity and Event Management course explores the technology, operational procedures, and management practices needed for successful cybersecurity. Cybersecurity and Event Management is a comprehensive course covering the extensive use of standards and best practices that are often used to guide or mandate cybersecurity implementation. The course enables students to define cybersecurity governance, assess risks, and manage strategy and tactics.

SECU 411 Extremist Groups and Security (3 Credits)
Understanding the motivation, tactics, and targeting trends of extremist groups is mandatory if managers and command staff are able to evaluate potential threats and develop appropriate countermeasures to protect the organization's personnel and other assets. Students discuss terrorism as a form of political violence and its effect on security management.
Pre-requisite: CJS 150 Introduction to Security

SECU 415 Intrusion Detection and Prevention Systems (3 Credits)
The Intrusion Detection and Prevention course is designed to provide knowledge in the area of intrusion detection and incident response once an intrusion has been detected. Topics covered in this course include computer security, computer network exploitation, intrusion detection, incident handling, hacker exploits, hacker tools and cybercrime investigative techniques.

SECU 422 Computer Security III (3 Credits)
This capstone course focuses on the importance of information security (INFOSEC) and the impact technology has in the field of security. Major domains covered are National Training Standard for Information Systems Security-(NSTISS) planning/management/ and policies/ procedures. Specific topics include: security planning, risk management, systems lifecycle management, contingency planning/disaster recovery, physical security measures, personal security practices and procedures, software security, network security, administrative controls, auditing, cryptosecurity, key management, transmission and TEMPEST security.
Pre-Requisite(s): SECU 322

SECU 430 Computer Hacking Forensic Investigator (3 Credits)
The Computer Hacking Forensic Investigator course will explore the technologies associated with the security discipline of digital forensics. CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students to acquire hands-on experience with forensic investigation techniques and forensic tools necessary to successfully carry out a computer forensic investigation.

SECU 465 Resource Manangement in Security (3 Credits)
This course explores the major issues of financial and human resource management, and combines theories with practical applications to emphasize current best practices. The first half of the course focuses on the fundamentals of human resource management, while the remaining half focuses on budgeting and financial management.
Pre-Requisite(s): CJS 150

SECU 1305 Special Topics: Intelligence Analysis and National Security (3 Credits)
This course covers selected topics in Professional Security Studies that are of recent or current interest in the field. The Intelligence Analysis and National Security topic is selected from the major domain of National Security. The other two domains of Corporate Security and Information Assurance/Cyber Security with be integrated.
Pre-Requisite(s): SECU 150

SECU 2305 Special Topics: National Security Policy (3 Credits)
This course covers selected topics in Professional Security Studies that are of recent or current interest in the field. The National Security Policy topic is selected from the major domain of National Security. The other two domains of Corporate Security and Information Assurance/Cyber Security with be integrated.
Pre-Requisite(s): SECU 150

SECU 3305 Special Topics: Executive Communications for National Security (3 Credits)
This course covers selected topics in Professional Security Studies that are of recent or current interest in the field. The Executive Communications for National Security topic is selected from the major domain of National Security. The other two domains of Corporate Security and Information Assurance/Cyber Security with be integrated.
Pre-Requisite(s): SECU 150

SECU 4305 Special Topics: Domestic Terrorism (3 Credits)
This course covers selected topics in Professional Security Studies that are of recent or current interest in the field. The Domestic Terrorism topic is selected from all three of this department's major domains: National Security, Corporate Security and Information Assurance/Cyber Security.
Pre-Requisite(s): SECU 150

SECU 5305 Special Topics: Extremist Groups (3 Credits)
This course focuses on understanding the motivation, tactics, and targeting trends of extremist groups so that security professionals are better able to evaluate potential threats and developed appropriate countermeasures to protect the organization's personnel and other assets. Students discuss terrorism and its effect on security management.
Pre-Requisite(s): SECU 150

SECU 6305 Special Topics: Critical Thinking (3 Credits)
This course examines the approaches to strategic critical decision making in contemporary national security, such as Critical Thinking and Intelligence Gathering (CTIG), Analysis of Competitive Hypothesis (ACH), and the Military Decision Making Process (MDMP). Students are immersed in field-based competency development exercises, leading to practitioner proficiency in critical thinking and problem solving.
Pre-Requisite(s): SECU 150

SECU 7305 Special Topics: Security Fraud (3 Credits)
The investigation of fraud by security professionals is the focus of this course. This course emphasizes forensic accounting techniques and methods to identify and prevent fraud.
Pre-Requisite(s): SECU 150