CYBER INITIATIVES

West Point READY

READY TO **SERVE**. READY TO **LEAD**.

Cybersecurity is critical to our national defense and prosperity. As the scope and capabilities of technology expands, so too does the need for cyber-savvy leaders with technical expertise and agility. The U.S. Army has continued to increase the size of its cyber corps and create new cyber programs; therefore, it is imperative to develop a robust pipeline of technical leaders to fill these key roles and strengthen our nation's cyber resiliency.

Every year, West Point provides the Army with approximately 1,000 second lieutenants. Approximately 40 of those officers will soon find themselves on the frontlines of cyber operations. These young leaders will be called upon to secure and defend networks against adversaries and to advance our military's strategic efforts within the realm of cyber operations. Every other graduate must also adapt to the implications of technology on their career fields. These young leaders are equally critical to the Army's success in future operations.

West Point offers a range of cyber initiatives aimed at educating and preparing cadets for these roles while simultaneously strengthening the Army's and nation's pipeline of cyber professionals. The Department of Electrical Engineering & Computer Science (EECS) leads one of West Point's essential cadet-oriented cyber initiatives: the **Cyber Team**. This team is comprised of two complimentary elements: the **Operations Team** and the **Policy Team.**

These programs advance cadets' expertise at the technical and policy levels through intercollegiate competition and invite them to pursue solutions to real-world problems. Furthermore, through these programs, cadets hone leadership and communication skills and develop relationships with prominent members of the cybersecurity community in academia, industry, and government.

Cyber Operations Team

The Cyber Operations Team is a nationally ranked team focused on developing cadets' technical expertise to attack and defend cyber networks. This team of about 20 cadets prepares for and competes in a series of prominent cybersecurity competitions throughout the year. While the Team is overseen by EECS, its cadets span academic departments, reflecting the multidisciplinary nature of cyber operations.

The Team trains twice a week and competes in about eight competitions throughout the year, including the prestigious Cybersecurity Awareness Worldwide (CSAW) Competition as well as the Cybersecurity & Infrastructure Security Agency (CISA) President's Cup, Collegiate Cyber Defense Competitions, SANS Academy Cup, and NSA Cyber Exercise, among others.

These one- to three-day competitions span the full cyber security spectrum from Defensive Cyber Operations to Offensive Cyber Operations; cadets must work as a team to effectively attack and defend network systems. In both scenarios, students conduct data forensics and analysis, effectively communicate findings, and develop software-based solutions to network attacks. In short, these competitions offer cadets the chance to practice skills that have direct applications to military cyber operations.

Cyper Policy Team

While cyber officers require technical competency, they must also understand how cyber policy fits into the larger strategic picture. The Cyber Policy Team serves to cultivate future leaders with a sophisticated understanding of cyber policy.

Similar to the Cyber Operations Team, the Cyber Policy Team is a multidisciplinary team comprised of about 20 cadets from a variety of academic departments. The Policy Team competes in six to seven competitions each year and has a history of winning and placing. The Atlantic Council's Cyber 9/12 Challenges serve as the foundation of the competition schedule. This series of competitions brings together students from around the world to compete in developing effective responses to policy scenarios related to a national and/or international cybersecurity crisis. Other competitions include the NYU Cybersecurity Awareness Worldwide (CSAW) Policy competition and the WMGIC x NATO Countering Disinformation Challenge.

Whereas the Operations Team focuses on the technical applications of cyber warfare, the Policy Team focuses on legal and policy implications. For the Cyber 9/12 Strategy Challenges, the Cyber Policy Team works together to research and develop a security briefing related to the crisis scenario. Once students arrive at the three-day competition, they present their briefing to a panel of subject matter experts and respond to questions. Cadets are then challenged to adapt their recommendations as the policy situation evolves. Through this rigorous competition, cadets gain invaluable experience in developing and communicating cyber-related policies and strategies. They also develop their professional network through interactions with teams, judges, and subject matter experts.

Photo: Lee Ross '73

FUNDING OPPORTUNITIES

Cyber Initiatives Endowment & Fund ..... **$4.5 million**

Competition Travel	$1.75 million endowment/$70,000 annual
Collegiate	$450,000 endowment/$18,000 annual
Domestic	$550,000 endowment/$22,000 annual
International	$750,000 endowment/$30,000 annual
Cyber Strategy Challenge Initiative	$450,000 endowment/$18,000 annual
Cadet Scenario Training	$150,000 endowment/$6,000 annual
Cadet Research	$150,000 endowment/$6,000 annual
Coach's Research & Training	$150,000 endowment/$6,000 annual
National Security Agency Cyber Exercise *(under consideration)*	$300,000 endowment/$12,000 annual
Cadet Cyber Operations Team Naming	$1 million
Cadet Competitive Cyber Policy Team Naming	$1 million

MARGIN OF EXCELLENCE

James Brandenburg | West Point Association of Graduates
698 Mills Road, West Point, NY 10996
Phone 845.446.1592
WestPointAOG.org

as of April 1, 2024