CENTER FOR CIVIL-MILITARY RELATIONS

Naval Postgraduate School
1635 Cunningham Road (Bldg. 259)
Monterey, CA 93943-5011

T +1.831.656.3171
F +1.831.656.3351
ccmrinfo@nps.edu
www.ccmr.org

Cybersecurity Policy and Practice
(MASL #P309370)

The Center for Civil-Military Relations (CCMR) offers a one-week seminar entitled "Cybersecurity Policy and Practice" for nations that are interested in developing capabilities to defend cyberspace. National security and economic prosperity are threatened daily through exploitation, intrusion or attack in cyberspace by criminal, transnational or regional competitors. This offering prepares decision-makers to effectively consider, design and implement policies and practices for safeguarding unfettered access to and use of cyberspace.

The key objectives of the seminar are to familiarize participants with:

- Trends, contexts, and implications of persistent cyber threats
- Roles, authorities, dependencies and vulnerabilities for cyberspace
- Commercial sector, civil agency, and military department cooperation mechanisms

In an effort to build capacity for economic growth and innovation, participants will explore policies and practices for maintaining advantage over competitors that seek to exploit, disrupt, deny, and degrade the networks and systems our societies and militaries depend upon. They will examine barriers to effective policy and practice development and ways to respond using a comprehensive approach for cybersecurity.

The seminar will offer a menu of congruent topics for selection by the nation to include:

- Policy aspects for a unique and ubiquitous domain, such as international regimes and norms, domestic regulatory structures, cyberspace deterrence, and cyberweapons control.
- Practices to enhance partner capabilities, such as security management, risk management, work force development, public-private partnerships, and interagency exercises.

The delivery format combines informational presentations on academic and practical frameworks with a capabilities based assessment of collective capacity to counter cyber threats in a notional scenario. The participants will learn how to identify and field capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance.

This event is delivered in partnership with the National Cybersecurity and Communications Integration Center, Air Force Institute of Technology, Air Force Research Institute, and with representatives from select International or Domestic Centers or Institutes for Cybersecurity.

Participants: The seminar is designed for senior international officials from ministries of defense, foreign affairs, and communications. Public and private sector representatives responsible for cybersecurity are welcome to attend.

Faculty Teams: consist of academic scholars, proven subject-matter experts and experienced practitioners.

Translation: course will be taught in English or be delivered with simultaneous interpretation.

Cost: Cost of the course will be roughly USD 75,000 under IMET/FMF/FMS funding depending on location.