PRACTICAL CYBER IMPLEMENTATION

RESIDENT: P170042 **MOBILE: P309370** **CERTIFICATION: PME, RDFP**

This course explores policies and practices necessary to protect and defend data, networks, systems, and platforms essential for military and security organizations and that underpin economic, social, governmental, and political activity in society. Instructors highlight the importance of civilian control throughout the cyber and MoD staff directorates, effective cybersecurity as a national security imperative, and introduce participants to cyber mission assurance, explore barriers to effective policy and practical implementation, and consider the latest practices and innovations for building cyber resilience. Monterey course iteration was conducted through P170370.

OBJECTIVES

Upon conclusion of this course, participants will be able to:

- Use frameworks/best practices, develop processes for cyber planning lines of effort for national security missions
- Identify international, national, contractual, statutory and regulatory influencers in MoD/Armed Forces Cyber
- Develop guidance including metrics, procedures and guidelines for operations, international/interagency efforts for stakeholder
- Address challenges to planning implementation when developing practices for operational use
- Create implementation plans/supporting guidance addressing MoD/Armed Forces requirements

TOPICS

The educational approach of this course combines content with practical exercises/case studies to provide the skills and knowledge needed to understand the process of cyber implementation.

- Review influencers that provide guidance and direction for MoD/Armed Forces lines of effort
- Apply implementation frameworks to for full scope joint/combined operations
- Discuss the challenges in moving from guidance to operational cyber execution
- Establish controls, metrics, and baselines to execute cyber guidance
- Develop guidance/standards for operational cyber
- Updating policies/practices to incorporate cyber innovations

- Identify decision makers, influencers, and relationships involved in shaping cyber defense planning (INPUTS)
- Developing Cyber Defense Planning and Foundational Lines of Effort (INTENT)
- Decide Foundational Cybersecurity for Mission Assurance Practices (CONTROLS & SOLUTIONS)
- Establishing Implementation Guidance (IMPLEMENTATION)
- Capstone Exercise

PARTICIPANTS

The course is for cyber defense implementation work by civilians, military officers (equivalents O-3 to general-level), government/civilian/private sectors, and technical/non-technical specialists. Cyberspace Policy/Practice Development staff; Intelligence Researchers/Operatives, Cyber Strategist/Practitioners, Budget, Human Resources and other defense planning staff should attend.

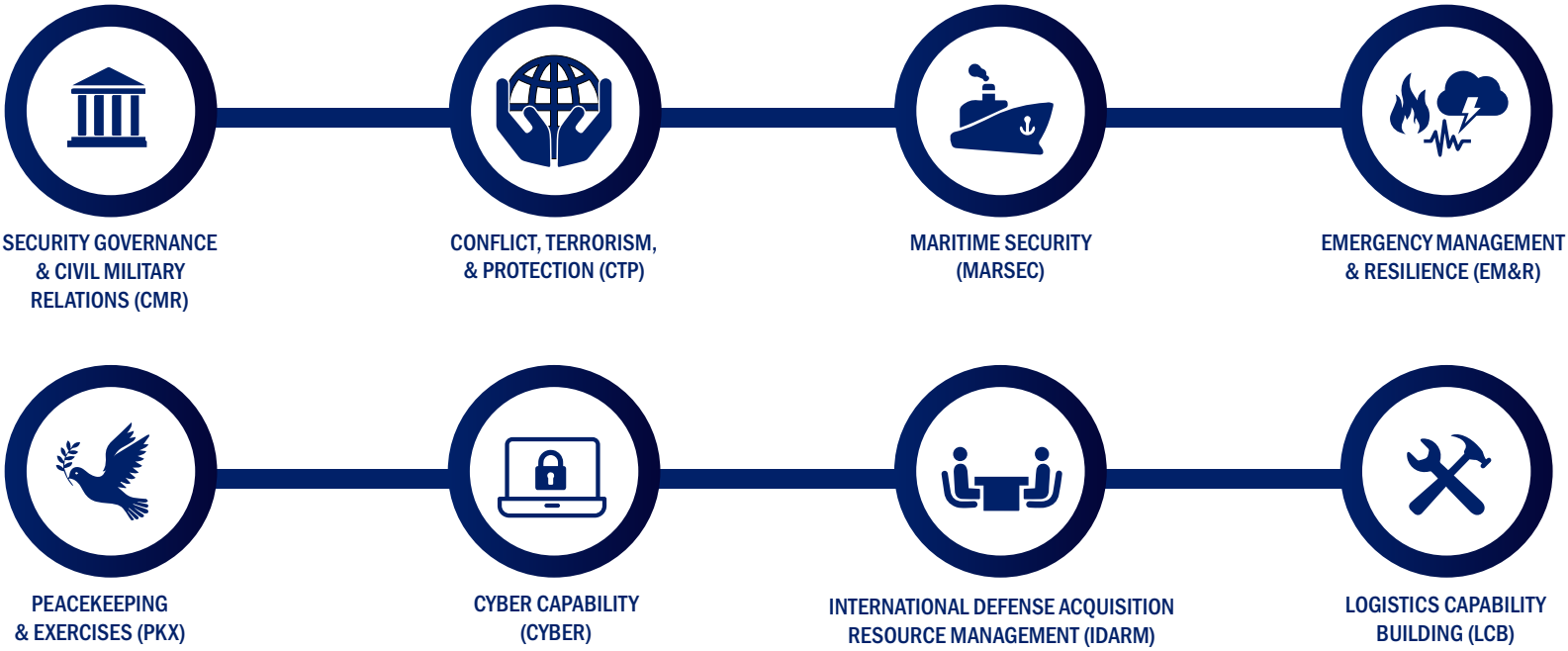
Institute for Security Governance
Naval Support Activity Monterey
1635 Cunningham Rd, Bldg 259
Monterey, CA 93943-5011

T +1 831.656.3171
F +1 831.656.3351
isginfo@nps.edu

LinkedIn
instituteforsecuritygovernance.org

ISG PROGRAM AREAS

ISG's tailored education and professional development programs support the sustainment of a comprehensive knowledge base and strengthen partner capacities to confront complex security and defense challenges. Engagements are designed to cultivate individual understanding of complex issues, foster peer-to-peer learning, and build international communities of interest.



FACULTY

ISG has a diverse faculty team grounded in professional experience from academic, military, government, and civil sectors. The core faculty are augmented by experts drawn from other parts of government, and U.S. and international subject matter experts drawn from universities, industry, think tanks, international organizations, and non-governmental organizations.

ENROLLMENT

Courses are conducted as part of the U.S. Government's Security Cooperation efforts. Interested partner nation personnel should contact their government's international cooperation section, or the relevant U.S. Embassy's security/military cooperation office for selection processes and enrollment. Interested U.S. citizens may contact ISG to discuss availability.

FUNDING

Educational programs are primarily implemented through Title 22 authorized programs (International Military Education and Training, Foreign Military Sales, Peacekeeping Operations) and various Title 10 authorized programs such as the Maritime Security Initiative (MSI) and Regional Defense Fellowship Program (RDFP).

ABOUT ISG

The Defense Security Cooperation University's (DSCU) Institute for Security Governance (ISG) is the Department of Defense's leading implementer for Institutional Capacity Building (ICB) and one of its primary international schoolhouses. As a component of the Defense Security Cooperation Agency (DSCA), ISG is charged with building partner institutional capacity and capability through tailored advising, education, and professional development programs grounded in American values and approaches.