BUILDING CAPABLE CYBERSECURITY INSTITUTIONS

THE CHALLENGE

Almost 4.6 billion people are active internet users. Online tools and platforms can be drivers of inclusive change and prosperity or destabilizing threats to privacy. Hactivists, criminals, and malign nation-states of all sizes exploit cyber vulnerabilities to compromise private data, steal intellectual property, evade sanctions, or otherwise threaten national and economic security. The effects of malicious cyber-enabled operations are not just virtual. Citizen safety and the integrity of institutions is eroding through increased cyberspace exploitation, intrusion, or disruption. Modern militaries rely on digitized critical infrastructure that may be vulnerable to cyber threats.

Securing cyberspace is fundamental to the national defense capacity of both the U.S. and its partners. Partners face a diverse range of cyberspace capacity building (CCB) challenges:

- Insufficient financial and human resources to secure and defend cyber assets
- Lack of policy and strategy for resourcing and developing cyber institutions and workforce
- No standard education and training pipeline for developing cyber workforces
- Defense institutions that do not own or control their network infrastructure and often rely on off-the-shelf commercial solutions that are not designed for warfighting
- Inability to meet cybersecurity standards required by the U.S. government for information sharing and interoperability
- Inability to guarantee protection of purchased U.S. defense platforms hosted on commercial or foreign owned information systems
- Variation in sophistication and type of cybersecurity threats across geographies
- Lack of awareness shared across the entire military force of cyber risks to operations

These conditions elevate the urgency and importance of sound policy, strategy, education, and training for CCB.

ABOUT ISG

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

This document is intended to frame the challenges, possibilities, and best practices associated with building partner nation cyber institutions, facilitating greater levels of mission assurance and interoperability with the U.S. and to highlight ISG's role as integrator, implementer, and partner within DoD's security cooperation community.

BUILDING CAPABLE CYBERSECURITY INSTITUTIONS

STATE OF THE FIELD

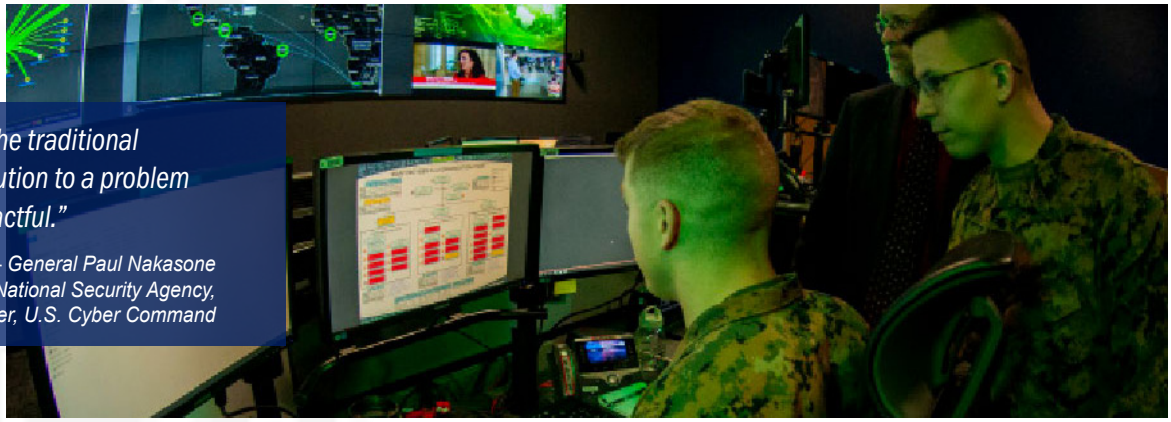
There are several U.S. and international frameworks that define the standards governing best practices in cybersecurity systems management and workforce development:

- National Institute for Standards and Technology (NIST) Cybersecurity Framework v1.1
- National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27000 Series: Information Security Management Systems Family of Standards (27001 – 27007)
- The Center for Information Security (CIS) v7

Partners with limited capacity and funding may find it challenging to integrate cybersecurity standards without tailoring these complex technology policies to each partner's unique needs. Even though the U.S. has laws and policies to guide cybersecurity requirements within DoD and across the government, there are challenges codifying cybersecurity maturity models and standards. Given the complexity and interdependencies in cyberspace, this is also a challenge in private sector integration of voluntary frameworks to assure a robust whole of society cybersecurity posture. A successful approach to building cyber capacity requires the assessment and understanding of unique partner capacities and constraints, acknowledging partners' social and political context, and tailoring right-sized ICB support.

"In today's cyber environment, the traditional acquisition model delivers a solution to a problem too late to be operationally impactful."

— General Paul Nakasone
Director, National Security Agency,
Commander, U.S. Cyber Command



WHY ICB MATTERS FOR CYBERSECURITY

In a globally connected world, it is a collective responsibility to design, build, and sustain secure and resilient information and communication technologies (ICTs) systems, and to better understand the interdependencies between technology and military operations. Military operations and national security depend on operational technology that aren't within the traditional scope of the ICT community.

The speed, scale, and scope of ever-evolving cyber threats can compromise our security, economic, and policy partnerships around the world. Cyberspace is now a fifth operational domain where malign actors operate against state and non-state actors that do not respect sovereign borders. Focused coordination, intensive knowledge exchange, and sustained capacity building among partner nations is required to prevent, mitigate, and effectively respond to cyber threats while protecting military networks and assets. U.S. cybersecurity depends, in part, on the maturity and efficacy of our partner nations' cybersecurity institutional capacity. For example:

- Strengthening intelligence sharing and military interoperability with our partners requires ironclad alignment on cybersecurity protections
- In the realm of cybercrime where criminals exploit sovereignty and legal jurisdiction, we rely on partnerships for comprehensive cyber threat detection and enforcement
- A physical and digital global supply chain requires collective protections for critical infrastructure

BUILDING CAPABLE CYBERSECURITY INSTITUTIONS

ICB BEST PRACTICES FOR CYBERSECURITY

Building the capacity of defense cyber institutions can help partner nations identify, assess, and better understand risks, capacities, and threats within their defense cyber ecosystem. The cyberspace institutional capacity building community can act as a convener and integrator, bringing together partner nation civilian and military officials to:

- Identify critical partner nation cybersecurity needs and agree on areas of mutual interest for engagement with the U.S.
- Devise risk mitigation strategies and codify applicable policies and procedures
- Build new capabilities or institutions that are resourced, trained, and equipped to effectively manage cybersecurity systems
- Align interoperability requirements between U.S. security cooperation assistance and partner nation systems
- Enhance the integrity and security of local cyber defense institutions
- Develop human capital strategies for building and sustaining a cyber workforce

CCB supports the development of cyberspace governance, national frameworks, policy, strategy, and workforce development planning, which can become a force multiplier for many other programs. Building new cyber capabilities together with a partner nation is not enough. These must be effectively integrated into their force structure, sustained and maintained, and well-coordinated with other capabilities. Therefore, ISG enables close partnership with diverse implementers, within DoD's security cooperation ecosystem as well as across industry and academia. Working together with the cybersecurity capacity building community, ISG is developing shared tools and approaches to enhance the outcome of its work alongside partner nations. In addition, the Institute is working to integrate cybersecurity into the mainstream of ICB planning, and to support the integration of country-level projects among the various implementers. The Institute's CCB activities encompasses several initiatives:

- Support the integration of partner nation cyber-related requirements into ICB planning and design and support the integration of capacity building projects at the country-level
- Support the development of a common assessment methodology and lend support to GCCs to conduct assessments of partner nation cyber capabilities as needed
- Deliver a range of capacity building and educational engagements on cyber governance, policy, and strategy in support of GCCs and partners
- Create tools and aides for the broader community of interest/practice. Most recently, the Institute conducted a study, initiated by ODASD Cyber Policy, and developed 1) a cyber-focused capacity building playbook; and, 2) a workforce development framework and compendium of relevant U.S. training/education in support of the broad cyber capacity building community. These products, developed through a collaborative process, aim to further harmonize and improve the cyber community's development of partners' cybersecurity capabilities.

Naval Support Activity Monterey
1635 Cunningham Rd, Bldg 259
Monterey, CA 93943-5011

T + 1831.656.3171
F + 1 831.656.3351
isginfo@.nps.edu

LinkedIn
instituteforsecuritygovernance.org

INSTITUTE FOR SECURITY GOVERNANCE
ADVANCING KNOWLEDGE | BUILDING CAPACITY | STRENGTHENING PARTNERS

DOD'S APPROACH TO INSTITUTIONAL CAPACITY BUILDING

WHAT IS INSTITUTIONAL CAPACITY BUILDING?

Institutional Capacity Building programs, overseen by DSCA, encompass Security Cooperation activities that directly support U.S. ally and partner nation efforts to improve security sector governance and core management competencies necessary to effectively and responsibly achieve shared security objectives.

ILLUSTRATIVE PARTNER INSTITUTIONS FOR ICB

Partner nations' civilian and military organizations focused at the strategic and operational levels such as Ministries of Defense and Interior, intelligence services, law enforcement organizations, military services, and legislatures.

ILLUSTRATIVE ICB DOMAINS

- Strategy & Policy
- Resource Management
- Human Resource Management
- Acquisition & Logistics
- Force Management
- Law & Human Rights

PRINCIPLES OF EFFECTIVE ICB

STRATEGICALLY DRIVEN

Driven by U.S. interests and values. When integrated early into Security Cooperation (SC) planning, ICB supports strategic dialogue about the partner's capability and will to execute a specified role.

PROBLEM FOCUSED

Assesses shortfalls in institutional performance that may impede partners' ability to execute role. Considers appropriate entry points for engagement and the enablers and inhibitors of change.

PARTNER CENTRIC

Avoids the projection or imposition of U.S. models, which may not fit a partner's specific context. Responsive to partners' priorities and their unique political and institutional dynamics.

MOVING FROM PROBLEM TO SOLUTION

SC PLANNING & ENGAGEMENT → JOINT PARTNER & U.S. ICB OPERATIONS

IDENTIFY PARTNER ROLE

Frame role U.S. wants partner to play and ensure SC objectives are feasible given capacity

FLAG SHORTFALLS THAT MAY REQUIRE ICB

Identify shortfalls in will and/or capacity that may impede partner's ability to execute role

JOINT PARTNER AND U.S. PLANNING

U.S. ICB providers and partner nation leaders validate problem and frame potential solutions

JOINTLY IMPLEMENT ICB SOLUTIONS

Deliver integrated ICB solutions across multiple stakeholders and assess viability of approach

JOINTLY MONITOR AND ADAPT

Continuously monitor progress and adapt actions based on what's working

ICB OFFERINGS

ADVISING & CONSULTING

Present partner with possibilities for institutional improvements or reform and assist with approaches tailored to partners' political and institutional context for change.

EDUCATION & TRAINING

Equip partners with the knowledge, skills, tools, and expertise to design and implement solutions.

CONFERENCES & SEMINARS

Engage partner stakeholders, explore country best practices, and help create space for progress.

SELECT SERVICES

- Resident/non-resident advising & consulting
- Multi-stakeholder workshops
- Tabletop Exercises (TTX)
- Resident courses
- Mobile engagement / training teams
- Senior Leader Engagement

ICB PLANNERS AND IMPLEMENTERS

- Defense Institute of International Legal Studies (DIILS)
- Defense Technology Security Administration (DTSA)
- Institute for Security Governance (ISG)
- Regional Centers

QUESTIONS ABOUT ICB?

Questions or comments about this Smart Sheet or any ICB topic?

Ask an ISG expert about any ICB question at:
isginfo@nps.edu