## \*\*Topicality\*\*

### SC =/= frameworks

#### Security cooperation activities are conducted THROUGH frameworks

**CRS 16** (Congressional Research Service, informing the legislative debate since 1914, “DOD Security Cooperation: An Overview of Authorities and Issues”, 8/23/16, <https://www.everycrsreport.com/reports/R44602.html>) // EL

This report provides a general overview of current DOD Title 10 authorities to assist foreign governments, militaries, security forces, and populations funded by the DOD budget. It presents background information on the evolving DOD security cooperation mission and the recent development of the **statutory framework through which DOD conducts security cooperation activities**. It provides summary overviews of nine categories of security cooperation assistance and activities, including the amounts of congressionally authorized funding, where available, and any legislatively required State Department input. It discusses recent issues related to the development, implementation, sustainment, and coordination of security cooperation to support continuing congressional oversight. Two tables in the appendix provide information on current Title 10 security cooperation authorities. The first catalogs current security cooperation authorities, noting legislative mandates for State Department input and notification and reporting requirements. The second provides a snapshot of authorized and/or appropriated funding levels for select security cooperation authorities.

### SC – Includes Training and Interoperability

#### SC includes arms sales, training and exercises, interoperability, and sovereign defense capabilities

Cooper 21 [R. Clarke Cooper is a Senior Fellow, Former U.S. Assistant Secretary of State for Political-Military Affairs, and the Former U.S. Alternative Representative to the UN Security Council; 12/23/21; <https://www.atlanticcouncil.org/blogs/new-atlanticist/a-multipolar-world-requires-more-adaptive-us-security-thinking/>] //CH

US security cooperation historically encompasses facilitating arms sales, staging military training and exercises, developing interoperability among allies and partners, and bolstering the sovereign defense capabilities of security partners. All these efforts need to continue at a deliberate pace—but in a post-Cold War world, the United States no longer has a monopoly on arms sales with an overt technological advantage in all areas.

### SC – Broader than DoD

#### SC is a community of branches not just a single branch or organization AND includes the DoS

Markel et al. 18 [M. Wade Markel is the director of the Forces and Logistics program in RAND Arroyo Center, and a senior political scientist at the RAND Corporation; “Career Development for the Department of Defense Security Cooperation Workforce”; 2018; <https://www.rand.org/pubs/research_reports/RR1846.html>] //CH \*Image is in the middle of text

The Security Cooperation Community

This appendix describes some of the significant organizations within the security cooperation community and explains their responsibilities with regard to security cooperation. It supplements the description of the security cooperation community in Chapter Two but is still only a partial rendering of those organizations that at various times contribute to the DoD’s conduct of security cooperation. Understanding organizations’ general roles and functions within the community is important for understanding the competencies members require in order to perform their functions. To recapitulate, the security cooperation community is

a subset of U.S government Executive Branch entities within the security cooperation enterprise directly responsible for managing or executing security cooperation programs or the policies that affect those programs (DoD, 2016, p. 9).

Overall, the goals of security cooperation community are

to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for selfdefense and multinational operations, and provide US forces with peacetime and contingency access to a host nation (Joint Chiefs of Staff, 2016, p. 9).

**No single organization has primary responsibility for attaining these objectives or concentrates exclusively on one aspect of security cooperation**. Rather, security cooperation is a capability that combatant commanders and U.S. embassies employ to further other U.S objectives, and is supported by capabilities in DoD components developed primarily to support the development and maintenance of U.S. military capabilities and capacity. To the extent that organizations and capabilities devoted primarily to security cooperation exist, they are constituted primarily to facilitate the leveraging of other U.S. military capabilities.

Within that general framework, organizations in the security cooperation community fall into one of four broad categories described briefly below and in greater detail in succeeding sections (see Figure A.1):

* Enterprise management (in the yellow box) organizations provide strategy and policy guidance and oversight to multiple security cooperation programs; they are responsible for integrating efforts from different U.S. and foreign stakeholders to achieve U.S. strategic goals.
* Implementing agencies (in the dark green box) ensure that individual programs are properly resourced and executed in accordance with policy guidance.
* Relationship management (in the light green box) organizations are responsible for translating strategy into action in specific countries and regions. They help initiate, plan, and facilitate security cooperation program activities involving U.S. and partner nation officials. It should be noted that these organizations also have a profound role in the development of strategy with respect to the country or region with which they are associated.
* Execution (in the light brown box) elements carry out program activities with partner-nation counterparts at the behest of higherlevel components of the community. For the most part, execution elements are not dedicated security cooperation assets but are operating force units or elements from organizations in the DoD infrastructure employed in support of security cooperation activities.

Yet while organizations may fall primarily into one of these four categories, members of their workforce do not align exclusively with these functions. For example, security cooperation offices have individuals with primary responsibility for international training manage - [Image inserted]

A picture containing diagram

Description automatically generated

ment and finance. Officials in implementing agencies maintain direct lines of contact with customers in partner nations, as do officials in organizations with a primary focus on enterprise management. The major salient characteristic of the security cooperation community is that it is complex, with diffuse authorities and responsibilities. Its success depends on the ability of officials to work across organizational and functional boundaries to achieve the larger goals of U.S. strategy.

### SC – Includes the DHS

#### The DHS can increase SC on cyber – empirics

DHS 22 [The United States Department of Homeland Security is the U.S. federal executive department responsible for public security; “**DHS to Increase Security Cooperation with Israel through New Arrangements**”; 3/3/22; <https://www.dhs.gov/news/2022/03/03/dhs-increase-security-cooperation-israel-through-new-arrangements>] //CH

WASHINGTON – This week, Department of Homeland Security (DHS) Under Secretary for Policy Robert Silvers visited Jerusalem and Tel Aviv, Israel to sign security agreements with the Government of Israel, engage with key Israeli government and private sector partners on a range of joint security issues, and deliver keynote remarks on DHS cybersecurity priorities at the CyberTech Global Conference.

“DHS is proud to continue to strengthen the bilateral relationship between the United States and Israel through new security arrangements,” said DHS Under Secretary for Policy Robert Silvers. “The arrangements signed this week between our Department and the Government of Israel underscore that Israel is a critical partner in advancing a broad range of international technology and security priorities.”

Under Secretary Silvers and Israel National Cyber Directorate (INCD) Director General Gaby Portnoy issued a Joint Statement of Intent that reflects a shared commitment between the two agencies to work together to combat ransomware, bolster cooperative research and development, strengthen critical infrastructure cybersecurity, increase resilience to cyber threats, and pursue expert exchanges in the area of emerging technology.

Building on the long-standing relationship between DHS and INCD, Under Secretary Silvers and Director Portnoy signed an arrangement with Israel’s Ministry of Public Security for INCD to join the Israel-U.S. Binational Industrial Research and Development Homeland Security Program, which will facilitate cyber-related research and development to enhance both countries’ resilience to evolving threats. They also signed a Memorandum of Understanding to further the joint work between INCD and DHS’s Transportation Security Administration (TSA) to advance cybersecurity cooperation in the aviation, maritime, mass transit, freight and passenger rail, and oil and natural gas sectors.

### SC – Not OHDACA

#### SC is distinct from actions under OHDACA

Defense 18 [The Office of the Secretary of Defense is a headquarters-level staff of the United States Department of Defense; “Fiscal Year (FY) 2019 President’s Budget Security Cooperation Consolidated Budget Display”; February 2018; <https://open.defense.gov/Portals/23/Documents/Security_Cooperation/Budget_Justification_FY2019.pdf>] //CH

DoD provides a range of humanitarian activities funded by the Overseas Humanitarian, Disaster, and Civic Aid (OHDACA) appropriation, from foreign disaster relief operations authorized by the Secretary of Defense to GCC security cooperation efforts. Although **the purpose of foreign disaster relief operations is not security cooperation**, the byproduct often strengthens existing bilateral security relationships and provides a bridge to new partners. Steady-state humanitarian assistance (HA) includes activities designed to relieve or reduce endemic conditions such as human suffering, disease, hunger, and privation. HA may also bolster a host nation’s capacity to reduce the risk of, prepare for, mitigate the consequences of, or respond to humanitarian disasters.

### SC – Yes OHDACA

#### OHDACA is part of security cooperation AND is part of the DoD

DSCA 20 [The Defense Security Cooperation Agency is a part of the United States Department of Defense; “C12 - Overseas Humanitarian, Disaster, and Civic Aid (OHDACA)”; Last Cited 2020 (10 U.S.C. 2561, 2020 edition); <https://samm.dsca.mil/chapter/chapter-12>] //CH

C12.1. - Overview

C12.1.1. General. The DoD conducts HA to relieve or reduce endemic conditions such as human suffering, disease, hunger, privation, and the adverse effects of unexploded explosive ordnance (UXO), particularly in regions where humanitarian needs may pose major challenges to stability, prosperity, and respect for universal human values. The OHDACA appropriation funds DoD HA activities that build the capacity of a partner nation (PN) government to provide essential humanitarian services to the civilian population and supports PN efforts to reduce the risk of, prepare for, and respond to humanitarian disasters thereby **OHDACA-funded programs offer a unique security cooperation tool** reducing reliance on international disaster relief assistance. When authorized, OHDACA funds are used to conduct FDR activities. OHDACA-funded programs offer a unique security cooperation tool for Combatant Commands (CCMDs) to gain access, visibility, and influence within their regions and achieve theater and U.S. national security objectives.

### SC – WM – TEVV

#### We meet – Aff is under the DoD

Schmidt et al. 21 [Eric Schmidt is a technologist and entrepreneur, served as Google’s Chief Executive Officer and Chairman from 2001 to 2011, as well as Executive Chairman and Technical Advisor, and co-founded Schmidt Futures in 2017; other author’s works listed on page 741; “National Security Commission on Artificial Intelligence”; Last cited 1/31/21; <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>] //CH

Component 3: Foster the JAIC AI Partnership for Defense (AI PfD) as a critical vehicle to further AI defense and security cooperation.

Launched in 2020, the AI PfD is a **DoD-led effort to convene partner nations** to “provide values-based global leadership” on **adoption of AI in the defense and security context**.16 Current members include Australia, Canada, Denmark, Estonia, Finland, France, Israel, Japan, Norway, South Korea, Sweden, and the United Kingdom.

### Cybersecurity – Cyber Threats

#### Cybersecurity is the protection of internet-connected systems from cyberthreats

Shea, Gillis, and Clark ND [Sharon Shea is executive editor of the Security Media Group, overseeing SearchSecurity, SearchCloudSecurity and SearchCompliance; Alexander S. Gillis is a technical writer and editor in the WhatIs group at TechTarget; Casey Clark is a former assistant site editor for SearchSecurity; “What is cybersecurity?”; No date; <https://www.techtarget.com/searchsecurity/definition/cybersecurity>] //CH

**Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats**. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

Why is cybersecurity important?

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

What are the elements of cybersecurity and how does it work?

The cybersecurity field can be broken down into several different sections, the coordination of which within the organization is crucial to the success of a cybersecurity program. These sections include the following:

* Application security
* Information or data security
* Network security
* Disaster recovery/business continuity planning
* Operational security
* Cloud security
* Critical infrastructure security
* Physical security
* End-user education