# \*\*T Supplement – FMPS 22\*\*

## \*\*Notes\*\*

#### Thank you to the following students who worked on this file:

Calvin Hwang

Claire Davis

Esther Liu

Kira Tretiak

Ruchi Agarwal

Questions, comments, concerns: [jasminestidham@gmail.com](mailto:jasminestidham@gmail.com) / jstid@umich.edu

## \*\*Security Cooperation\*\*

### Must Be DoD

#### DoD is the only predictable limit to security cooperation, anything else proves limits explosion is inevitable

Sally Sleeper 2021, Select RAND Research on Security Cooperation: 2006-2019, Santa Monica, Calif.: RAND Corporation, CP-A614-3, 2021. As of July 16, 2022: https://www.rand.org/pubs/corporate\_pubs/CPA614-3.html//cpd

Security cooperation is an important and expanding instrument of U.S. foreign policy that is employed widely to accomplish a diverse set of objectives. Security cooperation goals vary depending on current U.S. strategic and operational objectives and the partner nation that is being engaged. Goals can include building the capacity of partner security forces to improve the security environment, strengthening relationships with foreign militaries and governments, and securing access for U.S. military forces so they can more effectively operate abroad.

The type of security cooperation that DoD deploys depends on the objective at hand and capabilities of the partner nation. DoD tends to deploy building partner capacity programs and security force assistance to less developed partner nations in an effort to improve their tactical and operational capabilities, while defense institution building initiatives are used in similar contexts to strengthen ministries of defense at the strategic level. On the other hand, programs aimed at interoperability tend to be targeted at more-developed allies. DoD conducts about 3,000 to 4,000 security cooperation events each year in more than 130 countries, while total U.S. assistance to foreign militaries and police forces runs from $15 billion to $20 billion per year. Security cooperation activities touch tens of thousands of foreign security forces around the world every year. What do we know about security cooperation? Are the strategic and operational goals of the enterprise being met? Does security cooperation "work"? If so, under what conditions?

### AT: Can’t Include Security Assistance

#### There is no legal distinction between “security cooperation” and “security assistance”

Nina M. Serafino 05-26-2-16, Specialist in International Security Affairs, “Security Assistance and Cooperation: Shared Responsibility of the Departments of State and Defense”, Congressional Research Service. <https://sgp.fas.org/crs/natsec/R44444.pdf> accessed 7-16-22//cpd

The discussion of U.S. assistance to foreign military and other security forces is complicated by the lack of a standard and adequate terminology. “Military assistance,” “security assistance,” “security cooperation,” “security sector assistance,” “security force assistance,” and “defense articles and services” are all terms used in connection with the supply of weapons, equipment, supplies, and training to such forces and, in some cases, engagement with them. Some of these terms are defined by policy documents or in law (see Appendix A). Some authorities are labeled with two more informal terms—“build partner capacity” or “train and equip”—which are used in the discussion of specific authorities below.7

Terminology The two terms most commonly used today for assistance to foreign military and security forces are “security assistance” and “security cooperation.” Security assistance is the term most frequently used, regardless of the agency providing that assistance. There is no State Department definition for security assistance. The annual State Department congressional budget justification (CBJ), however, lists six budget accounts under the heading “International Security Assistance.” These accounts, with their underlying Title 22 authorities (the 1961 FAA and the AECA), are commonly regarded as the State Department’s security assistance portfolio.

### SC Includes Arms Sales

#### Security Cooperation includes FMS, DCS, hybrid sales, leases, and EDA

DSCA 10 [The Defense Security Cooperation Agency is a part of the United States Department of Defense; “SECURITY COOPERATION OVERVIEW”; 2010 (Uses US Code 2010 Edition); <https://www.dsca.mil/foreign-customer-guide/security-cooperation-overview>] //CH

The U.S. conducts Security Cooperation business with over 200 countries and international organizations around the world. We typically refer to specific Security Cooperation activities, such as sales of defense articles and services, as “programs” and conduct them under two primary U.S. legislative authorities: The Arms Export Control Act (AECA) (22 U.S.C. 2751 et seq.), as amended, and the Foreign Assistance Act of 1961 (FAA), as amended (22 U.S.C 2151 et seq.). Under these authorities, there are several methods available to provide foreign partners with U.S. defense articles and services. The most commonly used method is Foreign Military Sales (FMS) - but other alternatives might also be available to meet your country’s requirements. For any given purchase your country may be considering, there are benefits, limitations, and trade-offs associated with each of these methods.

**Foreign Military Sales (FMS)**

FMS is a program that allows your government to purchase defense articles and services as well as design and construction services, from the U.S. Government (USG). This program is operated on a “no-profit” and “no-loss” basis to the USG and requires an authorized representative from your government to submit a Letter of Request (LOR) to the USG for the desired defense articles and services.

Under FMS, the U.S. Department of Defense (**DoD**) procures defense articles and services for your country using the same acquisition process used to procure for its own military needs. This acquisition process is governed by the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS). You, the foreign purchaser, benefit from U.S. DoD technical and operational expertise, procurement infrastructure, and purchasing practices. Your country also benefits from the lower unit costs that result when the U.S. DoD is able to combine your purchase with one of its own to achieve greater economy of scale. In addition, the U.S. DoD ensures your purchase takes into consideration all of the necessary training, support, and sustainment to give you the lasting operational capability you seek, known as the “Total Package Approach”. Finally, a major FMS program increases your country’s interoperability with U.S. military forces, creating potential opportunities for joint training, joint exercises, cooperation in humanitarian assistance and disaster relief, and peacekeeping operations.

FMS requires a government-to-government agreement, known as a Letter of Offer and Acceptance (LOA) and also referred to as an “FMS case”. When your U.S. counterparts speak of “writing a case”, they are talking about drafting an LOA. The LOA is written by the USG and must be formally accepted by your government. The LOA specifies the items and services to be provided to your country and an estimated cost and timeframe for doing so. The USG may supply items from its own stocks or it may enter into a contract with a defense contractor to obtain the items on your behalf. Any contracts with U.S. defense contractors, if needed, will be written by the USG using standard USG competitive contracting procedures, to include robust oversight and auditing. The contract will be between the USG and the U.S. defense contractor. The USG then provides the equipment or service to your country as agreed in the government-to-government LOA. FMS customers are not legal participants in the procurement contract.

By Policy, the USG does not conduct FMS for profit. By U.S. law, the USG may not incur debt on an FMS sale to your country. The LOA will require that your country pay the full cost associated with the FMS sale - which includes the cost of the defense equipment/services and any costs incurred by the USG while providing you with the defense equipment/services. We must ensure that, when the equipment or service is delivered and the case is closed, the USG has neither made a profit nor passed a debt to the U.S. taxpayer.

To build and re-build the administrative infrastructure necessary to support individual FMS cases would be a slow process and very costly to our foreign partners. Therefore, the USG maintains a standing infrastructure at the DoD level, within each of the Military Departments (MILDEPs), and within select other DoD organizations that conduct FMS. That standing infrastructure - skilled employees, information technology systems, offices, etc. - is funded by an administrative surcharge applied to every FMS case. The FMS administrative surcharge fund is managed by the Defense Security Cooperation Agency (DSCA) under the oversight of the DoD Comptroller.

For additional general information on the FMS process, see SAMM Chapter 4.

**Direct Commercial Sale (DCS)**

DCS involves commercial contracts negotiated directly between your country and a U.S. defense contractor. DCS agreements are not administered by the USG and do not involve a government-to-government agreement. Instead, you deal with the U.S. contractor and that contractor is responsible for obtaining an export license from the Office of Defense Trade Controls, within the U.S. Department of State, to conduct each sale. The regulations for DCS are contained in the U.S. International Traffic in Arms Regulations (ITAR).

DCS is sometimes selected as an alternative to FMS when: a purchasing government's military requirements are significantly different from standard U.S. configurations; a purchasing government has a sufficiently sophisticated procurement staff with experience in defense systems; or when a purchasing government is seeking to establish a relationship between a U.S. manufacturer and its own domestic industry.

An extensive comparison of the advantages of FMS and DCS has been compiled and published by the Defense Institute of Security Cooperation Studies (DISCS – formerly known as DISAM) in Chapter 15 of its textbook, “The Management of Security Cooperation” - also referred to as “The Green Book”.

The U.S. DoD is generally neutral as to whether a sale should be accomplished using the FMS or the DCS process. However, as a matter of policy, the USG will not engage a potential FMS case with your country if you are already engaged in DCS discussions with a U.S. contractor. Please refer to the DSCA Policy Letter on concurrent FMS and Commercial Negotiations

There are times when the DoD requires that a purchase be accomplished through the FMS system. For example, the DoD requires all U.S. military training to be obtained through FMS. The DoD may also require defense articles to be sold “FMS-only.” Two common reasons for this are to ensure the security of sensitive technologies and the control of weapons and munitions to prevent proliferation. The cognizant U.S. MILDEP (Army, Navy, Air Force), or the U.S. manufacturer, will tell you whether or not a particular item is FMS-only.

**Hybrid Sales**

It is possible to separate the FMS-only portions of a purchase from those portions permitted to be sold via DCS. This process is common for a foreign government to mix FMS and DCS when making major purchases of complex systems, such as aircraft. These are known as hybrid sales and might, for example, involve purchase of an airframe through DCS, and avionics, weapons, and training through FMS. If you are initiating a DCS purchase with a company and expect that it will (or might) include items that will be purchased via the FMS system, you should contact the appropriate U.S. MILDEP or DSCA as early as possible. The delivery timeline of your DCS end-item will likely depend in great measure upon FMS items being integrated first, or upon FMS training being provided at the appropriate time. It is therefore important that you discuss your larger purchase plans and your operational objectives with the appropriate MILDEP or DSCA to obtain an expert assessment and firm understanding of the FMS timeline and any potential issues. The defense contractor you are working with may not have full knowledge of Military Department plans and timelines. Ultimately, the best source of information on any equipment that is to be provided by the USG is the USG itself.

**Leases**

The USG may lease defense articles to another country for temporary use (not to exceed five years). In order to be eligible for lease, an item must not be needed for USG use during the course of the lease and is generally limited to investment (non-consumable) type items. Countries may use a lease to meet a short-term need or to fill a critical defense requirement while waiting for a delivery of items purchased through FMS or DCS. Leases can also be entered into for a variety of other purposes, including cooperative research or development, military exercises, and communications or electronics interface projects. More detail on leases can be found in Section 11.6. of the SAMM.

**Excess Defense Articles (EDA)**

When defense articles are declared excess by the U.S. DoD, they may be sold through FMS or by grant to countries eligible to receive EDA. Keep in mind however, that not all excess DoD articles are made available for sale or grant; and U.S. government agencies are given the first opportunity to acquire EDA. For EDA sales to foreign customers, prices usually range from 5% to 50% of the original acquisition value, depending on the condition of the item. EDA is transferred on an “as-is, where-is” basis. This means that your country will be required to pay any repair and refurbishment costs and, generally, all transportation costs associated with getting the EDA to your country. More detail on EDA can be found in Section 11.3. of the SAMM.

The above options may be used in different combinations to satisfy your country’s unique requirements. A Security Cooperation program might consist of some items purchased through FMS, additional items through DCS, and still others obtained via lease or EDA. The USG can work with you to help you achieve the best “fit” for your needs.

### SC Includes Info-sharing

#### Security cooperation includes info sharing

Scott 17—Kevin D. Scott, vice admiral in the US Navy and Director of Joint Force Development, 5-23-17, Security Cooperation Joint Publican 3-20, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf>

**Security cooperation** (SC) **encompasses** all Department of Defense (DOD) interactions, programs, and **activities** with foreign security forces (FSF) and their institutions **to** build relationships that help **promote US interests**; enable partner nations (PNs) to **provide** the US **access to** territory, infrastructure, **information**, and resources; **and**/or to **build** and apply their **capacity and capabilities consistent with** US **defense objectives**. It **includes**, but is not limited to, military engagements with foreign defense and security establishments (including those governmental organizations that primarily perform disaster or emergency response functions), DOD-administered security assistance (SA) programs, combined exercises, international armaments cooperation, and **information sharing and collaboration.**

### SC Includes the DoS

#### The DoS manages and supervises all security cooperation

DSCA ND [The Defense Security Cooperation Agency is a part of the United States Department of Defense; “MAJOR USG STAKEHOLDERS IN SC”; No date; <https://www.dsca.mil/resources/major-usg-stakeholders-fms>] //CH

**The Department of State (DOS)**

**The Secretary of State is responsible for management and supervision of all aspects of U.S. security cooperation programs - including SC**. DOS determines whether (and when) there will be a U.S. program with, or sale to, a particular country and, if so, its size and scope.

The DOS Bureau of Political Military Affairs Office of Regional Security and Arms Transfers (PM/RSAT) is the lead DOS Bureau for SC matters, including transfer approvals and the notifications that must go to the U.S. Congress before a transfer can occur.

### 1NC – SC =/= Frameworks

#### Security cooperation involves training, equipping, and supporting foreign military forces. Frameworks are tools used to assess, monitor, and evaluate those security cooperation activities but ARE NOT security cooperation activities themselves

**CRS 17** (Congressional Research Service, informing the legislative debate since 1914, “DOD Security Cooperation: Assessment, Monitoring, and Evaluation”, 6/23/17, <https://crsreports.congress.gov/product/pdf/IN/IN10726>) // EL

As part of recent efforts to modify existing security cooperation authorities, the FY2017 National Defense Authorization Act (NDAA) (P.L. 114-328) enacted several new provisions that modify the budgeting, execution, administration, and evaluation of Department of Defense (DOD) security cooperation programs and activities. To date, the Department of Defense (DOD) has spent billions of dollars on efforts to train, equip, and otherwise support foreign military and security forces. In the 114th Congress, both the House and Senate Armed Services Committees examined various aspects of DOD security cooperation efforts. Yet, prior to this year, there has been no comprehensive, standardized framework to judge the effectiveness of security cooperation programs, as authorized by various security cooperation authorities (see CRS Report R44602, DOD Security Cooperation: An Overview of Authorities and Issues). In the conference report accompanying the FY2017 National Defense Authorization Act (NDAA), the conferees noted that **although there has been an increase in security cooperation activities over the past 15 years, DOD “has not applied** sufficient emphasis and resources to develop a **comprehensive framework to assess, monitor, and evaluate its security cooperation programs and activities**,” commonly referred to as AM&E.

#### Violation – the plan fiats a coordinative framework

#### That’s a voter:

#### Limits – infinite subsets of coordination framework aff’s under the three emerging tech areas decks predictability, preround prep, and negative engagement

#### Ground – they’re perceptually insignificant, it means they spike out of links to case turns, da’s, k’s, and make sketchy perms which is def abusive on an aff biased topic

### 2NC – No Frameworks!

#### Security cooperation includes building partner capacity, education, and training. Establishing frameworks is not security cooperation itself but a method of PREPARING security cooperation, which is distinct!

**Taliaferro 18** (Aaron C. Taliaferro, Project Leader - International Defense Consultant, “A Framework for Security Cooperation Planning”, The Institute for Defense Analyses, Aug 2018, <https://www.ida.org/research-and-publications/publications/all/a/af/a-framework-for-security-cooperation-planning>) // EL

"Building partner capacity has been a key component of U.S. defense strategy since the 2006 Quadrennial Defense Review was issued. However, but for a few exceptions, the Military Departments of the U.S. Armed Forces that have responsibility to organize, train, equip, and provide forces to U.S. Combatant Commands have not prepared their people to be good or even adequate at planning for steady-state, peacetime security cooperation activities, which is the principal way the Department of Defense (DOD) builds partner capacity. Rather, the focus of military education and training primarily remains on contingency and warfare planning. While useful in those contexts, it is not useful for steady-state, peacetime security cooperation planning. Not only are people poorly prepared, the DOD lacks a **framework for security cooperation planning**. This paper’s intent is to propose a framework for security cooperation planning that helps the DOD and its Military Departments understand how to adaptively influence, plan, and resource security cooperation activities carried out in various foreign nations and with members of foreign security forces."

### 1NC SC – Must be Binding vs MoUs

#### Security cooperation is legally binding

JCS 17 [The Joint Chiefs of Staff is the body of the most senior uniformed leaders within the United States Department of Defense, that advises the president of the United States, the secretary of defense, the Homeland Security Council and the National Security Council on military matters; “Security Cooperation”; 5/23/17; <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf>] //CH

Throughout the execution of SC activities, CCDRs and their staffs continually direct, assess, monitor, evaluate, and adjust the SC activities when possible and the CSCSs/country plans as required, while the component commands do the same with their supporting plans. However, once resourced, execution of specific SC activities occurs as planned unless a crisis affecting US forces and/or the PN precludes completion of those SC activities. SC activities normally take place through bilateral agreements that constitute binding legal obligations for both the USG and PN. As a result, any deviation from the terms of a bilateral agreement likely requires the consent of both governments. Consequently, major changes are unlikely during the execution of a specific SC activity. However, in the absence of a governing bilateral agreement and with several FYs of SC activities at various stages of planning, programming, and budgeting during any given calendar year, this process can make changes for the future.

#### A Memorandum of Understanding is not binding

Kenton 22 [Will Kenton is an expert on the economy and investing laws and regulations. He previously held senior editorial roles at Investopedia and Kapitall Wire and holds a MA in Economics from The New School for Social Research and Doctor of Philosophy in English literature from NYU; “Memorandum of Understanding (MOU)”; 6/24/22; <https://www.investopedia.com/terms/m/mou.asp>] //CH

What Is a Memorandum of Understanding (MOU)?

A memorandum of understanding is an agreement between two or more parties outlined in a formal document. It is not legally binding but signals the willingness of the parties to move forward with a contract.

The MOU can be seen as the starting point for negotiations as it defines the scope and purpose of the talks. Such memoranda are most often seen in international treaty negotiations but also may be used in high-stakes business dealings such as merger talks.

### 2NC – MoUs =/= Binding

#### MOUs aren’t binding

Defense 20 [The United States Department of Defense is an executive branch department of the federal government charged with coordinating and supervising all agencies and functions of the government directly related to national security and the United States Armed Forces; “DOD INSTRUCTION 4000.19”; 12/16/20; <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/400019p.pdf>] //CH

c. MOU.

An MOU is used to document a mutual understanding between any two or more parties that does not contain an expectation of payment, and under which the parties do not rely on each other to execute or deliver on any responsibilities. Support agreements for temporarily assigning federal civil service personnel between federal entities in accordance with Section 3341 of Title 5, U.S.C., cannot be executed via an MOU.

### 2AC C/I – MoU is part of SC

#### Memorandum of Understandings can be part of security cooperation

ANI 22 [Asian News International is an Indian news agency that offers syndicated multimedia news feed to news-bureaus in India and elsewhere; “China sings MoU on security cooperation with Solomon Islands”; 3/29/22; <https://theprint.in/world/china-sings-mou-on-security-cooperation-with-solomon-islands/892668/>] //CH

Beijing [China], March 29 (ANI): China has signed the **Memorandum of Understanding** (MoU) with the Solomon Islands on “**security cooperation**” which allow Beijing to send law enforcement forces to the Islands.

**The MoU on security cooperation** between China and Solomon Islands was signed on March 18. It will allow China to send police, Armed Police, military personnel and other law enforcement forces to the Solomon Islands, on request, to assist in maintaining social order and accomplish other tasks agreed upon by both countries, said the report.

#### It’s legally binding – it meets specific standards

Munoz 18 [Eugenia Munoz is a Legal Content Writer and paralegal at LegalVision, with a particular interest in startups and intellectual property; “Is a Memorandum of Understanding Legally Binding?”; 8/17/18/https://legalvision.com.au/memorandum-of-understanding-legally-binding/] //CH

A memorandum of understanding (MOU), also referred to as a letter of intent, heads of agreement or term sheet, can be an extremely useful commercial tool. Parties use MOUs to quickly and inexpensively set out the commercial terms of a transaction. They do this ahead of entering into a formal contract to get the deal moving. However, is a MOU legally binding? In this article, we outline some indicators that your MOU is legally binding.

It’s legally binding if it meets these circumstances

Is it a Final Agreement?

Firstly, a court will consider whether the parties have actually come to a final agreement. Often, parties use an MOU when they have commenced a commercial relationship but are still negotiating specific aspects of it.

If it is clear from the document that the parties are still negotiating, a MOU is probably not legally binding. Phrases such as “subject to further negotiation” will likely indicate that the parties have not come to a final agreement. Therefore, you should consider whether your MOU indicates that you have reached an agreement or that negotiations are still ongoing.

Is it a Complete Agreement?

To be legally enforceable, the MOU must contain all the essential terms of the agreement. Often, MOUs are not a complete agreement. Parties can leave several essential terms out because they have not decided on them yet.

Essential terms are the terms that parties must finalise before a court can enforce the agreement. For example, in an agreement between a gym and a client, the parties must agree to the time frame of the contract before the agreement is binding. However, deciding on the brand of the gym equipment is not necessary to enforce the agreement.

Accordingly, consider whether you have finalised the essential aspects of your agreement. Ask yourself whether enough information is present to hold the parties to their promises.

Was There an Exchange of Promises?

For the agreement to be legally binding, each party has to promise something of benefit to the other party, in exchange for something else. For example, in an agreement for the sale of a car, the buyer promises money and, in exchange, the seller promises the car.

Often, MOUs simply outline the common goals and expectations of the parties. They often use language that indicates discretion of performance, such as “Party A may” rather than “Party A will”. When the language suggests that a party can choose whether they hold up their end of the bargain, the MOU is not enforceable. Therefore, consider what the parties have promised each other and how certain those promises are.

Do You Have the Intention to be Legally Bound?

For the MOU to be binding, it must suggest that the parties intend to be legally accountable for their promises. To determine whether this is the case, consider the consequences of a breach.

If there is a lot at stake, it is likely that the parties intend to receive legal protection. In addition, look for clauses that explicitly state whether the parties intend for the law to bind them. Some MOUs expressly include clauses along the lines of “the parties do not intend to be legally bound by the above terms”.

MOUs often fall under the category of preliminary agreements, or “agreements to agree”. There are three categories of intention concerning preliminary agreements, where the parties:

1. have come to a complete agreement and intend to be bound immediately, but want to rewrite the terms in a detailed document;
2. have come to a complete agreement but do not intend to perform the agreement until they write a formal document; and
3. do not intend to be bound by the agreement unless they write a contract.

The first two categories indicate an intention to be legally bound by the terms of the agreement. If the MOU falls into the third category, the law will not bind the parties until there is a formal contract.

## \*\*Cybersecurity\*\*

### CIA Triad – Precision

#### CIA triad is key to define the scope of cybersecurity law

Jeff **Kosseff**, 20**18**, "Defining Cybersecurity Law," Iowa Law Review, https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/, accessed 7-16-2022//cpd

In short, the U.S. legal system lacks a consistent definition of the term “cybersecurity law.” This Article aims to fill that gap by defining “cybersecurity law.” Although “cybersecurity” is a commonly used term in legal circles, no scholarship has stepped back to define exactly what “cybersecurity law” is and the goals of statutes and regulations that aim to promote “cybersecurity.” By defining the scope and goals of this new legal field, policymakers can then examine how lawmakers could improve existing laws. Part II of this Article briefly describes the cybersecurity challenges that the United States faces by examining the cyberattack on Sony Pictures Entertainment. Part III broadly examines current cybersecurity threats to the United States and defines “cybersecurity law” as a legal framework that “promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security.” Part IV of this Article explains the current U.S. legal regime for cybersecurity and concludes that many of the most prominent cybersecurity laws only address a small portion of the broader legal framework. Part V examines the gaps in current U.S. cybersecurity law and suggests which areas of cybersecurity law policymakers could better address.

### Cyberspace

#### Cybersecurity is the ability to protect cyberspace from cyberattacks

Barrett et al. 20 [Matt Barrett and Jeff Marron are part of the Applied Cybersecurity Division of the Information Technology Laboratory, Victoria Yan Pillitteri, Jon Boyens, Stephen Quinn are part of the Computer Security Division of the Information Technology Laboratory, and Greg Witte and Larry Feldman are from the Huntington Ingalls Industries Annapolis Junction; “Approaches for Federal Agencies to Use the Cybersecurity Framework”; March 2020; <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf>] //CH

Cybersecurity [CNSSI 4009]

The ability to protect or defend the use of cyberspace from cyber attacks

### Cybersecurity =/= Information Security

#### The confidentiality, integrity, and availability of data is information security – that’s distinct from cybersecurity which is data protection

Holmes 22 [Rachael Holmes is a Senior Content Marketing Specialist for BitSight; “Cybersecurity vs. Information Security: Is There A Difference?”; 1/6/22; <https://www.bitsight.com/blog/cybersecurity-vs-information-security>] //CH

Information security is another way of saying “data security.” If you are an information security specialist, your concern is for the confidentiality, integrity, and availability of your data (this is often referred to as the “CIA”). Most modern business data resides electronically on servers, desktops, laptops, or in the cloud—but before all confidential information migrated online, it was sitting in a filing cabinet. And some confidential information still is. **Information security is concerned with making sure data in any form is kept secure**.

**Cybersecurity is all about protecting data that is found in electronic form** (such as computers, servers, networks, mobile devices, etc.) **from being compromised or attacked**. Cybersecurity involves identifying what the critical data is, where it resides, its risk exposure, and the technology you have to implement in order to protect it.

### Cybersecurity = Defense

#### Cybersecurity is digital protection from internal and external threats

IBM ND [International Business Machines Corporation is an American multinational technology corporation with operations in over 171 countries; “What is cybersecurity?”; No date; <https://www.ibm.com/topics/cybersecurity>] //CH

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

#### Cybersecurity is the protecting networks from unproved use or the confidentiality, integrity, and availability of information

CISA 19 [The Cybersecurity and Infrastructure Security Agency is a United States federal agency, an operational component under Department of Homeland Security oversight; “What is Cybersecurity?”; 11/14/19; <https://www.cisa.gov/uscert/ncas/tips/ST04-001>] //CH

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now—communication (e.g., email, smartphones, tablets), entertainment (e.g., interactive video games, social media, apps ), transportation (e.g., navigation systems), shopping (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), and the list goes on. How much of your daily life relies on technology? How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system?

### Cybersecurity = Digital Defense Spending

#### Cooperation with NATO on cybersecurity requires digital defense spending

* This is like not a good card at all

Maigre 22 [Merle Maigre is a Senior Fellow with CEPA's Transatlantic Leadership Program and CEPA's Digital Innovation Initiative, and the Senior Cyber Security Expert at Estonia's e-Governance Academy; “NATO’s Role in Global Cyber Security”; 4/06/22; <https://www.gmfus.org/news/natos-role-global-cyber-security>]

This should come with obvious financial and investment implications. Public debates on burden sharing within NATO for too long have focused on how much member states spend on defense in isolation, without adequate prioritizing where those funds are going. Member states should be rethink defense spending relative to emerging threats and collective security challenges. To ensure funding for cyber security is appropriately prioritized, NATO should strengthen a commitment to digital defense spending, building on the strong base it has developed in terms of doctrine, standards, and requirements.

### AT: CIA Triad Interp (OCOs aff)

#### The DOD says we meet all three!

DOD ‘15 [Department of Defense, The United States Department of Defense is an executive branch department of the federal government charged with coordinating and supervising all agencies and functions of the government directly related to national security and the United States Armed Forces, “Developing a Tactical Environment Cyber Operations Training Program,” TECO Study, September 15 2015, https://www.sans.org/media/security-training/TECO-Study.pdf]@RA

ICT includes systems or applications associated with computer and network hardware, software, and communication medium [5]. The technology encompasses computers, enterprise software, middleware , and data storage, which enable users to access, store, transmit, and manipulate information. Military cyber operations (DoDIN Ops, DCO, and OCO) focus primarily on ICT systems and their integration with military operations [1]. Exploitation FX3RD-35014 7 of ICT systems can result in loss of intelligence and proprietary information, degraded communication, loss of data processing and computing systems, and manipulation of data. Indeed, compromise of ICT systems effects the confidentiality, integrity, and availability of data that command and control decisions and daily operations depend on.

### AT: Property Rights Interp (OCOs aff)

#### We meet – DOD uses OCOS to protect property rights

Crowther and Ghori ‘15 [G. Alexander Crowther and Shaheen Ghori, Alex Crowther is a visiting research professor with a dual appointment in both the Jack D. Gordon Institute for Public Policy and the Department of Criminology and Criminal Justice, both within the Steven J. Green School of International and Public Affairs at FIU. Dr. Crowther is also an integral part of FIU’s Emerging Preeminent Program Cybersecurity@FIU, Shaheen Ghori is a research assistant at National Defense University. She has a B.A. from American University and a masters in cybersecurity from George Mason University, “Detangling the Web A Screenshot of U.S. Government Cyber Activity”, National Defense University Press, July 1 2015, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-78/jfq-78\_75-83\_Crowther-Ghori.pdf]@RA

The Offices of the U.S. Attorneys is the last major part of Justice that works cyber issues. One of their 10 priority areas is cyber crime.38 Their three areas of concentration are Internet stalking, computer hacking, intellectual property rights and forensics. They also assist the National Computer Forensics Institute.

Department of Defense

The DOD mission is to secure the Nation’s freedom of action in cyberspace and help mitigate risks to national security resulting from America’s growing dependence on cyberspace. Specific mission sets include directing, securing, and defending DOD Information Network (DODIN) operations (including the dot.mil domain); maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; and providing support to civil authorities and international partners.39

DOD articulates its cyber policy through the DOD Strategy for Operating in Cyberspace, dated July 2011, and Joint Publication 3-12, Cyberspace Operations, dated February 5, 2013. DOD’s operations are designed to achieve and maintain cyberspace superiority, defined as “the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.”40 DOD organizations are allowed to perform defensive cyber operations; however, full-spectrum cyber operations (including offensive cyber operations) are approved by the President and directed by the Secretary of Defense.41

## \*\*NATO\*\*

### NATO = Organization

#### NATO is a political and military security alliance formed in 1949

NATO 20 [The North Atlantic Treaty Organization is an intergovernmental military alliance; “ABOUT NATO”; Last changed 2020 (addition of 30th country); <https://nato.usmission.gov/about-nato/>] //CH

Formed in 1949 with the signing of the Washington Treaty, NATO is a security alliance of 30 countries from North America and Europe. NATO’s fundamental goal is to safeguard the Allies’ freedom and security by political and military means. NATO remains the principal security instrument of the transatlantic community and expression of its common democratic values. It is the practical means through which the security of North America and Europe are permanently tied together. NATO enlargement has furthered the U.S. goal of a Europe whole, free, and at peace.

#### The North Atlantic Treaty Organization is a group of 30 countries – that’s external from individual member-states

NATO 22 [The North Atlantic Treaty Organization is an intergovernmental military alliance; “10 things you need to know about NATO”; 5/10/22; <https://www.nato.int/cps/en/natohq/126169.htm>] //CH

Collective defence: **The North Atlantic Treaty Organization (NATO)** was founded in 1949 and is a group of 30 countries from Europe and North America that exists to protect the people and territory of its members. The Alliance is founded on the principle of collective defence, meaning that if one NATO Ally is attacked, then all NATO Allies are attacked. For example, when terrorists attacked the United States on 9/11 2001, all NATO Allies stood with America as though they had also been attacked.

#### Even Canada agrees

Canada 22 [The government of Canada is the body responsible for the federal administration of Canada; “Canada and the North Atlantic Treaty Organization”; 06/21/22; <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/nato-otan/index.aspx?lang=eng>] //CH

The North Atlantic Treaty was signed in Washington on April 4, 1949, establishing the North Atlantic Treaty Organization (NATO). **This political and military alliance** was formed to promote the stability of the North Atlantic area and to safeguard the freedom of its peoples, based on the principles of democracy, individual liberty and the rule of law.

Overview of North Atlantic Treaty Organization

This political and military alliance was formed to promote the stability of the North Atlantic area and to safeguard the freedom of its peoples, based on the principles of democracy, individual liberty and the rule of law.

## \*\*AT: DOD Agent CPs\*\*

### 2AC – Perm/L to NB

#### The counterplan links to the net benefit

Arabia ’21 [Christina; May 17; CRS Analyst in Security Assistance, Security Cooperation and the Global Arms Trade; Congressional Research Service, “Defense Primer: DOD “Title 10” Security Cooperation,” https://sgp.fas.org/crs/natsec/IF11677.pdf]

SC: Roles and Responsibilities

Many SC activities require DOD to coordinate with multiple DOD components and other federal departments, primarily DOS. Some DOD SC activities require varying levels of coordination with DOS. Within DOD, the Undersecretary of Defense for Policy (USD[P]) exercises overall direction, authority, and control over SC matters.

The Defense Security Cooperation Agency (DSCA) represents the interests of the Secretary of Defense and USD(P) in SC matters and is tasked with directing, administering, and executing many SC programs, developing SC policy, and providing DOD-wide SC guidance. DSCA is also DOD’s main interlocutor between the PNs, implementing agencies, and the defense industry. The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD-SO/LIC) oversees and approves some SC training activities that are managed by DSCA. U.S. Special Operations Command (SOCOM) coordinates those SC activities executed by special operations forces (SOF). DOS leads U.S. foreign aid and has final say on SA. DOS’s Bureau of Political-Military Affairs (PM) is the principal link to DOD and ensures that SA is integrated with other U.S. policies and activities at the country, regional, and global levels. PM also determines PN eligibility, appropriate SA programs, and which defense articles and equipment are permitted for transfer.