# Topicality---Starter Pack 2022

**Resolved: The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in one or more of the following areas: artificial intelligence, biotechnology, cybersecurity.**

## Resolved

### Resolved---Formal Vote---2AC

#### “Resolved” means declaring by a vote.

Merriam ’7 [Merriam-Webster Online Dictionary; carbon dated January 7, 2007; “resolve verb,” https://www.merriam-webster.com/dictionary/resolved]

3a: to declare or decide by a formal resolution and vote

b: to change by resolution or formal vote

// the house resolved itself into a committee

### Resolved---Legislative---2NC

#### “Resolved” requires a legislative instrument.

LSA ’5 [Louisiana State Legislature; 2005; Governing body of the state of Louisiana; Louisiana State Legislature, “Legislative Glossary,” <https://www.legis.la.gov/legis/Glossary.aspx>]

Resolution

A legislative instrument that generally is used for making declarations, stating policies, and making decisions where some other form is not required. A bill includes the constitutionally required enacting clause; a resolution uses the term "resolved". Not subject to a time limit for introduction nor to governor's veto. (Const. Art. III, §17(B) and House Rules 8.11, 13.1, 6.8, and 7.4 and Senate Rules 10.9, 13.5 and 15.1)

### Resolved---Certain---2NC

#### “Resolved” means certain.

Oxford 20 – Oxford Advanced Learner's Dictionary, “resolved”, http://www.oxforddictionaries.com/us/definition/american\_english/resolved

Definition of resolved in English:

adjective

[PREDICATIVE, WITH INFINITIVE]

Firmly determined to do something:

Constance was resolved not to cry

## The United States Federal Government

### USFG---Singular Whole---1NC

#### “United States” is a singular noun referring to the whole

Dr. James R. Hurford 94, General Linguistics Professor at the University of Edinburgh, Grammar: A Student’s Guide, p. 224

Singular

Explanation

A singular noun or pronoun in a language typically refers to just one thing or person, or to a mass of stuff, rather than to a collection of things or people. Other nouns which occur in the same grammatical patterns as typical singular nouns may be classified as grammatically singular.

Examples

Some singular nouns in English are waiter, inability, objection, cat, frostbite, garlic, refusal, gatepost, liair and region.

The English personal pronouns I, he. she and it are singular.

Contrasts

Singular contrasts with plural. A word cannot simultaneously be both singular and plural.

Relationships Singular and plural in a language belong to its system of number. It is common in languages for singular to be the unmarked member of the system, and for plural nouns to have some special marker, such as a suffix; this is true of English, where, for instance, the noun dog is singular, and its plural is formed by adding an ~s. The singular is rarely formed by adding something in this way.

The basic parts of speech to which singular applies are nouns and pronouns; other parts of speech or word-classes may be marked as singular by agreement with a singular noun or pronoun. In English, only verbs and demonstratives show this agreement; this and that are singular demonstratives, and is and was are forms of the verb be which show singular agreement.

Among the nouns, mass nouns are always singular. So we may say *This stuff is sticky* and *That wine tastes of bananas*. Count nouns show the distinction between singular and plural. Thus we have singular/plural pairs such as *tree/trees*, *diagram/diagrams* and *burial/burials*. Proper names are almost always singular. Even proper names formed from plural common nouns, such as *the United States*, tend to be singular, as in *The United States is ready to defend its vital interests*.

### USFG---Singular Whole---2NC

#### It’s not one branch.

Arthur Miller 86. Distinguished Visiting Professor of Law – Emory University. Summer 1986. “Congress, the Constitution, and First Use of Nuclear Weapons.” Review of Politics. Vol. 48, No. 3.

Three other points merit mention in this discussion of collective decision-making. First, both the formal and the secret constitutions allocate power over foreign relations and defense to the central government, to, that is, the United States of America visualized as a single entity. What, however, is "the" United States? The question has never been definitively answered; and indeed has seldom been asked in judicial opinion or scholarly discourse.42 Asked another way, the question is this: Where does sovereignty lie in the American polity? The formal constitution is supposedly based on popular sovereignty, with ultimate power resting in the people. That, however, is far from accurate. Proof positive that sovereignty lies in the "state" came when General Robert E. Lee surrendered at Appomattox: "the people" of the South were not to be permitted to exercise their "sovereignty." The powers of the national government are supposedly only those delegated to it, either expressly or impliedly. But that is scarcely accurate, as 200 years of constitutional development attest. The Framers of the formal constitution established a governmental system that, as Justice Robert Jackson commented, would ensure that the dispersed powers of the federal government would be integrated into a workable government. "Separateness but interdependence, autonomy but reciprocity" was the constitutional command.43 The meaning is unmistakable: "the" United States is a single metaphysical entity, encompassing state, society, and government in one artificial being. These terms are not synonymous. The state is the fundamental entity; government its apparatus; and society is composed of the individuals and groups governed. Much like the business corporation, the state-"the" United States-is an artificial construct, more a method than a thing. It exists in constitutional theory-in, for example, the state secrets privilege in litigation-even though judges and commentators alike often confuse the term with government and with society. A legal fiction that by itself can do no act, speak no work, and think no thought, the state (like the corporation) has "no anatomical parts to be kicked or consigned to the calaboose; no soul for whose salvation the parson may struggle; no body to be roasted in hell or purged for celestial enjoyment." 44 Despite loose language to the contrary from executive branch lawyers and even the Supreme Court, "the" state or "the" government-or "the" United States-is not to be equated with the executive branch. Nor with any one branch, for that matter; each branch is part of an indivisible whole.

#### “Government” is a collective noun, meaning the whole body

Dr. Loreto Todd 5, Professor and Reader in International English at the University of Leeds & Author of More Than 20 Books on Linguistics & English Usage, International English Usage, Ed. Hancock and Todd, p. 133

The term *collective noun* refers to a singular noun that has a plural implication (e.g. [for example,] *government*) and is used when the whole body (and not the constituent members) is being considered. The category *collective nouns* is not discrete, and it can be argued that some usages are midway between collective and mass nouns. For example, *team* is clearly a collective noun and *butter* is clearly a mass noun but it is not so easy to decide the status of such nouns as: hair linen royalty.

### USFG---Not Singular Whole---2AC

#### “The United States federal government” does not necessitate whole-of-government action.

Chicago ’13 [Chicago Manual of Style; carbon dated June 23, 2013; Questions and Answers, “Headlines and Titles of Works?” https://www.chicagomanualofstyle.org/qanda/data/faq/topics/CapitalizationTitles/faq0015.html]

A. The government of the United States is not a single official entity. Nor is it when it is referred to as the federal government or the U.S. government or the U.S. federal government. It’s just a government, which, like those in all countries, has some official bodies that act and operate in the name of government: the Congress, the Senate, the Department of State, etc.

### USFG---Not Singular Whole---1AR

#### “The” means a member of its class.

Webster ’7 [Merriam Webster online dictionary; carbon dated 2007; “the,” <https://www.merriam-webster.com/dictionary/the>

b—used as a function word to indicate that a following noun or noun equivalent is a unique or a particular member of its class

### USFG---the Three Branches/Not States---1NC

#### The “United States federal government” precludes the states.

U.S. Legal ’16 [U.S. Legal; 2016; Organization offering legal assistance and attorney access; U.S. Legal, “United States Federal Government Law and Legal Definition,” <https://definitions.uslegal.com/u/united-states-federal-government/>]

The United States Federal Government is established by the US Constitution. The Federal Government shares sovereignty over the United Sates with the individual governments of the States of US. The Federal government has three branches: i) the legislature, which is the US Congress, ii) Executive, comprised of the President and Vice president of the US and iii) Judiciary. The US Constitution prescribes a system of separation of powers and ‘checks and balances’ for the smooth functioning of all the three branches of the Federal Government. The US Constitution limits the powers of the Federal Government to the powers assigned to it; all powers not expressly assigned to the Federal Government are reserved to the States or to the people.

### USFG---the Three Branches/Not States---2NC

#### “Federal government” is national.

Thompson ’21 [Thompson School District; 2021; Public school district for Loveland, Colorado and surrounding area; Thompson Schools, “Structures of Government,” <https://www.thompsonschools.org/cms/lib/CO01900772/Centricity/Domain/3627/Structures%20of%20Government.pdf>]

Australia, Switzerland, Canada, Mexico, Germany, India, and some 20 other stats also have federal forms of government today. In the United States, the term ‘Federal Government’ is often used to refer to the National Government, but note that the 50 state governments are unitary in structure, not federal.

## Should

### Should---Certain---1NC

#### “Should” is mandatory.

Keller ’32 [W.H.; July 14; Judge on the Superior Court of Pennsylvania; Westlaw, “Foresi v. Hudson Coal Co.,” 106 Pa.Super. 307]

As regards the mandatory character of the rule, the word “should” is not only an auxiliary verb, it is also the preterite of the verb, “shall,” and has for one of its meanings, as defined in the Century Dictionary: “Obliged or compelled (to); would have (to); must; ought (to); used with an infinitive (without to) to express obligation, necessity or duty in connection with some act yet to be carried out.” We think it clear that it is in that sense that the word “should” is used in this rule, not merely advisory. When the judge in charging a jury tells them that, unless they find from all the evidence, beyond a reasonable doubt, that the defendant is guilty of the offense charged, they should acquit, the word “should” is not used in an advisory sense, but has the force or meaning of “must,” or “ought to,” and carries with it the sense of \*313 obligation and duty equivalent to compulsion. A natural sense of sympathy for a few unfortunate claimants who have been injured while doing something in direct violation of law must not be so indulged as to fritter away, or nullify, provisions which have been enacted to safeguard and protect the welfare of thousands who are engaged in the hazardous occupation of mining.

### Should---Certain---2NC

#### “Should” is obligatory, NOT advisory.

Riddle ’14 [Finis E; December 22; Justice on the Supreme Court of Oklahoma; Westlaw, “St. Louis & S. F. R. Co. v. Brown,” 45 Okla. 143]

The specific grounds of objection are that the court should have used the word “shall” instead of “should,” that the word “should” is merely advisory, and that the jury was left at its discretion in the matter of reduction of the damages. It has been said that the word “should” is the past tense of the word “shall,” and we think, in the connection in which it was used, the jury understood that it meant more than simply advisory.

In the case of Smith v. State, 142 Ind. 288, 41 N. E. 595, the Supreme Court of Indiana held that it was more imperative than the word “may.”

In the case of Lynch v. Bates, 139 Ind. 206, 38 N. E. 806, where the court charged the jury that in passing upon the weight of the evidence, etc., they “should” take into consideration \*1081 the interest of the witness, etc., the court reversed the case, holding that the word “should” there was too imperative.

In the case of Durand's Adm'r v. N. Y. & L. B. R. Co., 65 N. J. Law, 656, 48 Atl. 1013, the court held that the word “should” implies the performance of some obligation or duty. Often the word “shall” is used to mean “may.” So, it will be seen that either of the terms cannot be considered abstractly, but must be considered in connection with the subject-matter and sense in which it is used.

#### “Should” means “must.”

Stroud ’2k [John F Jr; July 7; Judge on the Court of Appeals of Arkansas; Westlaw, “Guest v. San Pedro,” 70 Ark. App. 389]

The interpretation of this section, which appears to be a question of first impression, turns upon the meaning of the word “should” in the phrase “[a]ny partial abatement or reduction of child support should not exceed 50% of the child-support obligation during the extended visitation period.” In Little v. State, 261 Ark. 859, 554 S.W.2d 312 (1977), the supreme court ruled that the trial court, giving an instruction on circumstantial evidence, had not misled the jury by using the word “should” instead of “must” in stating that circumstances should point to and be consistent with guilt but should be inconsistent with any other reasonable hypothesis. The Little court opined that use of the word “must” would have been preferable to the use of “should,” but the court noted that the \*396 words are often synonymous. 261 Ark. at 884, 554 S.W.2d at 324, citing Rodale, The Synonym Finder 780 (Special Deluxe Ed.).

Similarly, we hold that the word “should” is equivalent to the word “must” as used in the phrase “any partial abatement or reduction of child support should not exceed 50% of the child-support obligation during the extended visitation period.” We hold that the 50% limitation in Administrative Order No. 10 is mandatory: abatement or reduction of child support during an extended visitation period cannot exceed 50% of the child-support obligation during the extended visitation period.

### Should---AT: Certain---2AC

#### “Should” is advisory, not certain. It also equals “ought.”

Richman ’16 [James; August 17; Judge on the Second Circuit, California’s Court of Appeals; Westlaw, “Marin Assn. of Pub. Emps. v. Marin Cty. Employees' Ret. Assn.,” 2 Cal. App. 5th 674]

There is, of course, no bar to the Supreme Court adopting a Court of Appeal's reasoning as its own. Yet there is legitimate reason to question whether that was what the Supreme Court intended in 1983. First, as just shown, only the least authoritative of the three sources cited \*\*385 actually supports the word “must,” while the two Supreme Court decisions employ “should.” Second, barely a month later, the Supreme Court—speaking though the same justice—filed another decision which used the “should” formulation from the 1955 Allen decision as quoted in Abbott.20 Third, the 1983 Allen decision involved retirees (and Flournoy the widow of a retiree), who historically receive a heightened degree of judicial protection. (See fn. 19, ante.) Fourth, and most significantly, the “must” formulation has never been reiterated by the Supreme Court, which has instead uniformly employed the “should” \*699 language from the 1955 Allen decision. (Olson v. Cory, supra, 27 Cal.3d 532, 541, 178 Cal.Rptr. 568, 636 P.2d 532 [“Although an employee does not obtain any ‘absolute right to fixed or specific benefits ... there [are] strict limitation[s] on the conditions which may modify the pension system in effect during employment.’ [Citation.] Such modifications must be reasonable and any ‘ “changes in a pension plan which result in disadvantage to employees should be accompanied by comparable new advantages” ’ ”]; Legislature v. Eu (1991) 54 Cal.3d 492, 529–530, 286 Cal.Rptr. 283, 816 P.2d 1309 [quoting Olson]; City of Huntington Beach v. Board of Administration (1992) 4 Cal.4th 462, 472, 14 Cal.Rptr.2d 514, 841 P.2d 1034 [“changes in a pension plan which result in disadvantage to employees should be accompanied by comparable new advantages,” citing Allen v. City of Long Beach, supra, 45 Cal.2d 128, 131, 287 P.2d 765].)

It thus appears unlikely that the Supreme Court's use of “must” in the 1983 Allen decision was intended to herald a fundamental doctrinal shift. “Should,” not “must,” remains the court's preferred expression. And “should” does not convey imperative obligation, no more compulsion than “ought.” (Lashley v. Koerber (1945) 26 Cal.2d 83, 90, 156 P.2d 441; see People v. Webb (1986) 186 Cal.App.3d 401, 409, fn. 2, 230 Cal.Rptr. 755 [“the word ‘should’ is advisory only and not mandatory”].) In plain effect, “should” is “a recommendation, not ... a mandate.” (Cuevas v. Superior Court (1976) 58 Cal.App.3d 406, 409, 130 Cal.Rptr. 238.)

### Should---AT: Certain---1AR

#### “Should” is not certain.

White ’26 [Warren L; January 8; Judge on the Springfield Court of Appeals of Missouri; Westlaw, “Hubbard v. Turner Department Store Co.,” 220 Mo.App. 95]

3 The verb “should” has various shades of meaning. In its ordinary meaning it does not express certainty as the word “will” sometimes does. In the telegram under consideration it seems to be used in the sense that, from the anticipated profits, plaintiff might receive a bonus of $25 to $50 per month. It is nothing more than an expression of opinion, with no definite assurance that such would be the result. The expression, “twenty–five to fifty dollars per month extra,” adds nothing to the certainty or definiteness of the proposal but is merely suggestive. The whole expression, “a part of profits that should mean from twenty–five to fifty dollars per month extra, to our minds cannot possibly be construed as guaranty or an unconditional promise to pay a minimum of $25 per month or a maximum of $50 per month out of the profits, in addition to the agreed salary. It is merely suggestive. Moreover, no method is provided for determining what the share of plaintiff in the profits might be; no per cent. is named. Whether net or gross profits or whether profits from the whole store or only the furniture department, were to be the basis of settlement, is all left to conjecture. There is no stipulation as to when settlements were to be made, which, obviously, might be either weekly, monthly, annually, or whenever the employment should cease. The expression in the telegram, “if you want to come and work hard, we will take care of you in good shape,” avails plaintiff nothing from the standpoint of law. The whole telegram is one well calculated to mislead, whether deliberate or not. Morally, defendant was under some obligation to increase plaintiff's salary in the event the concern prospered and plaintiff worked hard; but, legally, we are confronted with an insurmountable obstacle in so far as affording relief to plaintiff is concerned. It is an elemental and fundamental rule of law that a contract, to be valid, “must be certain and unequivocal in its essential terms, either within itself or by reference to some other agreement or matter.” 6 R. C. L. 644; 9 Cyc. 245; 18 R. C. L. 494; Burks v. Stam, 65 Mo. App. 455; Blaine v. Knapp & Co., 140 Mo. 241, 41 S. W. 787; United Press v. New York Press Co., 164 N. Y. 406, 58 N. E. 527, 53 L. R. A. 288; Varney v. Ditmars, 217 N. Y. 223, 111 N. E. 822, Ann. Cas. 1916B, 758.

### Should---Immediate---1NC

#### “Should” is immediate.

Summers ’94 [Edward; November 8; Justice of the Oklahoma Supreme Court; Oklahoma State Courts Network, “Kelsey v. Dollarsaver Food Warehouse of Durant,” <https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287#marker3fn13>]

4 The legal question to be resolved by the court is whether the word "should" [13](https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287#marker3fn13) in the May 18 order connotes futurity or may be deemed a ruling in praesenti.[14](https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287" \l "marker3fn14) The answer to this query is not to be divined from rules of grammar;[15](https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287" \l "marker3fn15) it must be governed by the age-old practice culture of legal professionals and its immemorial language usage. To determine if the omission (from the critical May 18 entry) of the turgid phrase, "and the same hereby is", 1 -- makes it an in futuro ruling - i.e., an expression of what the judge will or would do at a later stage - or 2 -- constitutes an in in praesenti resolution of a disputed law issue, the trial judge's intent must be garnered from the four corners of the entire record.[16](https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287" \l "marker3fn16)

Footnote 13:

[13](https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287#marker2fn13) "Should" not only is used as a "present indicative" synonymous with ought but also is the past tense of "shall" with various shades of meaning not always easy to analyze. See 57 C.J. Shall § 9, Judgments § 121 (1932). O. JESPERSEN, GROWTH AND STRUCTURE OF THE ENGLISH LANGUAGE (1984); St. Louis & S.F.R. Co. v. Brown, 45 Okl. 143, 144 P. 1075, 1080-81 (1914). For a more detailed explanation, see the Partridge quotation infra note 15.

Certain contexts mandate a construction of the term "should" as more than merely indicating preference or desirability. Brown, supra at 1080-81 (jury instructions stating that jurors "should" reduce the amount of damages in proportion to the amount of contributory negligence of the plaintiff was held to imply an obligation and to be more than advisory); Carrigan v. California Horse Racing Board, 60 Wash. App. 79, [802 P.2d 813](https://www.oscn.net/applications/oscn/deliverdocument.asp?box1=802&box2=P.2D&box3=813) (1990) (one of the Rules of Appellate Procedure requiring that a party "should devote a section of the brief to the request for the fee or expenses" was interpreted to mean that a party is under an obligation to include the requested segment); State v. Rack, 318 S.W.2d 211, 215 (Mo. 1958) ("should" would mean the same as "shall" or "must" when used in an instruction to the jury which tells the triers they "should disregard false testimony").

Footnote 14:

[14](https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=20287#marker2fn14) In praesenti means literally "at the present time." BLACK'S LAW DICTIONARY 792 (6th Ed. 1990). In legal parlance the phrase denotes that which in law is presently or immediately effective, as opposed to something that will or would become effective in the future [in futurol]. See Van Wyck v. Knevals, [106 U.S. 360](https://www.oscn.net/applications/oscn/deliverdocument.asp?box1=106&box2=U.S.&box3=360), 365, 1 S.Ct. 336, 337, 27 L.Ed. 201 (1882).

### Should---AT: Immediate---2AC

#### “Should” refers to the future.

Brown ’8 [Mary Ann Brown; May 14; Judge on the Court of Appeals of Iowa; Westlaw, “In re Est. of Guthrie,” 752 N.W.2d 452]

Brock and Kaitlyn look to the word “should” in the phrase “in the event any of my children should predecease me” and claim the district court improperly found the word looked to the future. They claim the word should be interpreted as the past tense of “shall” to imply a duty or obligation. See Black's Law Dictionary 1379 (6th ed.1990). Looking at the phrase as a whole, however, rather than at a single word, we determine the phrase is considering possible future events. See In re Estate of Grulke, 546 N.W.2d 626, 627 (Iowa Ct.App.1996) (noting we must ascertain a testator's intent from the entire will).

## Substantially Increase

### Substantially Increase---Considerably---2AC

#### “Substantially increase” means make considerably greater.

Viviano ’13 [David; July 29; Justice for the Supreme Court of Michigan; Lexis, “People v. Hardy,” 494 Mich. 430]

The phrase begins with the words "conduct designed." HN8 "Designed" means "to intend for a definite purpose."25 Thus, the word "designed" requires courts to evaluate the intent motivating the defendant's conduct.26 Next, we come to the words "substantially increase." "Substantial" means "of ample or considerable amount, quantity, size, etc."27 To "increase" means "to make greater, as in number, size, strength, or quality; augment."28 Applying these definitions to the relevant text, we conclude that HN9 it is proper to assess points under OV 7 for conduct that was intended to make a victim's fear or anxiety greater by a considerable amount.29

### Substantially Increase---Considerably---1AR

#### “Substantially increase” means making considerably greater.

Beckering ’19 [Jane N; March 28; Court of Appeals Judge in the State of Michigan; Westlaw, “People v. Guthrie,” No. 341269, 2019 WL 1411111]

The Hardy Court addressed what is required to establish that a defendant engaged in conduct “designed to substantially increase the fear and anxiety a victim suffered during the offense,” reasoning as follows:

The phrase begins with the words “conduct designed.” “Designed” means “to intend for a definite purpose.” Thus, the word “designed” requires courts to evaluate the intent motivating the defendant's conduct. Next, we come to the words “substantially increase.” “Substantial” means “of ample or considerable amount, quantity, size, etc.” To “increase” means “to make greater, as in number, size, strength, or quality; augment.” Applying these definitions to the relevant text, we conclude that it is proper to assess points under OV 7 for conduct that was intended to make a victim's fear or anxiety greater by a considerable amount. [Hardy, 494 Mich. at 440-441, 835 N.W.2d 340.]

## Substantially

### Substantially---Not All/AT: Subsets---2AC

#### “Substantially” includes subsets and can be either quantitative or qualitative.

Sotomayor ’17 [Sonya; February 22; Justice of the Supreme Court of the United States, J.D. from Yale University, A.B. in History from Princeton University; Justia, “Life Technologies Corp. v. Promega Corp., 580 U.S. \_\_\_ (2017),” <https://supreme.justia.com/cases/federal/us/580/14-1538/#tab-opinion-3694340>]

The threshold determination to be made is whether §271(f)(2)’s requirement of “a substantial portion” of the components of a patented invention refers to a quantitative or qualitative measurement. Life Technologies and the United States argue that the text of §271(f)(1) establishes a quantitative threshold, and that the threshold must be greater than one. Promega defends the Federal Circuit’s reading of the statute, arguing that a “substantial portion” of the components includes a single component if that component is sufficiently important to the invention.

We look first to the text of the statute. Sebelius v. Cloer, 569 U. S. \_\_\_, \_\_\_ (2013) (slip op., at 6). The Patent Act itself does not define the term “substantial,” and so we turn to its ordinary meaning. Ibid. Here we find little help. All agree the term is ambiguous and, taken in isolation, might refer to an important portion or to a large portion. Brief for Petitioners 16; Brief for Respondent 18; Brief for United States as Amicus Curiae 12. “Substantial,” as it is commonly understood, may refer either to qualitative importance or to quantitatively large size. See, e.g., Webster’s Third New International Dictionary 2280 (defs. 1c, 2c) (1981) (Webster’s Third) (“important, essential,” or “considerable in amount, value, or worth”); 17 Oxford English Dictionary 67 (defs. 5a, 9) (2d ed. 1989) (OED) (“That is, constitutes, or involves an essential part, point, or feature; essential, material,” or “Of ample or considerable amount, quantity, or dimensions”).

### Substantially---Not All/AT: Subsets---1AR

#### “Substantially” means greatly, NOT entirely.

Burke ’12 [Christopher; April 27; United States Magistrate Judge; Westlaw, “Virgin Atl. Airways Ltd. v. Delta Airlines, Inc.,” No. CIV.A. 11-61-LPS-CJB, WL 1636147]

The Court agrees, and finds that such a result would be at odds with the established law. See, e.g., Circle R, Inc. v. Trail King Indus., Inc., 21 F. App'x 894, 898 (Fed.Cir.2001) (reversing a district court decision that construed the phrase “substantially flat” to mean “entirely flat”); York Prods., Inc. v. Cent. Tractor Farm & Family Ctr., 99 F.3d 1568, 1572–73 (Fed.Cir.1996) (construing “substantially the entire height” as “nearly the entire height”). The adverb “substantially” is typically defined to mean “to a great or significant extent,” or “for the most part; essentially.”4 The adjective “flat” is typically defined to mean “smooth and even; without marked lumps to indentations” or “having a broad level surface.”5 These ordinary definitions are generally consistent with the patent specification discussed at length above, which depicts and describes seat-to-bed systems with constituent surfaces that are close to, though not entirely, flat. (See ′861 patent, col. 9–10; col. 13 (describing multiple embodiments with “substantially flat” passenger-bearing surfaces that are composed of “substantially coplanar[ ] and contiguous” surfaces)6 As such, although the patent specification and claims lead to the inescapable conclusion that the claimed “substantially flat bed” must consist of surfaces that are flat to a great extent, those surfaces need not be precisely so. (See, e.g., id., col. 33:12–17; 36:32–33; 43:7–8; 46:54–56).

Footnote 4 begins:

See http://oxforddictionaries.com/definition/substantially; http://www.wordreference.com/definition/substantially; see also http:// www.merriam-webster.com/dictionary/substantially (“being largely but not wholly that which is specified”). Cf. Circle R, 21 F. App'x at 898 (citing similar definitions for “substantially”); York Prods., 99 F.3d at 1572–73 (same).

#### “Substantially” does not mean wholly.

Zoss ’98 [Paul; November 16; Magistrate Judge on the United States District Court for the Northern District of Iowa; Lexis, “Bailey v. United States,” 39 F. Supp. 2d 1132, 1138]

To do this, the court will need a working definition of the terms "substantial" and "substantially." Courts have given these terms widely different meanings, depending on the context. See Victor v. Nebraska, 511 U.S. 1, 19, 114 S. Ct. 1239, 1250, 127 L. Ed. 2d 583 (1994) ("substantial" means either "not seeming or imaginary" or "that specified to a large degree" in the context of a reasonable doubt instruction, citing Webster's Third New International Dictionary 2280 (1981)); Kluener v. Commissioner of Internal Revenue, 154 F.3d 630, 637 (6th Cir. 1998) ("substantial" means something less than a preponderance, but more than a mere reasonable basis, citing 26 C.F.R. P1.6662-4(d)(3) (1997)); Id., at 639 ("substantial" means "considerable" or "ample"); Canyon Air Tour Coalition v. Federal Aviation Administration, 332 U.S. App. D.C. 133, 154 F.3d 455, 474 (D.C. Cir. 1998) ("substantial" may well be defined as meaning "more than half," "being that specified to a large degree or in the main," "not seeming or imaginary," "considerable in amount"); York Products, Inc. v. Central Tractor Farm & Family Center, 99 F.3d 1568, 1572-73 (Fed. Cir. 1996) ("substantially" means "considerable in . . . extent," citing American Heritage Dictionary Second College Edition 1213 (2d ed. 1982) or "largely but not wholly that which is specified," citing Webster's Ninth New Collegiate Dictionary 1176 (9th ed. 1983)); Koch v. United States, 47 F.3d 1015, 1021 (10th Cir. 1995) ("substantially" means "justified in substance or in the main -- that is, justified to a degree that could satisfy a reasonable person." (citations omitted)); Laitram Machinery, Inc. v. Carnitech, 884 F. Supp. 1074, 1085 (E.D.La. 1995) (definition of "substantially" in a patent case is a jury question); C.E. Equipment Co., Inc. v. United States, 17 Cl. Ct. 293, 299 (1989) ("substantially" means "less than totally"); Darlington v. Studebaker-Packard Corporation, 191 F. Supp. 438, 439 (N.D. Ind 1961) ("The word 'substantially' is a relative term and should be interpreted in accordance with context of claim in which it is used."). At trial, the court will expect the parties to propose appropriate definitions for these terms for the court to use in deciding this case.

### Substantially---Certain---1NC

#### “Substantially” is certain.

Shepard ’98 [Justice Shepard on the Appellate Court of Illinois, First District; March 1, 1898; Westlaw, “Bass v. Pease,” 79 Ill. App. 308]

“Outward,” “open,” “actual,” “visible,” “substantial” and “exclusive” mean, in the connection that they are employed in the cases referred to, substantially the same thing. They mean “not concealed,” “not hidden, exposed to view,” “free from concealment, dissimulation, reserve or disguise;” “in full existence; denoting that which not merely can be, but is, opposed to potential, apparent, constructive and imaginary;” “veritable, genuine, certain, absolute;” “real, at present time, as a matter of fact;” “not merely nominal, opposed to form,” ““actually existing, true;” “not including, admitting or pertaining to any others; undivided, sole;” “opposed to inclusive.” Anderson's Law Dictionary and The Century Dictionary, under appropriate headings.

### Substantially---Certain---2NC

#### Same card, but from Words and Phrases.

Words and Phrases ’4 [Words and Phrases; 1904; Collected, Edited, and Compiled by the Members of the Editorial Staff of the National Reporter System; Judicial and Statutory Definitions of Words and Phrases, “Outward,” vol. 7, p. 5124]

The words “outward,” "open,” “actual,” “visible,” “substantial,” and “exclusive,” in connection with a change of possession, mean substantially the same thing. They mean not concealed, not hidden, exposed to view; free from concealment, dissimulation, reserve, or disguise; in full existence; denoting that which not merely can be, but is opposed to potential, apparent, constructive, and imaginary; veritable, genuine, certain, absolute, real at present time, as a matter of fact not merely nominal, opposed to form, actually existing, true; not including, admitting, or pertaining to any others; undivided, sole, opposed to inclusive. Base v. Pease, 79 III App. 308, 318.

#### Same card mostly, but from a policy debate textbook.

Edwards ’8 [Richard; 2008; Professor of Communication Studies at Baylor University, Ph.D. in Communication Studies from the University of Iowa; Competitive Debate: The Official Guide, “Policy Debate Final Round,” p. 227]

And, “substantial” means the increase must be definite. Potential future increases are not topical. Words and Phrases, 1964, accessed online: “Substantial means not concealed, denoting that which not merely can be, but is supposed to be, potential, certain, absolute, real at the present time.”

### Substantially---Considerably---2AC

#### “Substantially” means “considerably.”

O’Connor ’2 [Sandra Day; January 8; Justice on the Supreme Court; Westlaw, “Toyota Motor Mfg., Kentucky, Inc. v. Williams,” 534 U.S. 184]

Our consideration of this issue is guided first and foremost by the words of the disability definition itself. “[S]ubstantially” in the phrase “substantially limits” suggests “considerable” or “to a large degree.” See Webster's Third New International Dictionary 2280 (1976) (defining “substantially” as “in a substantial manner” and “substantial” as “considerable in amount, value, or worth” and “being that specified to a large degree or in the main”); see also 17 Oxford English Dictionary 66–67 (2d ed.1989) (“substantial”: “[r]elating to \*197 or proceeding from the essence of a thing; essential”; “[o]f ample or considerable amount, quantity, or dimensions”). The word “substantial” thus clearly precludes impairments that interfere in only a minor way with the performance of manual tasks from qualifying as disabilities. Cf. Albertson's, Inc. v. Kirkingburg, 527 U.S., at 565, 119 S.Ct. 2162 (explaining that a “mere difference” does not amount to a “significant restric[tion]” and therefore does not satisfy the EEOC's interpretation of “substantially limits”).

### Substantially---Considerably---1AR

#### “Substantially” is NOT a term of art, so you should avoid defining it in a limiting fashion.

Arkush ’2 [David; January 1; J.D. Candidate at Harvard Law School; Harvard Civil Rights-Civil Liberties Law Review, “Preserving "Catalyst" Attorneys' Fees Under the Freedom of Information Act in the Wake of Buckhannon Board and Care Home v. West Virginia Department of Health and Human Resources,” vol. 37, p. 151]

Since the Supreme Court appears to have emphasized the classification in Buckhannon,(FN96) plaintiffs may find it useful or necessary to discuss whether "substantially prevail" is a legal term of art. The only clear consequence of classification as a "legal term of art" is that courts may be more likely to consult Black's Law Dictionary to define such words. The Buckhannon Court declared "prevailing party" a term of art and seems to have relied heavily on the 1997 edition of Black's, which defined the phrase as a "party in whose favor judgment is rendered."(FN97) Justice Scalia's concurrence similarly emphasized the special status of the term "prevailing party," writing, "[w]ords that have acquired a specialized meaning in the legal context must be accorded their legal meaning."(FN98)

Plaintiffs should argue that the term "substantially prevail" is not a term of art because if considered a term of art, resort to Black's 7th produces a definition of "prevail" that could be interpreted adversely to plaintiffs.(FN99) It is commonly accepted that words that are not legal terms of art should be accorded their ordinary, not their legal, meaning,(FN100) and ordinary-usage dictionaries provide FOIA fee claimants with helpful arguments. The Supreme Court has already found favorable, temporally relevant definitions of the word "substantially" in ordinary dictionaries:

"[S]ubstantially" suggests "considerable" or "specified to a large degree." See Webster's Third New International Dictionary 2280 (1976) (defining "substantially" as "in a substantial manner" and "substantial" as "considerable in amount, value, or worth" and "being that specified to a large degree or in the main"); see also 17 Oxford English Dictionary 66-67 (2d ed. 1989) ("substantial": "[r]elating to or proceeding from the essence of a thing; essential"; "of ample or considerable amount, quantity or dimensions").(FN101)

### Substantially---Not Covert---1NC

#### Interpretation – the plan must be public.

#### “Substantial” increases in cooperation cannot be concealed

Words and Phrases 64 (40W&P 759)

The words" outward, open, actual, visible, substantial, and exclusive," in connection with a change of possession, mean substantially the same thing. They mean not concealed; not hidden; exposed to view; free from concealment, dissimulation, reserve, or disguise; in full existence; denoting that which not merely can be, but is opposed to potential, apparent, constructive, and imaginary; veritable; genuine; certain: absolute: real at present time, as a matter of fact, not merely nominal; opposed to form; actually existing; true; not including, admitting, or pertaining to any others; undivided; sole; opposed to inclusive.

#### Limits and ground – secrecy adds a proliferation of internal modifications and delete core functional generics, undermining research and clash.

### Substantially---Not Covert---2NC

#### “Substantially” excludes covert action.

Edwards ‘8 [Richard; 2008; Professor of Communication Studies at Baylor University, Ph.D. in Communication Studies from the University of Iowa; Competitive Debate: The Official Guide, “Policy Debate Final Round,” p. 227]

And, “substantial” means the increase must be definite. Potential future increases are not topical. Words and Phrases, 1964, accessed online: “Substantial means not concealed, denoting that which not merely can be, but is supposed to be, potential, certain, absolute, real at the present time.”

#### “Substantially” excludes covert action.

Shepard ’98 [Justice Shepard on the Appellate Court of Illinois, First District; March 1, 1898; Westlaw, “Bass v. Pease,” 79 Ill. App. 308]

“Outward,” “open,” “actual,” “visible,” “substantial” and “exclusive” mean, in the connection that they are employed in the cases referred to, substantially the same thing. They mean “not concealed,” “not hidden, exposed to view,” “free from concealment, dissimulation, reserve or disguise;” “in full existence; denoting that which not merely can be, but is, opposed to potential, apparent, constructive and imaginary;” “veritable, genuine, certain, absolute;” “real, at present time, as a matter of fact;” “not merely nominal, opposed to form,” ““actually existing, true;” “not including, admitting or pertaining to any others; undivided, sole;” “opposed to inclusive.” Anderson's Law Dictionary and The Century Dictionary, under appropriate headings.

### Substantially---AT: Not Covert---2AC

#### Contextually, action in defense alliances like NATO can be secret.

Rapp-Hooper 15 – Mira Rapp-Hooper, Political Science PhD at Columbia University (earned by submitting this paper), Political Science MPhil at Columbia University. [Absolute Alliances: Extended Deterrence in International Politics, PhD thesis at Columbia University, https://doi.org/10.7916/D85Q4TWX]//BPS

Defense pacts may be symmetric or asymmetric, both in terms of the capabilities of member states and in terms of treaty obligations. They may form between major and minor powers, or between equals, and the treaty obligations may vary between partners or may be identical. If defense pacts specify an alliance duration when they enter into force, the mean specified length is seven and one-half years. In actuality, a typical defense pact lasts for about 20 years.36 Most defense pacts are public, but occasionally states sign defensive alliances in which part or all of the treaty is kept secret.37 Moreover, many defense pacts are quite specific—approximately half of non-security guarantee defense pacts specify an adversary, theater, alliance, or particular military contingency as the target of the pact.38

Footnote 37 begins:

37 Approximately 12% of all non-security guarantee defense pacts have secret clauses or are secret in their entirety.

#### Private talks can limit a public treaty.

James D. Morrow 2K, PhD, Professor, Poli Sci, Stanford University, June 2000, "Alliances: Why Write Them Down?", Annual Review of Political Science, Vol. 3, https://www.annualreviews.org/doi/10.1146/annurev.polisci.3.1.63

Signaling could also occur within alliances. Secret alliances pose a particular problem for this argument; how can something private signal information (Ritter 2000)? Often, there may be a problem of uncertainty between possible allies. They may not know the extent of one another's commitment. Private talks that limit the applicability of the alliance address some of the problems of entrapment and abandonment by allowing each ally to declare what interests it is willing to fight for, allowing the other to adjust its actions accordingly. Secrecy would be a benefit because the allies might not wish to communicate the limits of their commitment to states outside the alliance. This concern could lead to secret provisions appended to a public treaty.

#### U.S. law treats MOUs as binding treaty obligations concluded by the executive

Barrett ’20 [Jill; 2020; Visiting Reader in the School of Law at Queen Mary University of London; and Robert Beckman, Emeritus Professor of Law at the National University of Singapore; Handbook on Good Treaty Practice, p. 105]

The Name of the Document Does Not Determine its Legal Status

A document which meets the legal criteria for being a treaty is a treaty, whatever its particular designation. No matter how non-binding the title sounds, if the content and context make clear that it is governed by international law, it may be a treaty. Conversely, a document could be entitled ‘treaty’ or ‘agreement’, but if it is evident from its contents or context that it is not governed by international law, it is not a treaty. This can make the task of distinguishing treaties from non-binding international instruments difficult. The document signed by the Foreign Minister of Bahrain which was interpreted by the ICJ as a binding agreement to take the dispute with Qatar to the ICJ, was called ‘Minutes’. Minutes of meetings do not usually have treaty status, but if an internationally binding agreement is entered into at the meeting, the record of the meeting could bind the parties.

The title ‘MOU’ is particularly apt to cause confusion. In the practice of many States, this title is used only for instruments which they consider to be political rather than legal. The practice of some States on this point is so consistent that the use of the title MOU may be taken as an indication of their intention that the instrument not be governed by international law. For example, Australia, Canada, New Zealand and the UK and many other States follow the same practice in this regard. However, in the practice of some other States, the title MOU is used for agreements which are treaties under international law, but which are classified for domestic law purposes as executive agreements (meaning that the approval of the legislature is not required). The United States, for example, follows this practice. When States with different practices conclude an MOU, it may be a treaty or it may not. Unsurprisingly, perhaps, some States appear to have no consistent practice, using the term MOU without regard to whether or not the document is intended to be a treaty. Some, such as New Zealand, seek to avoid using the title MOU at all because of the confusion it has generated.64

### Substantially---Immediate---1NC

#### “Substantially” is immediate.

Shepard ’98 [Justice Shepard on the Appellate Court of Illinois, First District; March 1, 1898; Westlaw, “Bass v. Pease,” 79 Ill. App. 308]

“Outward,” “open,” “actual,” “visible,” “substantial” and “exclusive” mean, in the connection that they are employed in the cases referred to, substantially the same thing. They mean “not concealed,” “not hidden, exposed to view,” “free from concealment, dissimulation, reserve or disguise;” “in full existence; denoting that which not merely can be, but is, opposed to potential, apparent, constructive and imaginary;” “veritable, genuine, certain, absolute;” “real, at present time, as a matter of fact;” “not merely nominal, opposed to form,” ““actually existing, true;” “not including, admitting or pertaining to any others; undivided, sole;” “opposed to inclusive.” Anderson's Law Dictionary and The Century Dictionary, under appropriate headings.

### Substantially---Immediate---2NC

#### “Substantially” means immediately.

Words and Phrases ’4 [Words and Phrases; 1904; Collected, Edited, and Compiled by the Members of the Editorial Staff of the National Reporter System; Judicial and Statutory Definitions of Words and Phrases, “Outward,” vol. 7, p. 5124]

The words “outward, open, actual, visible, substantial, and exclusive,” in connection with a change of possession, mean substantially the same thing. They mean not concealed; not hidden; exposed to view; free from concealment, dissimulation, reserve, or disguise; in full existence; denoting that which not merely can be, but is opposed to potential, apparent, constructive, and imaginary; veritable; genuine; certain; absolute; real at present time, as a matter of fact, not merely nominal; opposed to form; actually existing; true; not including admitting, or pertaining to any others; undivided; sole; opposed to inclusive. Bass v. Pease, 79 Ill. App. 308, 318.

### Substantially---Not Numerical---2AC

#### “Substantially increase” doesn’t imply a numerical cutoff.

Hartmann ’7 [August 20; Hon; Judge in the High Court of Hong Kong; Legal Reference System, “In the High Court of the Hong Kong Special Administrative Region Court of First Instance Matrimonial Causes No. 6 of 2007,” <https://legalref.judiciary.hk/lrs/common/ju/ju_frame.jsp?DIS=58463&currpage=T>]

19. The word ‘substantial’ is not a technical term nor is it a word that lends itself to a precise measurement. In an earlier judgment on this issue, that of S. v. S. [2006] 3 HKLRD 251, I said that it is not a word —

“… that lends itself to precise definition or from which precise deductions can be drawn. To say, for example, that ‘there has been a substantial increase in expenditure’ does not of itself allow for a calculation in numerative terms of the exact increase. It is a statement to the effect that it is certainly more than a little but less than great. It defines, however, a significant increase, one that is weighty or sizeable.”

### Substantially---Not Numerical---1AR

#### Throw out cutoffs.

Prost ’4 [Sharon; June 18; Federal Court of Appeals Judge on the Federal Circuit; Westlaw, “Comm. for Fairly Traded Venezuelan Cement v. United States,” 372 F.3d 1284]

The URAA and the SAA neither amend nor refine the language of § 1677(4)(C). In fact, they merely suggest, without disqualifying other alternatives, a “clearly higher/substantial proportion” approach. Indeed, the SAA specifically mentions that \*1290 no “precise mathematical formula” or “ ‘benchmark’ proportion” is to be used for a dumping concentration analysis. SAA at 860 (citations omitted); see also Venez. Cement, 279 F.Supp.2d at 1329–30. Furthermore, as the Court of International Trade noted, the SAA emphasizes that the Commission retains the discretion to determine concentration of imports on a “case-by-case basis.” SAA at 860. Finally, the definition of the word “substantial” undercuts the CFTVC's argument. The word “substantial” generally means “considerable in amount, value or worth.” Webster's Third New International Dictionary 2280 (1993). It does not imply a specific number or cut-off. What may be substantial in one situation may not be in another situation. The very breadth of the term “substantial” undercuts the CFTVC's argument that Congress spoke clearly in establishing a standard for the Commission's regional antidumping and countervailing duty analyses. It therefore supports the conclusion that the Commission is owed deference in its interpretation of “substantial proportion.” The Commission clearly embarked on its analysis having been given considerable leeway to interpret a particularly broad term.

#### Percentages are arbitrary.

Viscasillas ’4 [Pilar; October 24; Professor at the Universidad Carlos III de Madrid; CISG Advisory Council Opinion, “Contracts for the Sale of Goods to Be Manufactured or Produced and Mixed Contracts (Article 3 CISG),” <http://cisgac.com/default.php?ipkCat=128&ifkCat=146&sid=146>]

2.8. Legal writers who follow the economic value criterion have generally quantified the term "substantial part" by comparing Article 3(1) CISG (substantial) with Article 3(2) CISG (preponderant): substantial being less than preponderant. In this way, legal writers have used the following percentages to quantify substantial: 15%,[14] between 40% and 50%,[15] or more generally 50%.[16] At the same time, other authors, although they have not fixed any numbers in regard to the quantification of the term "substantial" have declared that "preponderant" means "considerably more than 50% of the price" or "clearly in excess of 50%".[17] Thus it seems that for the latter authors, the quantification of the term "substantial" is placed above the 50% figure. Also, some Courts have followed this approach.[18]

2.9. To consider a fixed percentage might be arbitrary due to the fact that the particularities of each case ought to be taken into account; that the scholars are in disagreement; and that the origin of those figures is not clear.[19]

Therefore, it does not seem to be advisable to quantify the word "substantial" a priori in percentages. A case-by-case analysis is preferable and thus it should be determined on the basis of an overall assessment.

## Increase

### Increase---Causal---1NC

#### The transitive “increase” implies a cause-and-effect relationship.

Goldstein ’1 [Thomas C, Jonathan S Massey, Amy Howe, George J Fowler, III, Lawrence R Demarcay; December 4; former clerk for Judge Patricia Wald of the D.C. Circuit, co-founder of SCOTUS Blog, notably second chair for Laurence Tribe and David Boies on behalf of Vice President Al Gore in *Bush v. Gore*; J.D. from Harvard Law School, former clerk to Justice William J Brennan, Jr; the list goes on; Westlaw, Appellate Brief for “Republican National Committee v. Taylor,” WL 36038162]

The rules of grammar confirm that the Contest Statement is untruthful because it implies a cause-and-effect relationship between the Bill and Medicare increases. When a subject and verb are not followed by an object - e.g., in the sentence, “Under the bill, Medicare spending increases” - the verb is intransitive. When an object follows the verb- as in the Contest Statement (the “bill... increases... spending on Medicare”)-the verb is transitive. The definition of the *intransitive* verb “increase” is “to become greater in size, amount, degree, etc.; grow.” Webster's New World College Dictionary 684 (3d ed. 1995). But the definition of the *transitive* verb “increase” - the verb used in the Contest Statement - is “to *cause* to become greater in size, amount, degree, etc.; *add to*; *augment*.” Id. (emphasis added). It cannot be said that the Bill would have caused Medicare spending to become greater in size in the period from 1995 to 2002, or that the Bill would have added to or augmented Medicare spending in those years.

### Increase---Causal---2NC

#### “Increase” in the transitive active voice requires causation.

Ho ’17 [Derek T, Silvija A Strikis, Hilary P Gerzhoy, H Blair Hahn, and Christiaan A Marcum; August 18; Partner at Kellogg, Hansen, Todd, Figel, & Frederick PLLC, J.D. from Harvard Law School, Former Law Clerk to Justice David H. Souter; Partner at Kellogg, Hansen, Todd, Figel, & Frederick PLLC, Former Law Clerk to Justice Sandra Day O'Connor; the list goes on; Westlaw, Appellate Brief for “In Re: Lipitor (Atorvastatin Calcium) Marketing, Sales Practices and Products Liability Litigation,” WL 4050003]

The district court held Dr. DeMicco's admission insufficient to avoid summary judgment because it was “at best, evidence of association, not causation.” JA2055(CMO 97, at 22); JA2155(CMO 100, at 46). That ruling is contrary to the \*64 plain language of Dr. DeMicco's email. The verb “increase,” when used in the transitive active voice (i.e., with a direct object, here, “the risk”) means “to make greater” – i.e., to cause an increased risk. See Webster's Third New International Dictionary 1145 (2002). That is the very definition of general causation. See, e.g., Kuhn v. Wyeth, Inc., 686 F.3d 618, 626 (8th Cir. 2012) (defining general causation as the requirement “that use of [a drug] increases the risk of [a disease]”); Jenkins v. Slidella L.L.C., No. 05-370, 2008 WL 2649510, at \*4 (E.D. La. June 27, 2008) (defining general causation in a toxic tort as the requirement that “exposure to the substance at issue increases the risk of a particular injury”).43

### Increase---Make Greater---2AC

#### “Increase” means adding extent.

Phillips ’2 [Louis M; May 1; Judge on the Bankruptcy Court of M.D. Maryland; Westlaw, “In re Goldberg,” 277 B.R. 251]

In determining the plain meaning of the phrase “increases the obligor's insolvency,” the Court initially notes that this phrase makes no reference whatsoever to a “reasonably equivalent value” test26 or even to the “fair consideration” test of the Section 3 of the UFCA.27 Instead, Article 2036 of the Civil Code merely uses the word “increases,” and the absence of “reasonably equivalent value” language or “fair consideration” language rings loudly in the Court's judicial ear. Accordingly, the Court will focus on the plain meaning of the term “increases.” Taking note from one of the dictionaries of choice of the United States Supreme Court,28 the Court finds that the definition of the word “increase” in Webster's Ninth New Collegiate Dictionary reads as follows:

\*270 [T]o become progressively greater (as in size, amount, number, or intensity) .... to make greater: AUGMENT .... INCREASE, ENLARGE, AUGMENT, MULTIPLY mean to make or become greater. INCREASE used intransitively implies progressive growth in size, amount, intensity; used transitively it may imply simple not necessarily progressive addition ... the act or process of increasing: as ... addition or enlargement in size, extent, quantity.

Webster's Ninth New Collegiate Dictionary 611 (1990) (emphasis added).

### Increase---Make Greater---1AR

#### “Increase” means to make greater in quality or strength.

Kristl ’4 [Kenneth T, James R May, Keri N Powell, Howard I Fox, John D Walke, David G McIntosh, Ann B Weeks, Jonathan F Lewis; October 26; Partner at Winston & Strawn LLP, Former Law Clerk to District Court Judge William C. Lee, J.D. from Chicago-Kent College of Law; Westlaw, Appellate Brief in “the State of New York v. United States Environmental Protection Agency,” WL 5846438]

The sole textual basis EPA asserts for its extraordinary position is an argument based on the word “increases” in §111(a)(4). Specifically, EPA claims that, even when a change causes emissions to rise to the highest level reached in the past ten years, it does not “increase[]” them. EPA Br. 69-71, 86. According to EPA's untenable argument, Congress did not specify how an increase is to be measured, and thus left EPA free to interpret “increases” as it wishes. Id.

The term “increases” is not an empty vessel that EPA can fill as it chooses. Instead, absent further congressional guidance, the term must be given its ordinary meaning. Engine Mfrs. Assn. v. South Coast Air Quality Management District, 124 S. Ct. 1756, 1761 (2004); Bluewater Network v. EPA, 370 F.3d 1, 13 (D.C. Cir. 2004). The ordinary meaning of “increase” is “to make greater, as in number, size, strength, or quality.” Random House Webster's Unabridged Dictionary, 2d Ed. (1999), at 969. Thus, a change that makes emissions greater “increases” them. EPA's interpretation contravenes the Act's plain meaning under Chevron Step One, or in the alternative “diverges from any realistic meaning” under Chevron Step Two. See, e.g., NRDC v. Daley, 209 F.3d 747, 753 (D.C. Cir. 2000).2

### Increase---Net---1NC

#### “Increase” must be net increases.

Ortega ’91 [Reuben; December 31; Associate Justice on California’s Second Appellate District; Westlaw, “Department of Water & Power v. Energy Resources Conservation & Development Commission,”2 Cal. App. 4th 206]

Action was brought to determine whether California Energy Resources Conservation and Development Commission could exercise certification jurisdiction over electrical power plant repowering project. The Superior Court, Los Angeles County, No. BS003230, John Zebrowski, J., ordered issuance of preemptory writ of mandate commanding Commission to cease its exercise of such certification jurisdiction, and Commission appealed. The Court of Appeal, Ortega, J., held that: (1) term “increase,” as used in statute giving the Energy Commission modification jurisdiction over any alteration, replacement, or improvement of equipment that results in increase of 50 megawatts or more in power plant's electrical generating capacity, referred to “net” increase in power plant's total generating capacity, and (2) Commission could exercise construction jurisdiction only over construction at new, not existing, sites.

### Increase---Net---2NC

#### “Increases” must be on net.

Hall ’72 [Pike; February 1; Judge on the Court of Appeal of Louisiana, Second Circuit; Westlaw, “O. C. Lanier, v. Trans-World Life Insurance Company,” 258 So. 2d 103]

1The key terms used in the agreement have well defined meanings in the ‘debit’ insurance filed. ‘Increase’ means the net increase in premiums generated by an agent calculated by subtracting ‘lapses' or premiums lost on policies previously issued from gross premiums added by new policies sold. ‘One time’ means a payment made as salary or bonus to the agent on a dollar for dollar or ‘one for one’ basis measured by the net increase.

#### “Increase” must be on net.

McGuffey ’20 [Carroll; Summer; partner at Troutman Pepper Hamilton Sanders LLP; Natural Resources & Environment, “Reforming New Source Review: What Project Emissions Accounting Really Means, and Why It Should Survive,” p. 37]

The debate over how to count changes in emissions when determining NSR applicability is as old as the program itself. The CAA requires permitting for any “increase” in emissions, 42 U.S.C. §§ 7411, 7475, 7479, but it does not define the word “increase,” leaving room for interpretation. Such ambiguity leaves EPA in charge of deciding how sources must determine whether an “increase” will occur. New York, 413 F.3d at 22-24. In fact, a different dispute over the ambiguities in the very same statutory provision resulted in the Supreme Court's now famous (or infamous) Chevron decision on agency deference. Chevron U.S.A., Inc. v. Natural Res. Def. Council, 467 U.S. 837, 865 (1984) (concluding that the EPA's method of calculating emissions is a reasonable policy choice).

In an attempt to define the ambiguous word “increase,” EPA has adopted increasingly complex regulations, but those rules have consistently maintained that source owners must be allowed to consider the overall “net effect” of a project on the stationary source as a whole. This idea has taken on many names and forms over time--referred to variously as the “bubble concept,” “contemporaneous netting,” “project netting,” and now “Project Emissions Accounting.” The only debate has been in deciding what rules are needed to right-size the NSR permitting program so that permits are required only for those projects that truly warrant such review.

No one can predict with any certainty how the D.C. Circuit will receive PEA. However, the D.C. Circuit already decided long ago that the CAA allows EPA significant discretion in deciding how sources should calculate emissions increases and decreases in applying NSR permitting requirements.

The issue of whether and how to count multiple changes in emissions under NSR arose in the context of legal challenges to EPA's 1978 NSR rules. Alabama Power Co. v. Costle, 636 F.2d 323, 399-403 (D.C. Cir. 1980). In that lengthy opinion, specifically the portion authored by Judge Wilkey, the court recognized that there were two logical ways to interpret the word “increase” in the statute--a source must either determine the “net effect” or count only increases and ignore decreases.

The court resoundingly rejected the idea that decreases should be ignored, calling the idea “unreasonable and contrary to the expressed purposes of the [Act].” Instead, the court decided that the statute requires EPA to “look at any change proposed for a plant, and decide whether the net effect of all the steps involved in that change is to increase the emission of any air pollutant [;] this is commonly termed the ‘bubble’ concept.” Id. at 401 (emphasis added). To explain its reasoning, the court noted that “[t]he bubble concept is precisely suited to preserve air quality within a framework that allows cost-efficient, flexible planning for industrial expansion and improvement.” Id. at 402.

### Increase---Preexistence---1NC

#### To “increase” means expanding already-existing cooperation.

Buckley ’6 [Jeremiah S, Joseph M. Kolar; November 13; partners at Buckley Kolar LLP; Westlaw, Brief of Amici Curiae for “Mortgage Insurance Companies of America and Consumer Mortgage Coalition,” WL 3309503]

First, the court said that the ordinary meaning of the word “increase” is “to make something greater,” which it believed should not “be limited to cases in which a company raises the rate that an individual has previously been charged.” 435 F.3d at 1091. Yet the definition offered by the Ninth Circuit compels the opposite conclusion. Because “increase” means “to make something greater,” there must necessarily have been an existing premium, to which Edo's actual premium may be compared, to determine whether an \*26 “increase” occurred. Congress could have provided that “adverse action” in the insurance context means charging an amount greater than the optimal premium, but instead chose to define adverse action in terms of an “increase.” That definitional choice must be respected, not ignored. See Colautti v. Franklin, 439 U.S. 379, 392-93 n.10 (1979) (“[a] definition which declares what a term ‘means' … excludes any meaning that is not stated”).

Next, the Ninth Circuit reasoned that because the Insurance Prong includes the words “existing or applied for,” Congress intended that an “increase in any charge” for insurance must “apply to all insurance transactions - from an initial policy of insurance to a renewal of a long-held policy.” 435 F.3d at 1091. This interpretation reads the words “existing or applied for” in isolation. Other types of adverse action described in the Insurance Prong apply only to situations where a consumer had an existing policy of insurance, such as a “cancellation,” “reduction,” or “change” in insurance. Each of these forms of adverse action presupposes an already-existing policy, and under usual canons of statutory construction the term “increase” also should be construed to apply to increases of an already-existing policy. See Hibbs v. Winn, 542 U.S. 88, 101 (2004) (“a phrase gathers meaning from the words around it”) (citation omitted).

### Increase---Preexistence---2NC

#### Plain language agrees.

Brown ’3 [Anna J; July 17; Federal District Court Judge in Oregon; Westlaw, Mark v. Valley Insurance Company, 275 F. Supp. 2d 1307]

FCRA does not define the term “increase.” The plain and ordinary meaning of the verb “to increase” is to make something greater or larger.4 Merriam–Webster's Collegiate Dictionary 589 (10th ed.1998). The “something” that is increased in the statute is the “charge for any insurance.” The plain and common meaning of the noun “charge” is “the price demanded for something.” Id. at 192. Thus, the statute plainly means an insurer takes adverse action if the insurer makes greater (i.e., larger) the price demanded for insurance.

An insurer cannot “make greater” something that did not exist previously. The statutory definition of adverse action, therefore, clearly anticipates an insurer must have made an initial charge or demand for payment before the insurer can increase that charge. In other words, an insurer cannot increase the charge for insurance unless the insurer previously set and demanded payment of the premium for that insured's insurance coverage at a lower price.

## Its

### Its---Possessive/Exclusive---1NC/2NC

#### “Its” is exclusive---legal interpretations mean the plan must solely apply to US security cooperation funding streams

Brent ’10 [Douglas F.; June 2; attorney; “Reply Brief on Threshold Issues of Cricket Communications, Inc.,” online: <http://psc.ky.gov/PSCSCF/2010%20cases/2010-00131/20100602_Crickets_Reply_Brief_on_Threshold_Issues.PDF>] italics and bold in the original

AT&T also argues that Merger Commitment 7.4 only permits extension of “any given” interconnection agreement for a single three year term. AT&T Brief at 12. Specifically, AT&T asserts that because Cricket adopted the interconnection agreement between Sprint and AT&T, which itself was extended, Cricket is precluded from extending the term of its agreement with AT&T. Id This argument relies upon an inaccurate assumption: that the agreement (contract) between Sprint and AT&T, and the agreement (contract) between Cricket and AT&T, are one and the same. In other words, to accept AT&T’s argument the Commission must conclude that two separate contracts, i.e. the interconnection between Sprint and AT&T in Kentucky (“Sprint Kentucky Agreement”) and the interconnection between Cricket and AT&T in Kentucky (“Cricket Kentucky Agreement”), are one and the same. Upon this unstated (and inaccurate) premise AT&T asserts that “***the ICA*** was already extended”; id. at 14, and “***the ICA*** Cricket seeks to extend was extended by Sprint . . . .”; id. at 15, and, finally, “Cricket cannot extend ***the same ICA*** a second time . . . .” Id. (emphasis added in all). Note that in the quoted portions of the AT&T brief (and elsewhere) AT&T uses vague and imprecise language when referring to either the Sprint Kentucky Agreement, or the Cricket Kentucky Agreement, in hopes that the Commission will treat the two contracts as one and the same. But it would be a mistake to do so. The contract governing AT&T’s duties and obligations with Sprint is a legally distinct and separate contract from that which governs AT&T’s duties with Cricket. The Sprint Kentucky Agreement was approved by the Commission in September of 2001 in Case Number 2000-00480. The Cricket Kentucky Agreement was approved by the Commission in September of 2008 in Case Number 2008-033 1. AT&T ignores the fact that these are two separate and distinct contracts because it knows that the merger commitments apply to ***each*** agreement that an individual telecommunications carrier has with AT&T. Notably, Merger Commitment 7.4 states that “AT&T/BellSouth ILECs shall permit ***a requesting telecommunications carrier*** to extend ***its*** current interconnection agreement . . . . As written, the commitment allows any carrier to extend “***its***” agreement. Clearly, the use of the pronoun “its” in this context is possessive, such that the term “its” means - ***that*** particular carrier’s agreement with AT&T (and not any other carrier’s agreement). Thus, the merger commitment applies to each agreement that an individual carrier may have with AT&T. It necessarily follows then, that Cricket’s right to extend its agreement under Merger Commitment 7.4 is separate and distinct right from another carrier’s right to extend its agreement with AT&T (or whether such agreement has been extended).

#### Its is possessive and refers to the party preceding its use

US District Court 7 (United States District Court for the District of the Virgin Islands, Division of St. Thomas and St. John, “AGF Marine Aviation & Transp. v. Cassin, 2007 U.S. Dist. LEXIS 90808,” Lexis)//BB

The Court inadvertently used the word "his" when the Court intended to use the word "its." The possessive pronoun was intended to refer to the party preceding its use--AGF. Indeed, that reference is consistent with the undisputed facts in this case, which indicate that Cassin completed an application for the insurance policy and submitted it to his agent, Theodore Tunick & Company ("Tunick"). Tunick, in turn, submitted the application to AGF's underwriting agent, TL Dallas. (See Pl.'s Mem. of Law in Supp. of Mot. for Summ. J. 5.)

#### Possessive pronouns require exclusion

Frey 28 (Judge – Supreme Court of Missouri, Supreme Court of Missouri,

320 Mo. 1058; 10 S.W.2d 47; 1928 Mo. LEXIS 834, Lexis)

In support of this contention appellant again argues that when any ambiguity exists in a will it is the duty of the court to construe the will under guidance of the presumption that the testatrix intended her property to go to her next of kin, unless there is a strong intention to the contrary. Again we say, there is intrinsic proof of a  [\*1074]  strong intention to the contrary. In the first place, testatrix only named two of her blood relatives in the will and had she desired [\*\*\*37]  them to take the residuary estate she doubtless would have mentioned them by name in the residuary clause. In the second place, if she used the word "heirs" in the sense of blood relatives she certainly would have dispelled all ambiguity by stating whose blood relatives were intended. Not only had  [\*\*53]  she taken pains in the will to identify her own two blood relatives but she had also identified certain blood relatives of her deceased husband. Had it been her intention to vest the residuary estate in her blood relatives solely, she would certainly have used the possessive pronoun "my" instead of the indefinite article "the" in the clause, "the above heirs."its is geographical.

#### Grammatically, this refers solely to U.S. policy

Manderino 73 (Justice – Supreme Court of Pennsylvania, “Sigal, Appellant, v. Manufacturers Light and Heat Co”., No. 26, Jan. T., 1972, Supreme Court of Pennsylvania, 450 Pa. 228; 299 A.2d 646; 1973 Pa. LEXIS 600; 44 Oil & Gas Rep. 214, Lexis)

On its face, the written instrument granting easement rights in this case is ambiguous. The same sentence which refers to the right to lay a 14 inch pipeline (singular) has a later reference to "said lines" (plural). The use of the plural "lines" makes no sense because the only previous reference has been to a "line" (singular). The writing is additionally ambiguous because other key words which are "also may change the size of its pipes" are dangling in that the possessive pronoun "its" before the word "pipes" does not have any subject preceding, to which the possessive pronoun refers. The dangling phrase is the beginning of a sentence, the first word of which does not begin with a capital letter as is customary in normal English [\*\*\*10]  usage. Immediately preceding the "sentence" which does not begin with a capital letter, there appears a dangling  [\*236]  semicolon which makes no sense at the beginning of a sentence and can hardly relate to the preceding sentence which is already properly punctuated by a closing period. The above deviations from accepted grammatical usage make difficult, if not impossible, a clear understanding of the words used or the intention of the parties. This is particularly true concerning the meaning of a disputed phrase in the instrument which states that the grantee is to pay damages from ". . . the relaying, maintaining and operating said pipeline. . . ." The instrument is ambiguous as to what the words ". . . relaying . . . said pipeline . . ." were intended to mean.

#### Its is possessive and requires ownership

**Glossary of English Grammar Terms, 2005**

(http://www.usingenglish.com/glossary/possessive-pronoun.html)

Mine, yours, his, hers, its, ours, theirs are the possessive pronouns used to substitute a noun and to show possession or ownership. EG. This is your disk and that's mine. (Mine substitutes the word disk and shows that it belongs to me.)

#### “Its” means belonging to it

**Oxford English Dictionary 14** http://www.merriam-webster.com/dictionary/its

Its

A. As adj. poss. pron. Of or belonging to it, or that thing (L. ejus); also refl., Of or belonging to itself, its own (L. suus).

### Its---Associated With---2AC

#### Its means associated with

**Oxford Dictionaries Online, No Date** (“Its”, <http://oxforddictionaries.com/definition/its?view=uk>)

its

Entry from World dictionar

Pronunciation:/ɪts/

possessive determiner

belonging to or associated with a thing previously mentioned or easily identified: turn the camera on its side

he chose the area for its atmosphere

#### Of or relating to

Webster’s ’10 [Merriam-Webster’s Online Dictionary, “its”, http://www.merriam-webster.com/dictionary/its]

Main Entry: its

Pronunciation: \ˈits, əts\

Function: adjective

Date: circa 1507

: of or relating to it or itself especially as possessor, agent, or object of an action <going to its kennel> <a child proud of its first drawings> <its final enactment into law>

## Security Cooperation---Requires DOD

### SC---DOD---1NC

#### “Security cooperation” requires the DOD.

Quinn ’19 [Major Jason A. Quinn; 2019; Judge Advocate in the United States Army; the Military Law Review, “Other Security Forces Too: Traditional Combatant Commander Activities Between U.S. Special Operations Forces and Foreign Non-Military Forces,” vol. 227]

Under this definition, “security sector assistance” includes the relevant policies, programs, or activities of any executive agency. Complicating matters, though, Congress has considered a proposed definition for “security sector assistance” that, in contrast to the presidential policy definition,130 encompasses DoS programs, but not DoD or other executive agency programs.131 In addition, Congress has defined “security cooperation” as DoD specific,132 but it has not defined “security assistance.”

The DoD adheres to the presidential policy definition and further defines “security cooperation” as all its relationship building and foreign partner development activities, including “security assistance,” which the DoD defines as a subset of security cooperation that is funded and authorized by the DoS and administered by the Defense Security Cooperation Agency.133 The DoS, on the other hand, uses the term “security assistance” in a manner that contradicts the DoD's definition, employing it to describe any DoS or DoD assistance to foreign military or other security forces.134

### SC---DOD---2NC

#### “Security cooperation” is defined in government documents to require the DOD.

JCS ’17 [Joint Chiefs of Staff; May 23; publishing with the Army, Marine Corp, Air Force, Navy, and Coast Guard; Security Cooperation, Joint Publication 3-20, “Glossary,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf]

PART II—TERMS AND DEFINITIONS

defense institution building. Security cooperation conducted to establish or reform the capacity and capabilities of a partner nation’s defense institutions at the ministerial/department, military staff, and service headquarters levels. Also called DIB. (Approved for inclusion in the DOD Dictionary.)

foreign military sales. That portion of United States security assistance for sales programs that require agreements/contracts between the United States Government and an authorized recipient government or international organization for defense articles and services to be provided to the recipient for current stocks or new procurements under Department of Defense-managed contracts, regardless of the source of financing. Also called FMS. (Approved for incorporation into the DOD Dictionary.)

international military education and training. Formal or informal instruction provided to foreign military students, units, and forces on a non-reimbursable (grant) basis by offices or employees of the United States, contract technicians, and contractors, and the instruction may include correspondence courses; technical, educational, or informational publications; and media of all kinds. Also called IMET. (Approved for incorporation into the DOD Dictionary.)

partner nation. 1. A nation that the United States works with in a specific situation or operation. (JP 1) 2. In security cooperation, a nation with which the Department of Defense conducts security cooperation activities. (JP 3-20) Also called PN. (Approved for incorporation into the DOD Dictionary.)

security assistance. Group of programs authorized by the Foreign Assistance Act of 1961, as amended; the Arms Export Control Act of 1976, as amended; or other related statutes by which the United States provides defense articles, military training, and other defense-related services by grant, lease, loan, credit, or cash sales in furtherance of national policies and objectives, and those that are funded and authorized through the Department of State to be administered by Department of Defense/Defense Security Cooperation Agency are considered part of security cooperation. Also called SA. (Approved for incorporation into the DOD Dictionary.)

security cooperation. All Department of Defense interactions with foreign security establishments to build security relationships that promote specific United States security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide United States forces with peacetime and contingency access to allied and partner nations. Also called SC. (Approved for incorporation into the DOD Dictionary.)

#### The Greenbook defines “security cooperation” much the same.

DSCU ’21 [Defense Security Cooperation University; last updated May 2021; University created by the Defense Security Cooperation Agency, which is part of the Department of Defense; Greenbook, “Introduction to Security Cooperation,” Ch. 1, https://www.dscu.edu/documents/publications/greenbook/01\_Chapter.pdf?id=1]

The term security cooperation was first introduced in 1997 by the Defense Reform Initiative (DRI). At that time, the Defense Security Assistance Agency (DSAA) already had day-to-day management responsibilities of many security assistance programs authorized by the Foreign Assistance Act (FAA) and the Armed Export Control Act (AECA). The DRI proposed that DSAA also manage certain Department of Defense (DoD)-funded international programs along with their personnel and associated resources. In order for U.S. government (USG) agencies, the private sector, and foreign governments to better understand DSAA’s enlarged mission and diverse functions beyond security assistance (SA), DoD re-designated DSAA as the Defense Security Cooperation Agency (DSCA), effective 1 October 1998.

In recent years, DSCA has absorbed management responsibilities for many DoD international programs while also leading the wider USG security cooperation enterprise. However, many security cooperation programs continue to be managed by other elements of the Office of the Secretary of Defense (OSD), the combatant commands (CCMDs), or the military departments (MILDEPs). Further complicating the management of security cooperation was the in-country point of contact between the USG and the host nation. This point of contact was either the Defense Intelligence Agency (DIA)- sponsored Defense Attaché Office (DAO) or the DSCA-sponsored Security Cooperation Office (SCO). These two spigots of securiy cooperation within a country required a broad knowledge and skill baseline of the very different international programs that are initiated, funded, and managed throughout the DoD, its agencies and the MILDEPs. Most disconnects regarding SCO-DAO coordination of incountry security cooperation were generally resolved with the establishment of the Senior Defense Officials/Defense Attaché (SDO/DATT) having oversight over both the SCO and DAO organizations.

On 9 June 2004 that DoD published a formal, yet still very broad, definition of security cooperation in Joint Pub 1-02:

All DoD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a host nation.

DODD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation, 29 December 2016, further defines security cooperation with assigned responsibilities:

All DoD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to allied and partner nations. This includes DoD-administered security assistance programs.

According to Title 10 U.S. Code Section 301, the term “security cooperation programs and activities of the Department of Defense” means any program, activity (including an exercise), or interaction of the DoD with the security establishment of a foreign country to achieve a purpose as follows: (A) To build and develop allied and friendly security capabilities for self-defense and multinational operations. (B) To provide the armed forces with access to the foreign country during peacetime or a contingency operation. (C) To build relationships that promote specific United States security interests. Other DoD policy statements identify DoD-managed or administered security assistance programs as components of security cooperation.

#### “Security cooperation” is by the DOD.

Eerden ’20 [Captain James R. R. Van Eerden; Spring; recently graduate from the Expeditionary Warfare School of Marine Corps University, where he completed a prestigious fellowship program and graduated first in his class; Journal of Advanced Military Studies, “Seeking Alpha in the Security Cooperation Enterprise: A New Approach to Assessments and Evaluations,” vol. 11, no. 1]

Security Cooperation Defined

Security Cooperation, Joint Publication (JP) 3-20, provides the following definition of security cooperation: 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 U.S. interests; enable partner nations (PNs) to provide the U.S. access to territory, infrastructure, information, and resources; and/or to build and apply their capacity and capabilities consistent with U.S. defense objectives.5

The Fiscal Year (FY) 2019 President’s Budget: Security Cooperation Consolidated Budget Display outlines seven categories of security cooperation activity, including military-to-military engagements, support to operations, and humanitarian and assistance activities, among others.6 The security cooperation framework traditionally includes security assistance (SA), security force assistance (SFA), and some aspects of foreign internal defense (FID).7 In the context of this article, the term security cooperation refers primarily to military-to-military engagements, where the U.S. military engages in training partner forces under the auspices of Title 10 and Title 22 authorities.

#### “Security cooperation” requires the Department of Defense.

Defense ’16 [Department of Defense; February 15; Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” https://irp.fas.org/doddir/dod/jp1\_02.pdf]

security cooperation — All Department of Defense interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation. Also called SC. See also security assistance. (JP 3-22)

### SC---Requires DSCA---1NC

#### All security cooperation is executed by the DSCA

Hooper ’19 [Lt. General Charles and Michael O’Hanlon; June 4; Director of the Defense Security Cooperation Agency; Senior Fellow and Director of Research, Foreign Policy, Brookings; “How Security Cooperation Advances U.S. Interests,” Brookings Institute Foreign Policy Studies Program event]

Well, thank you, Mike, and thanks very much for having me. And good morning, everybody. I am the director of the Defense Security Cooperation Agency and it's the agency that does more and is known by less people than anybody else in Washington, so I always welcome the opportunity to tell everybody about it.

The Defense Security Cooperation Agency is mandated by Congress to execute all security cooperation, some on behalf of the State Department, much on behalf of the Department of Defense, writ large and worldwide. It is most known for being the executive agent for foreign military sales, and that's what most people know about us. But we're also responsible for excess defense articles. We are the executive agent for all five Department of Defense regional centers, so the Marshall Center in Germany; the Inouye Center, Asia-Pacific Center for Security Studies, in Hawaii.

We're also responsible, and we'll talk a little bit about this later, for what I call institutional capacity-building. That is the complement to foreign military sales that ensures that our partners have the human resources and the defense institutional development to properly utilize the equipment we buy for them in the interest of national security.

Our headquarters is here in Crystal City, in Washington. We also work with the Security Cooperation's officers worldwide. We work with the COCOMs. And we're under actually, and this is unique for the United States, we work for the Under Secretary of Defense for Policy. So we work for Mr. John Rood. And the reason I say that is in many countries, the acquisitions and the arms sales come under the acquisitions or the logistics directorates or work directly in some of our competitors, for those companies, those state-owned companies. But here in the United States security cooperation and arms sales is a policy tool and not a tool for anything else. So that's basically kind of a snapshot of what DSCA does.

MR. O'HANLON: So, great. That's very helpful. And let me ask a couple more follow-up questions just to continue to refine our understanding.

So a command like Africa Command, where you spent three years, which does a lot of training in the field, is all of that training essentially under your purview? Or the parts that do not involve U.S. weapons transfers or sales, are they potentially separate and you coordinate, but you're not in charge of that? Is that correct?

GENERAL HOOPER: Well, that's a very good question. The geographic combatant commands still have the responsibility for executing security cooperation in their respective commands. We work by, with, and through those commands. The weapons sales portion of it, or the defense articles and services portion of it, comes directly under DSCA's supervision. Some of the training exercises and other things we work collaboratively with the combatant commands. And then in some cases, for example, in institutional capacity-building, we work together in a synergistic fashion to effect that security cooperation.

So it's equal parts. Some things we're principally responsible for, some things the combatant commands are responsible for, and some things we work jointly together.

MR. O'HANLON: And as we start to paint this picture of your responsibilities and how you work with others, I also wanted to bring in foreign military assistance and financing. And my understanding is that there are parts of foreign military assistance of various types that we give through the State Department and other types we give through DOD. It depends a little bit on the recipient and the nature of the aid. Could you help us understand that a little bit, too? Because I'm sure some of that money is what's being used to buy the weapons that you're overseeing the transfer of.

GENERAL HOOPER: Absolutely. And that's also a very good question. So let's start on what we call the Title 22 on the State Department side.

We are the executive agent. The State Department has responsibility for foreign military sales and we are, in effect, the executive agent for the State Department in foreign military sales. Now, there are two real big components of security cooperation. One is what we call Title 22, which is the State Department supervised element for which we are the executive agent. The other half of it is the Title 10 piece.

So, for example, as a result of the Fiscal Year '17 NDAA, we had several different authorities and a disparate group of authorities that were all consolidated into one, the majority into one authority, 333, Section 333, that many of you may be familiar with. And this constitutes the Title 10 security cooperation piece.

The biggest way to distinguish between the two is our State Department responsibilities are principally focused to a great extent on defense articles and services, whereas our Title 10 responsibilities fall, in many cases, more into the realm of institutional capacity-building, exercises, and other types of things like that.

MR. O'HANLON: That's interesting. So you could think of it the hardware, sort of the weapons, the hardcore stuff, that's through State. The people side, the softer side, the software side is through DOD.

GENERAL HOOPER: Right.

MR. O'HANLON: It's almost the opposite of what some people might guess.

GENERAL HOOPER: Right. And we, in many respects, serve as a catalyst to bring all of that together at the national level.

### SC---Tradeoff Link---2NC

#### “Security cooperation” can use either DOD or DOS resources.

JCS ’17 [Joint Chiefs of Staff; May 23; publishing with the Army, Marine Corp, Air Force, Navy, and Coast Guard; Security Cooperation, Joint Publication 3-20, “Executive Summary,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf]

Security Cooperation in Strategic Context

|  |  |
| --- | --- |
| Security cooperation (SC) provides ways and means to help achieve national security and foreign policy objectives. | 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 Purposes | SC helps develop partnerships that encourage and enable PNs to act in support of aligned US strategic objectives. SC activities often complement other United States Government (USG) foreign assistance to provide stability, help mitigate drivers of conflict, and assure key partners and allies. Additionally, SC supports US military campaign and contingency plans with necessary access, critical infrastructure, and PN support and enables the achievement of strategic objectives, such as deterring adversaries, preventing conflict, and enhancing the stability and security of PNs. |
| SC and the Instruments of National Power | SC programs and activities are normally integrated and synchronized with the other instruments of national power depending upon how other interagency partners implement the national strategy (e.g., national security strategy) to achieve strategic objectives. |
| Security Sector Assistance and United States Foreign and Defense Policies | In accordance with foreign policy direction established by the Department of State (DOS), DOD leads on defense policy issues that involve national security interests with military or defense equities. Presidential Policy Directive (PPD)-23, Security Sector Assistance, details the USG effort to implement security sector assistance (SSA) more efficiently, including the strategy to build security relationships, partner capacity, and capabilities to achieve national security objectives. PPD-23 establishes the integrated country strategy (ICS) as the core organizing document for USG foreign assistance activities supporting a particular PN. ICSs link goals for the PN to US national security priorities, SSA objectives, and if appropriate, to regional security objectives. |
| Theater Strategy and Estimate  Theater strategy bridges national strategic guidance and joint planning. | Theater strategy outlines a geographic combatant commander’s (GCC’s) vision for integrating resources and synchronizing military activities and operations in conjunction with the application of other instruments of national power to achieve theater objectives and Guidance for Employment of the Force-directed strategic objectives. GCCs’ theater strategies, as reflected in their theater campaign plans (TCPs), typically emphasize military engagement, SC, and deterrence through routine shaping activities. The strategic estimate, which is continually updated, helps to determine the missions, objectives, and potential activities required in the campaign plan. |
| Internal Defense and Development | Internal defense and development is the full range of measures taken by a nation to promote its growth and protect itself from subversion, lawlessness, insurgency, terrorism, and other threats to its security. It focuses on both security and building viable civic, social, and economic institutions that respond to the needs of that nation’s population. |

Security Cooperation Relationships

|  |  |
| --- | --- |
| SC Related Activities and Operations  Department of Defense (DOD) policy supports SC activities that enable building security relationships, building partner capacity, and gaining/maintaining access. | SC uses a combination of programs and activities by which DOD, in coordination with DOS, encourages and enables countries and organizations to partner with the US to achieve strategic objectives. Foreign assistance consists of a number of legally authorized programs that can be grouped into the general categories of development assistance, humanitarian assistance, and SA with the strategic purpose of promoting long-term host nation (HN) and regional stability. SA is a group of programs the USG uses to provide defense articles, military training, and other defense-related services by grant, loan, credit, or cash sales to advance national policies and objectives. SA is generally overseen by DOS, and in many cases administered by DOD as SC. SC is the group of programs or activities employed by DOD in cooperation with PNs to achieve US security objectives, and some SC is foreign assistance, but not all. Security force assistance is the set of DOD SC activities that contribute to unified action by the USG to support the development of the capacity and capabilities of FSF and their supporting institutions, whether of a PN or an international organization (e.g., regional security organization), in support of US objectives. Security sector reform (SSR) is a comprehensive set of programs and activities that an HN government undertakes with USG assistance to improve the way it provides safety, security, and justice. Defense institution building (DIB) is a primary form of DOD support to SSR. DIB comprises SC typically conducted at the ministerial/department, military staff/service headquarters, and related agency/supporting entity level to develop the strategic and operational aspects of a PN’s defense institutions. Other SC-related activities and programs include military engagements; joint combined exchange training; Regional Defense Combating Terrorism Fellowship Program; combined exercises for training, train-and-equip initiatives, and international military education and training (IMET); and international armaments cooperation. |
| SC and Joint Operations | A significant number of SC activities are conducted as a part of the GCCs’ TCPs, but limited contingencies, crises responses, or major operations can also involve some form of SC. The foreign internal defense program is the participation by civilian and military agencies of a government in any of the action programs taken by another government, or other designated organization, to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to their security. Counterinsurgency (COIN) is the comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes. COIN is primarily a political struggle and incorporates a wide range of activities by the HN government of which security is only one, albeit an important one. Counterterrorism are those activities and operations conducted to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. Countering weapons of mass destruction, across the three lines of effort (prevent acquisition, contain and reduce threats, and respond to crises), includes activities conducted across the USG to counter efforts to coerce or attack the US, its Armed Forces, allies, partners, and interests with chemical, biological, radiological, or nuclear weapons. Counterdrug operations are those civil or military actions taken to reduce or eliminate illicit drug trafficking. Stability activities include military missions, tasks, and activities conducted outside the US in coordination with or in support of other instruments of national power to maintain or reestablish a safe and secure environment, and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. Foreign humanitarian assistance consists of DOD activities conducted outside the US and its territories to directly relieve or reduce human suffering, disease, hunger, or privation. Peace operations normally include international efforts and military missions to contain conflict, reestablish the peace, shape the environment to support reconciliation and rebuilding between two or more factions within the indigenous population, and facilitate the transition to legitimate governance. Civil-military operations are the activities of a commander performed by designated civil affairs or other military forces that establish, maintain, influence, or exploit relations between military forces, indigenous populations, and institutions, by directly supporting efforts for stability within an HN or a region. Military information support operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives. Countering threat networks is the aggregation of activities across the USG that identify, analyze, neutralize, disrupt, or destroy threat networks. Personnel recovery is the sum of military, diplomatic, and civil efforts to affect the recovery and reintegration of isolated personnel. |
| SC Authorities and Programs | SC activities are conducted with DOD funds, forces, and authorities, and with DOS SA funds and authorities, administered by DOD. |
| DOD SC Roles and Responsibilities | The Under Secretary of Defense for Policy (USD[P]) oversees, integrates, and coordinates DOD policies and plans for coordination of SC policies, goals, and priorities for the Secretary of Defense (SecDef) with the Military Departments (MILDEPs), DOS, and other interagency partners to enable greater unity of effort in activities that support national security objectives. The Defense Security Cooperation Agency (DSCA) represents the interests of SecDef and USD(P) in SC matters and is charged to direct, administer, and provide DODwide guidance to DOD components and representatives to execute DSCA-managed SC programs. The Under Secretary of Defense for Acquisition, Technology, and Logistics is responsible for establishing and maintaining policies for the effective development of international acquisition, technology, and logistics programs, including international armaments cooperation (e.g., science and technology collaboration, logistics support), to support SC priorities. In conjunction with USD(P), the Joint Staff reviews the SC activities included in combatant command (CCMD) campaign plans to ensure the planning guidance has been met. Geographic CCMDs are the primary organizations for SC planning and integrating SC activities into their TCPs. Functional CCMDs prepare campaign plans that integrate their forces, resources, and funding for SC activities in coordination with the geographic CCMDs, their Service components, international organizations and, when appropriate, the affected security cooperation organizations (SCOs). US Special Operations Command coordinates SC activities to be executed by special operations forces (SOF) with the geographic CCMDs through their theater special operations commands, including the deployment of special operations liaison officers, as well as SOF Service components. MILDEPs and Services support combatant commander (CCDR) campaign plans and simultaneously pursue Service-specific SC objectives consistent with national and theater strategic objectives. SCOs work under the authority of the chief of mission (COM). The SCO is responsible for assessing whether a PN can build and sustain capacity and has the greatest visibility over the execution of SC activities. The senior defense fficial/defense attaché (SDO/DATT) serves as the diplomatically accredited defense attaché and chief of the SCO (if an SCO is present). The SDO/DATT, or a designated member of the SCO, is the point of contact for SC planning and development of the country plan with the GCC planners. Subject to COM approval, the SDO/DATT is the lead integrator for SC activities with the PN. The National Guard may appoint an officer to serve at the US mission under the SDO/DATT as the State Partnership Program liaison for the partner state’s National Guard with the GCC and HN. |
| Department of State SC Roles and Responsibilities  The chief of mission is the personal representative of the President to the country of accreditation, and is responsible to the Secretary of State for the direction, coordination, and supervision of all US Government executive branch employees in that country (except those under the command of a US area military commander). | DOS maintains interagency coordination with respective counterparts in DOD concerning future SA programs and SC activities with PNs. COMs facilitate the coordination of PN security-related requirements that become part of the specific SA programs and SC activities conducted by US military with those PNs. The country team is the senior USG coordinating and supervising body in a foreign country. With guidance from DOS and the COM, the country team develops the ICS regarding the PN, which influences the CCDR’s development of a country-specific security cooperation section (CSCS)/country plan for that PN. Bureau of Political-Military Affairs (PM) is DOS’s principal link to DOD. PM provides policy direction in the areas of international security, SA, military operations, defense strategy and plans, and defense trade. |

#### Even if “security cooperation” doesn’t make PICs competitive, it suggests normal means includes DOD resources and DOS funds.

JCS ’17 [Joint Chiefs of Staff; May 23; publishing with the Army, Marine Corp, Air Force, Navy, and Coast Guard; Security Cooperation, Joint Publication 3-20, “Security Cooperation Relationships,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf]

SC uses a combination of programs and activities by which DOD, in coordination with DOS, encourages and enables countries and organizations to partner with the US to achieve strategic objectives. SC involves an overarching functional relationship rather than a hierarchical relationship with its associated activities/programs. The definition of SC deliberately encompasses a multitude of actions, programs, and missions. Many SC activities are functionally related and dependent upon DOD-administered and DOS-funded SA as part of DOS foreign assistance, in addition to Service funds.

#### “Security cooperation” includes DOD and DOS coordination.

JCS ’17 [Joint Chiefs of Staff; May 23; publishing with the Army, Marine Corp, Air Force, Navy, and Coast Guard; Security Cooperation, Joint Publication 3-20, “Security Cooperation Relationships,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf]

5. Security Cooperation Roles and Responsibilities

SC involves planning and interagency coordination by a myriad of organizational entities from the departmental level down to the SCO in an HN, as well as participating US military units. The following have significant roles and responsibilities for SC activities:

a. DOD. The USD(P) oversees, integrates, and coordinates DOD policies and plans for coordination of SC policies, goals, and priorities for SecDef with MILDEPs, DOS, and other interagency partners to enable greater unity of effort in activities that support national security objectives. DODD 5132.03, DOD Policy and Responsibilities Relating to Security Cooperation, details USD(P) responsibilities for SC. USD(P) and DOS counterparts are responsible for the approvals, the funding, and other authorities required by CCDRs and the Services for planning and executing SC activities in support of PN requirements and US security objectives. USD(P) typically designates/delegates certain responsibilities for SC to assistant or deputy assistant secretariat levels. USD(P) also oversees the development of policy governing the use of the G-TSCMIS to support the resourcing, assessment, planning, and monitoring of SC activities.

(1) DSCA. DSCA is a separate agency of DOD under the direction, authority, and control of USD(P). DSCA represents the interests of SecDef and USD(P) in SC matters and is charged to direct, administer, and provide DOD-wide guidance to DOD components and representatives to execute DSCA-managed SC programs. DSCA serves as the resource sponsor for G-TSCMIS and oversees the development and continued sustainment of the enterprise system. DSCA conducts SC and sales negotiations with foreign countries in accordance with USD(P) and DOS guidance and negotiates and concludes SC-related international programs. DSCA delegates the administration of SC programs, as appropriate, to either the MILDEPs, CCMDs, DOD agencies, or DOD field activities. DSCA establishes appropriate agreements and procedures with CCMDs and the Defense Intelligence Agency (DIA) for the respective SDOs/DATTs, to provide guidance and oversight of SC programs for which DSCA is responsible. DSCA advises the Defense Technology Security Administration (DTSA) of proposed transfers of significant new technologies and/or weapons systems and determinations of whether significant items or specific sales must be sold exclusively through FMS.

(2) DTSA. DTSA is a DOD field activity under the authority, direction, and control of the USD(P) that serves as the point of contact for development and implementation of DOD policy concerning technology security, export controls, and certain non-proliferation for military and dual-use items. DTSA identifies and mitigates national security risks associated with the international transfer of advanced technology and critical information. DTSA provides new and emerging partners with technological awareness via bilateral and multilateral engagements and negotiations, thereby ensuring applicable PNs have the agreements and security mechanisms in place to properly protect US technology. This assistance facilitates DOD objectives to build partnership capacity and capability and enhance interoperability. Additionally, DTSA responsibilities include managing the Space Launch Monitoring Program; DOD’s patent security review process; the development of DOD policy on technology security and foreign disclosure processes; and advising DOD leadership on the development of policy and procedures governing the disclosure and protection of classified military, and controlled unclassified information, to international partners.

(3) Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) is responsible for establishing and maintaining policies for the effective development of international acquisition, technology, and logistics programs, including international armaments cooperation (e.g., science and technology collaboration, logistics support), to support SC priorities. In coordination with USD(P), USD(AT&L) supports the development of policies and procedures for foreign transfer of defense-related articles, services, and technologies. In coordination with USD(P) and DOS, USD(AT&L) identifies, prioritizes, and pursues defense agreements required to facilitate the transfer of defense-related articles, services, and technologies to partners.

(4) In coordination with USD(P), the Under Secretary of Defense for Intelligence (USD[I]) provides guidance for and oversight of intelligence-related SC, including programs and resources, to build PN intelligence capabilities in support of SC priorities. USD(I) also ensures defense intelligence collection and analysis is sufficient to support SC planning, execution, and assessment, monitoring, and evaluation efforts.

(5) JS. The JS assists the CJCS regarding statutory responsibilities for the unified strategic direction of the US Armed Forces. However, the JS exercises no executive authority. The JS represents CJCS’s implementation guidance for military plans and programs and provides the CJCS with military advice concerning SC. In conjunction with USD(P), the JS reviews the SC activities included in CCMD campaign plans to ensure the planning guidance has been met. The JS also reviews allocation recommendations prior to SecDef approval of forces and other resources for the execution of military activities in campaign plans and operation orders. The JS produces the annual DOD campaign plan assessment template in consultation with USD(P) to integrate and coordinate Service support of CCMD campaign plans, as required. The JS recommends force and activity designators for priorities in the distribution of defense articles, defense services, and military education and training between and among PNs, organizations, and the US Armed Forces and recommends priorities for allocation of materiel and equipment for PNs when competing needs cannot be resolved by Director, DSCA. The JS collects and reviews the CCDRs’ campaign plans and the CCDRs’ assessments and evaluations, and advises the CJCS on the effectiveness of DOD SC efforts.

(6) CCMDs. Geographic CCMDs are the primary organizations for SC planning and integrating SC activities into their TCPs. Functional CCMDs prepare campaign plans that integrate their forces, resources, and funding for SC activities in coordination with the geographic CCMDs, their Service components, international organizations and, when appropriate, the affected SCOs. United States Special Operations Command (USSOCOM) coordinates SC activities to be executed by SOF with the geographic CCMDs through their theater special operations commands (TSOCs), including the deployment of special operations liaison officers, as well as SOF Service components. US Transportation Command coordinates movement within the Defense Transportation System, including integration of DOD and PN cargo distribution into existing force flow and global synchronization activities, as well as TDPs. CCMD planners should coordinate with COMs, through the SDO/DATTs, during the development of ICSs. These ICSs should, in turn, inform CCMD SC planners in the development of their required CSCSs/country plans. SC planning is typically led by the plans directorate of a joint staff (J-5) and supported by the other directorates (e.g., logistics directorate of a joint staff [J-4] for building PN logistic capacity). CCMD desk officers often lead country planning and work directly with the SDO/DATTs in their AORs and their counterparts in the Service component commands to develop country-level plans and identify forces and resource requirements. These desk officers are also the principal link between DOD-level staffs (OSD and JS) and the SDO/DATTs and their applicable country teams. CCMDs review their campaign plans by objectively and subjectively assessing, monitoring, and evaluating the effects of their SC activities in achieving desired objectives relative to attaining the intended end state. CCDRs must prioritize and approve the SC requirements of PNs established through coordination by the SDO/DATTs (as DOD members of COMs’ country teams) and Service component commands. CCMDs integrate SC activities into their CSCSs/country plans and campaign plans as necessary.

(7) TSOC. TSOCs are subordinate unified commands established by USSOCOM to plan, coordinate, conduct, and support joint special operations. These commands, and SOF, are under the combatant command (command authority) of USSOCOM, and under the operational control of the GCCs. Normally, GCCs exercise operational control of SOF through the TSOCs when operating within their AORs. TSOCs coordinate SOF integration and Service component support of SOF for FID, SFA, COIN, CT, FHA, unconventional warfare, and other special operations core activities in all campaigns and operations. TSOCs support SOF conducting SFA activities and other SC activities in support of the GCCs’ TCPs.

(8) MILDEPs, Services, and Service Component Commands. MILDEPs and Services support CCDR campaign plans and simultaneously pursue Service-specific SC objectives consistent with national and theater strategic objectives. MILDEPs, Services, and USSOCOM, in its Service-related responsibilities, support the CCMDs in shaping of the strategic security environment by enabling security conditions favorable to US objectives and interests. The Services may prepare Service CSPs at the discretion of the Service chief. Service CSPs integrate Title 10, USC, programs to support CCMD campaign and Service institutional objectives. If developed, and when appropriate, Services may synchronize CSPs with CCMD campaign plans through their respective component commands. The US Marine Corps and the US Navy each submit independent Service CSPs via the Department of the Navy. The US Army and the US Air Force submit their CSPs via their respective MILDEPs. Services are also responsible for executing sales made through SA. The Service component commands prepare supporting objectives and plans at the discretion of the component commander, CCDR, or Service chief to satisfy the requests or requirements of the supported commander’s plan. Supporting plans should be coordinated with the MILDEPs and may include organize, train, and equip responsibilities such as exercises, readiness, interoperability, augmentation, joint enablers, and capabilities development. Service components should also coordinate with SDO/DATTs on the country teams to determine potential military capabilities that could be made available to PNs through SC.

(9) SCO. This organization includes all DOD elements located in a foreign country with assigned responsibilities for carrying out SA/SC management functions. An SCO works under the authority of the COM. SCOs may be referred to as military assistance advisory groups, military missions and groups, offices of defense and military cooperation, liaison groups, and defense attaché personnel who have been designated to perform SA/SC functions. Military units conducting SC activities in an HN normally work closely with and coordinate with the SCO, but their lines of authority are through their Service components and the supported CCDR, not through the SDO/DATT to the COM. The SCO is responsible for assessing whether a PN can build and sustain capacity and has the greatest visibility over the execution of SC activities. Generally, the SCO is responsible for evaluating the results of SC activities and investments for the COM and GCC. Title 22, USC, Section 2321i (FAA) outlines the seven legislated SCO SA functions as follows:

(a) Equipment and services case management (i.e., FMS case management).

(b) Training management.

(c) Program monitoring.

(d) Evaluation and planning of the host government’s military capabilities and requirements.

(e) Administrative support.

(f) Promoting rationalization, standardization, interoperability, and other defense cooperation measures.

(g) Liaison functions exclusive of advisory and training assistance.

(10) SDO/DATT. The SDO/DATT serves as the diplomatically accredited defense attaché and chief of the SCO (if an SCO is present). As the COM’s principal military advisor on defense and national security issues and the senior DOD military officer assigned to a US diplomatic mission, the SDO/DATT serves as the single point of contact for all DOD matters involving the US mission or DOD elements assigned to or working from the US mission. All DOD elements under COM authority are within the coordinating authority of the SDO/DATT, except for the Marine security guard detachment and naval support units. The SDO/DATT operates under the authority of the COM and is the key figure within the US mission for establishing and fostering an SC relationship with the HN. The SDO/DATT, in collaboration with the GCC and other DOD components, provides DOD input to the ICS. The SDO/DATT, or a designated member of the SCO, is the point of contact for SC planning and development of the country plan with the GCC planners. Subject to COM approval, the SDO/DATT is the lead integrator for SC activities with the PN. For SC purposes, the SDO/DATT normally maintains coordination with Service/SOF components and their SMEs when assessing the HN for building partner capacity. The SDO/DATT, in coordination with the supported GCC, serves under the joint oversight and administrative management of the USD(P) and USD(I) through the Directors of DSCA and the DIA.

(11) The National Guard may appoint an officer to serve at the US mission under the SDO/DATT as the State Partnership Program (SPP) liaison for the partner state’s National Guard with the GCC and HN. The National Guard officer is nominated by the partner state’s adjutant general, approved by the National Guard Bureau (NGB), and accepted by the supported GCC. The National Guard officer coordinates all SPP events and activities among the NGB, US partner state, the specific country team, and the HN to facilitate the supported GCC SC policies, plans, and objectives. Also, the National Guard officer may assist in coordinating required support for bilateral and/or multilateral military engagements between the US and the HN, including activities not under SPP.

b. DOS. DOS maintains bureaus and offices (e.g., Office of US Foreign Assistance Resources, Bureau of East Asia and Pacific Affairs) functionally and/or geographically aligned with interagency partners (especially DOD), international organizations, and foreign nations to coordinate effective execution of the diplomacy, development, and defense aspects of US foreign policy. DOS analyzes the requirements for security-related assistance as part of USG foreign assistance. DOS maintains interagency coordination with respective counterparts in DOD concerning future SA programs and SC activities with PNs.

(1) COM. The COM, typically the US ambassador, is the principal officer in charge of a US diplomatic facility abroad. The COM is the personal representative of the President to the country of accreditation, and is responsible to the Secretary of State (SECSTATE) for the direction, coordination, and supervision of all USG executive branch employees in that country (except those under the command of a US area military commander). As statutorily mandated, the COM directs and supervises all activities in country and coordinates the resources and programs of the USG through the country team. COMs approve the ICSs developed through their country teams in coordination within DOS and through interagency coordination with DOD and other interagency partners at the national level. COMs, through the SDO/DATTs on their country teams, coordinate on the CCDRs’ CSCSs/country plans that will become part of the campaign plans. COMs facilitate the coordination of PN security-related requirements that become part of the specific SA programs and SC activities conducted by US military with those PNs.

(2) Country Team. The country team is the senior USG coordinating and supervising body in a foreign country. Headed by the COM, it includes the SDO/DATT, heads of all US embassy sections, and the senior member of each of the other represented USG departments or agencies, as desired by the COM. The country team issues directives to consulates, tasks action items for DOS offices and bureaus, and works to deconflict/balance all agency programs and priorities within the context of the COM’s ICS for that country. Depending on the size of a US embassy and the nature of US interests in a country, each country team may be configured differently—and some may include more than 40 interagency representatives, in addition to section chiefs and the head of the local USAID mission. With guidance from DOS and the COM, the country team develops the ICS regarding the PN, which influences the CCDR’s development of a CSCS/country plan for that PN.

(3) Bureau of Political-Military Affairs (PM). PM is DOS’s principal link to DOD. PM provides policy direction in the areas of international security, SA, and defense trade. PM’s primary counterpart in DOD is the Office of the Assistant Secretary of Defense for Strategy, Plans, and Capabilities. Joint force and Service planners may coordinate with PM through OSD and the JS.

## Security Cooperation---Excludes Security Assistance

### SC---Excludes Security Assistance---1NC

#### Security cooperation refers exclusively to mil-to-mil coop authorized explicitly by US Code---diplomatic and economic activities are security assistance

Tankel ’20 [Stephen and Tommy; October 28; associate professor at American University, an adjunct senior fellow at the Center for a New American Security, has served on the House Foreign Affairs Committee and in the Office of the Under Secretary of Defense for Policy; non-resident senior associate at the Center for Strategic and International Studies, served as deputy assistant secretary of defense for security cooperation and was the senior defense and intelligence adviser to Senate Majority Leader Harry Reid; War on the Rocks, “Retooling U.S. Security Sector Assistance,” <https://warontherocks.com/2020/10/reforming-u-s-security-sector-assistance-for-great-power-competition>]

The United States provides security sector assistance to foreign civilian and military forces, agencies, and institutions ranging from local law enforcement and judicial systems to standing militaries. This assistance is intended to strengthen U.S. access to key territories and facilities, shape partners’ national security decision-making and governance, and build their capacity and capabilities for use against shared threats and adversaries. It also promotes the U.S. defense industry via arms transfers, supports the infrastructure and operations of multilateral organizations such as NATO, and increases military interoperability. The State Department implements assistance across the entire security sector, including organizations responsible for defense, law enforcement, and security of key assets like ports and borders. The Department of Defense has a narrower mandate, and provides assistance to partner militaries under the umbrella of security cooperation. The Pentagon also engages in a range of other activities — combined exercises, staff talks, port visits, and officer exchanges — that fall under security cooperation as well. We use the term security sector assistance for simplicity, and distinguish where these additional security cooperation activities are relevant. The U.S. government does not typically define Foreign Military Sales as assistance, but we believe it should, and that it ought to factor Direct Commercial Sales into its assistance planning as well. Both types of sales can lead to sustained U.S. engagement with a partner in the form of training, maintenance, and sustainment for the purchased items.

Over the last several years, the national security enterprise has, with a great many fits and starts, endeavored to shift its broader focus — from weapons systems to diplomacy — away from counter-terrorism and toward strategic competition with state actors. As part of this shift, policymakers have attempted to realign security assistance to contribute more directly to strategic competition, primarily by creating new resources for security assistance in Europe and the Asia-Pacific region. The European Deterrence Initiative, launched in 2014, has allocated around $6 billion annually to enhance America’s deterrent posture vis-à-vis Russia. It has been supplemented by the Ukraine Security Assistance Initiative, authorized by Congress in Fiscal Year 2016 to provide $250 million in security assistance to bolster Ukraine’s security. Congress also created the Southeast Asia Maritime Security Initiative in 2014, later re-designated as the Indo-Pacific Maritime Security Initiative, and funded it as a five-year, $425 million security assistance effort, which it has since extended through FY2025. This program is intended to improve the ability of Southeast and East Asian nations to address growing Chinese assertiveness in the South China Sea. In the FY2021 defense bill currently being finalized, Congress is set to authorize a Pacific Deterrence Initiative, modeled on the European Deterrence Initiative, with as much as $6 billion annually to improve U.S. posture in the Asia-Pacific region, reportedly with a significant security assistance component.

These efforts have been laudable, but far from sufficient. The European Deterrence Initiative has largely been used to shift enduring costs for U.S. military presence in Europe into the Overseas Contingency Operations portion of the defense budget. It has also dedicated the vast majority of funds to posture and equipment pre-positioning, with little attention to security assistance beyond combined exercises — a significant missed opportunity. The Ukraine Security Assistance Initiative has been managed insularly by the U.S. Europe Command, which has bypassed synchronization with other Defense Department and U.S. government stakeholders, leading to a focus on the provision of “training and equipment at the expense of developing a long-term strategic vision and implementation of meaningful defense reform.” In the Asia-Pacific, the Maritime Security Initiative has shown promise, but its relatively limited funding has failed to significantly contribute to a rebalance of assistance toward the region, and it has largely funded projects with little deterrent value. Incoming U.S. Indo-Pacific Commander Adm. Philip Davidson declared, “China is now capable of controlling the South China Sea in all scenarios short of war with the United States.” Moreover, none of these initiatives have prioritized partner security sector governance — a vital element of any strategy that seeks to shape the behavior of U.S. allies and partners. As Congress considers the Pacific Deterrence Initiative, it is essential that these mistakes — failure to integrate security assistance with other instruments of national power, overemphasis on posture at the expense of cooperation, and too little ambition for assistance initiatives — are not repeated. Even avoiding them, however, will go only so far in terms of optimizing security sector assistance for the challenges ahead. The U.S. government should also address broader challenges with the way security sector assistance is prioritized and executed.

Still an Outmoded Instrument

To increase the effectiveness of security sector assistance for strategic competition, the United States should address deficiencies related to where and how it uses this assistance. Currently, assistance is focused on the wrong countries and being used to build the wrong capabilities. Assistance remains over-directed toward countries in the Middle East, Africa, and South and Central Asia, rather than to those in Europe and Southeast Asia where the main competition with Russia and China occurs. There are several reasons for this disparity.

First, annual commitments to Israel and Egypt — totaling $3.3 billion and $1.3 billion, respectively — eat up a large portion of the Foreign Military Financing budget. The origins of U.S. munificence to both countries is linked to the “payoff for peace,” that is, the U.S. commitment to Israel and Egypt after they signed the 1979 Camp David Accords. Distinct from the Foreign Military Sales program, through which the State Department brokers purchases of U.S.-made defense articles and defense services by foreign partners, the Foreign Military Financing program provides grants and loans to help partners, generally lower-income countries, purchase those articles and services. It is intended to be the premier program for building the capabilities of frontline allies and partners. Given its purpose, one would think that the United States would be steering more Foreign Military Financing toward Europe and Asia.

Second, the 9/11 attacks brought new requirements: promoting counter-terrorism cooperation and rapidly building the capacity of local part­ner forces, especially the creation or enhancement of tactical units, to address “urgent and emergent threats.” This naturally led to a focus on countries where terrorists operated or might take root, which reinforced the geographic focus on the Middle East, and expanded it to include countries in Central and South Asia. This focus was especially marked at the Defense Department. The amount of assistance it administers climbed significantly since 9/11, and totaled just over $7.5 billion in the FY2021 budget request. Approximately $6.5 billion comes from contingency funds for capacity building in Afghanistan, Iraq, and other conflict zones. Supporting these conflicts created additional security assistance cost centers among partners that played critical roles supporting counter-terrorism operations and U.S. logistics footprints. For example, Pakistan received over $23 billion in security assistance and military reimbursements as a result of its importance to the United States as a counter-terrorism partner after 9/11. Jordan has also experienced a marked increase in assistance over the same period, receiving close to $10 billion.

Overall, the United States spends about $20 billion annually on security sector assistance, of which only approximately 8 percent is allotted to Europe, East Asia, and the Pacific, according to Security Assistance Monitor. Addressing this imbalance will require the departments of State and Defense to reprioritize their budget requests, and Congress to cease earmarking security sector assistance dollars based on outmoded objectives.

The overriding focus on counter-terrorism in U.S. security sector assistance programs and national security strategy more broadly over the past two decades has not only contributed to its orientation toward the Middle East, Africa, and South and Central Asia. It also compounded challenges related to how the United States uses assistance, specifically America’s emphasis on countering urgent threats and on capacity building for counter-terrorism or special operations units. Where the State Department provides assistance to civilian security sector forces and institutions in other countries, it overemphasizes building tactical capabilities for law enforcement (that is, training small operational units on narrow capabilities like interdicting narcotraffickers or conducting counterterrorism raids) at the expense of the administrative capacity and professionalism of these forces and institutions. Defense Department assistance has similarly focused on building the tactical capabilities of partner militaries. Such tactical assistance — which often includes status-signaling weapons systems and resources to supplement partner personnel training budgets — is often prioritized by partners as well, particularly in the absence of effective U.S. messaging on the importance of broader reforms.

The U.S. emphasis on counter-terrorism led to a buildup of Special Operations Command and the services’ special operations forces components as well, and a commensurate focus on building the capacity of their special operations counterparts in other countries. Although the services dispense assistance, they don’t invest much in terms of the planning necessary to tie the execution of this assistance to either specific objectives or longer-term engagements. Other than the Army’s Security Force Assistance Brigades, the services don’t organize for the security sector assistance mission. Even in the Asia-Pacific, the main focus of assistance prior to the Maritime Security Initiative was the special operations forces capacity-building mission in the Philippines. This focus on special operations force has left the services, and U.S. partners’ conventional forces, out of the equation in many places. Iraq and Afghanistan are a notable exception, but even in these countries the United States has focused on building specific types of military units with a heavy emphasis on partner special operations capacity.

While the United States has directed security sector assistance toward the Middle East and South and Central Asia, and focused more on building partners’ tactical capacity for counter-terrorism, Russia and China are using aggressive military pressure to coerce neighbors and compete in new domains, such as cyber and space. They are also using instruments of statecraft outside the traditional security arena, such as economic pressure, lawfare, and even technical standards-setting. For example, China has used commercially flagged fishing vessels to perform militia-like functions in support of its activities around South China Sea features. Russia has used its cyber capabilities to disrupt critical infrastructure, interfere in elections, undermine political leaders, and spread disinformation throughout NATO-aligned Eastern Europe. The United States has failed to keep pace — either on its own in terms of its use of all instruments of national power, or in terms of the security assistance it provides partners to enhance their capabilities to mount effective responses and build resilience.

Optimizing Security Sector Assistance

If security assistance is to be an effective tool in strategic competition, then the U.S. government needs to step up its game. Washington should develop a sophisticated, integrated planning process at the State Department and Department of Defense for security assistance; significantly increase the Foreign Military Financing budget, or redirect spending from the Middle East and North Africa to Asia and Eastern Europe; use security assistance to convey strategic messages to both rivals and partners; and feature human rights considerations more prominently when engaging in arms sales. This would require the United States to address underlying deficiencies in planning, prioritization, and execution in ways that account for the unique challenges that Russian and Chinese approaches to competition bring: the use of disinformation, private security contractors, cyber tools, and civilian and commercial actors such as commercial fishing fleets. This is not to suggest that Washington should look to security sector assistance as the solution to all of its national security challenges — far from it. Rather, assistance should be better integrated with other instruments of national power. The following recommendations are intended to close the gap between where the United States currently is regarding its use of security sector assistance and where it needs to be to compete effectively. Some of these recommendations are focused more squarely on China and Russia, whereas others relate to broader reforms to the security sector assistance enterprise.

First, it is essential to create coordinated, department-wide planning processes at the departments of State and Defense. The U.S. government is hamstrung by inefficient and incoherent planning and coordination processes that do not allocate assistance based on U.S. foreign policy priorities, country prioritization, availability of resources, and regional and country-specific assumptions. Congressional earmarks make prioritization more difficult, but getting rid of them won’t solve the problem. Policymakers should recognize the fundamentally interdisciplinary nature of many aspects of strategic competition and begin to break down stovepipes both within and between key agencies involved in the planning and execution of security assistance. Interagency coordination should move beyond mere deconfliction and concurrence toward a truly collaborative real-time planning and response. Lack of coordination also exists within departments, which should reform their assistance planning processes. Of equal importance, security sector assistance planning and prioritization should account for the fact that China and Russia are mounting sustained challenges to governance and rule of law at the regional, national, and multinational levels. Advancing governance and rule of law therefore should be a key aim of assistance.

The State Department has a wider mandate for security assistance, encompassing both military aid and assistance for civilians. It is also supposed to use security assistance to advance broader, more long-term objectives like trade and investment, efforts to help allies and partners develop an innovation base, and major diplomatic initiatives. To fulfill this mission, the State Department should develop a planning process that elevates common interagency objectives for assistance, deconflicts competing objectives where necessary, identifies security assistance resources projected to be available for the period of time necessary to achieve such objectives, and recommends the allocation of assistance based on U.S. foreign policy priorities. Those priorities should be derived from the next administration’s national security strategy and informed by the availability of resources, and regional and country-specific assumptions. State also needs to create a framework to guide the use of assistance as dictated by the above planning process in alignment with other instruments of national power, and a framework for factoring in how arms sales — both Foreign Military Sales and Direct Commercial Sales — might affect U.S. security assistance planning and broader U.S. foreign policy objectives. Last year, the House of Representatives passed a State Authorization Act that required these and other reforms, but it has languished in the Senate since then.

Defense Department assistance should focus narrowly on four inherently military objectives: supporting State Department-coordinated efforts to build long-term capacity so that an ally or partner can manage its own security challenges; achieving a fundamental improvement in U.S. posture to prevail (including via coalitions) in a potential contingency, for example by assisting a partner to build a deep-water port or develop the capability to contribute in a specific role to potential coalition operations; generating short-term capacity when deemed necessary to achieve strategic objectives or improving interoperability for a specific goal; and responding to real-time developments, such as deterrent signaling, personnel recovery, or humanitarian response. Defense Department planners should be required to identify the objective(s) they’re serving and justify their plans on that basis. They also should be conducting a rigorous analysis to identify gaps in Pentagon plans for contingency scenarios involving near-peer competitors or other real-time developments that could impact U.S. interests, and basing priorities for security assistance on those gaps. Stronger links between contingency planning and security cooperation will help focus Defense Department security assistance and advance strategic competition.

Second, a more sophisticated and coordinated planning process should lead the United States to redirect security assistance to U.S. allies and partners in Asia and Eastern Europe, and expand the nature of assistance provided. The U.S. government has begun shifting some assistance, such as Section 333 capacity building administered by the Pentagon, away from U.S. Central Command countries to countries in the U.S. European Command and U.S. Indo-Pacific Command regions. The State and Defense departments need to accelerate this shift to compete more effectively with Russia and China. The United States should be using Foreign Military Financing, as well as Maritime Security Initiative funding and other programs, to help regional states in Asia develop anti-access/area denial systems to challenge Chinese power-projection operations. The departments of State, Defense, and Homeland Security should also be coordinating to increase support for U.S. Coast Guard cooperation with allies and partners to challenge China’s white hull strategy.

Realizing a significant reallocation of security assistance in support of strategic competition will require increasing the overall budget for Foreign Military Financing. These budgets have declined from a peak of $9.4 billion in FY2015 to the current year’s $7.5 billion, while the importance placed on security cooperation with allies and partners and the variety of threats they face have increased. The amount of such an increase will depend on the needs of key allies and partners, and whether Congress is willing to reduce Foreign Military Financing to Israel and Egypt, which in some years accounts for nearly two-thirds of the program’s budget. Unquestionably, the State Department can improve its prioritization of the remaining amount, which is spread across more than 100 partners globally, but those limited resources go only so far.

In our experience, selling Congress on an injection of resources or on reductions to Israel and Egypt will require considerable effort. The State Department would need not only to provide a compelling strategy for how resources that can be freed up by reducing commitments to Israel and Egypt will be used to improve America’s national security posture. It also will need to provide a convincing assessment that such reductions will not infringe on Israel’s qualitative military edge in the region or lead to a breakdown in the peace treaties between Israel and Egypt. We believe these crucial U.S. interests — Israel’s security and regional stability — can be maintained at lower aid levels. However, we are also realistic about the political challenges that make such a shift so difficult regardless of what any policy analysis suggests. For this reason, although we typically would recommend starting with a reallocation of existing resources before increasing the overall budget, in this instance we recognize that directing more money to the problem might be the least-worst option. A compelling case can be made for new resources and authorities to expand the types of aid provided under Foreign Military Financing — including to address the gaps identified above, such as cyber security and law enforcement. The argument will be strongest if it is articulated within broader strategies for competing with China and Russia.

In addition to Foreign Military Financing, there are a mix of other programs the United States could use to increase the capacity and capabilities of key Eastern European NATO allies. As Max Bergmann observed on these pages a few years ago, Congress is likely to be unwilling to provide much assistance funding through traditional grant methods, especially as Eastern European countries are wealthier than typical grant assistance recipients. This approach is deeply flawed: Many of Eastern Europe’s governments lack the economic wherewithal to engage in the types of military development necessary to compete with Russia. Moreover, the United States has clear and urgent goals in the region that should not be left dependent on the vicissitudes of partners’ budget politics. At the same time, we agree with Bergmann that the United States cannot and should not shoulder too much of the responsibility for these countries, which should demonstrate a commitment to acquisitions. One of the problems with Foreign Military Sales, though, is that U.S. weapons systems that Eastern European militaries would need to compete with Russia are top-of-the-line and likely unaffordable for midtier countries. Providing excess defense articles is one workaround, but this puts recipients at the mercy of what is available. Bergmann’s recommendation that the United States provide a mix of grants and loans to help NATO countries make acquisitions themselves is a fine one, and we would offer complementary or alternative approaches as well. The U.S. government could consider a lend-lease program in which equipment itself is provided via a loan or low-cost lease for a period of time to be used in an agreed-upon manner, after which the recipient could purchase the equipment at a reduced cost. Pooled sales and multilateral cooperative platforms modeled on the Movement Coordination Center Europe are other promising solutions. Any one of these models would be an improvement on the current approach.

As China, Russia, and others compete across a range of domains stretching beyond traditional military strength — cyber security, law enforcement, and disinformation — the U.S. government should enhance its ability to provide timely, relevant assistance in these areas. In our experience in government, American allies and partners routinely ask for this assistance. Yet, U.S. capacity building in each of these areas is immature. Cyber security assistance is meagerly resourced and often ad hoc, with limited assistance programs spread incoherently across government agencies. Likewise, intelligence and law enforcement capacity building are limited and often plagued by turf battles. Enabling allies and partners to counter disinformation represents an emerging area of focus, and Washington should rise to the occasion. In many of these areas, effective governance is often one of the most crucial gaps America’s allies and partners confront. To meet these challenges, the United States should reimagine security sector assistance, factor in its impact on governance and rule of law, and increase the involvement of the departments of Homeland Security, Justice, and Treasury.

#### Any other interp expands the topic to include arms sales, lend-lease programs, law enforcement, and critical infrastructure---on a bidirectional topic with no unique neg ground, that massively overstretches the research burden and undermines preparedness for all debates

### SC---Excludes SA---2NC Must-Read

#### Topical affs can only derive authority to act from Title 10 security coop provisions---none of the very Title 22 sources of “security cooperation” authorize multilateral coop---we’ll insert this comprehensive list of all SC authorities.

---AT: aff ground/no topical affs---relevant sources of Title 10 authority to defend topical affs are underlined

Thaler et al. ’16 [David E., Michael J. McNerney, Beth Grill, Jefferson P. Marquis, Amanda Kadlec; 2016; Senior International/Defense Researcher at the RAND Institute, M.I.A. in International Security Policy from Columbia; Acting Director, International Security and Defense Policy Center; Senior International/Defense Researcher and Affiliate Faculty, Pardee RAND Graduate School; RAND Institute, “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1438/RAND_RR1438.pdf>]

List of Existing SC Authorities

The following is an extensive list of Title 10 and other authorities and relevant Public Laws that are categorized as activity-based, mission-based, or partner-based and divided into subcategories based on their primary purpose. This list is current as of the FY 2016 NDAA. The list differentiates core authorities (in regular font) from supporting statutes (in italicized font), as described in Chapter Four. At the end of the categorized authorizations is a list of key SC programs that originate in appropriations and not authorization legislation.

Although the focus of our study is on Title 10 authorities, we include SC-related Title 22, Title 50, and Title 6 authorities in brackets at the end of each relevant subcategory of activities.

Existing Activity-Based Authorities

• Military-to-Military Engagements

- U.S. Code, Title 10, Section 168, Military-To-Military Contacts and Comparable Activities

- U.S. Code, Title 10, Section 1050, Latin American Cooperation: Payment of Personnel Expenses

- U.S. Code, Title 10, Section 1050a, African Cooperation: Payment of Personnel Expenses

- U.S. Code, Title 10, Section 1051, Bilateral or Regional Cooperation Programs: Payment of Personnel Expenses

- U.S. Code, Title 10, Section1051a, Liaison Officers of Certain Foreign Nations; Administrative Services and Support; Travel, Subsistence, Medical Care, and Other Personal Expenses

- Public Law 104-201, Section 1082, Exchange of Defense Personnel Between the United States and Foreign Countries

- Public Law 111-84, Section 1207, Authority for Nonreciprocal Exchanges, amended by Public Law 114-92, Section 1204, Extension of Authority for Nonreciprocal Exchanges of Defense Personnel Between the United States and Foreign Countries

- Public Law 112-239, Section 1275, U.S. Participation in Headquarters Eurocorps

- Public Law 113-291, Section 1203, Enhanced Authority for Provision of Support to Foreign Military Liaison Officers of Foreign Countries While Assigned to the Department of Defense

- [U.S. Code, Title 22, Section 2151, Congressional Findings and Declaration of Policy, U.S. Development Cooperation Policy]

- [U.S. Code, Title 22, Section 2767, Authority of President to Enter Into Cooperative Projects with Friendly Foreign Countries]

- [U.S. Code, Title 22, Section 2396g(2), Availability of Funds: Distinguished Visitor Orientation Tours]

- [Public Law 113-66, Section 1205, Authorization of National Guard State Partnership Program, as amended by Public Law 114-92, Section 1203, Redesignation, Modification, and Extension of National Guard State Partnership Program (Title 32 authority)]

• Exercises

- U.S. Code, Title 10, Section 153, Chairman: Functions

- U.S. Code, Title 10, Section 166a, Combatant Commands: Funding Through the Chairman of Joint Chiefs of Staff (CCIF) (for combined exercises, military education, and training)

- U.S. Code, Title 10, Section 2010, Participation of Developing Countries in Combined Exercises: Payment of Incremental Expenses

- U.S. Code, Title 10, Section 2011, Special Operations Forces: Training with Friendly Foreign Forces

- U.S. Code, Title 10, Section 2805, Unspecified Minor Construction

- Public Law 113-66, Section 1203, Training of General Purpose Forces of the U.S. Armed Forces with Military and Other Security Forces of Friendly Foreign Countries

• Individual Education / Technical Training

- U.S. Code, Title 10, Section 184, Regional Centers for Security Studies

- U.S. Code, Title 10, Chapter 905, Aviation Leadership Program

- U.S. Code, Title 10, Section 2111b, Senior Military Colleges: Department of Defense International Student Program

- U.S. Code, Title 10, Section 2103, Eligibility for Membership Senior Reserve Officers' Training Corps

- U.S. Code, Title 10, Section 2114, Uniformed Services University of the Health Sciences Students: Selection; Status; Obligation

- U.S. Code, Title 10, Section 2166, Western Hemisphere Institute for Security Cooperation

- U.S. Code, Title 10, Section 2249c, Regional Defense Combating Terrorism Fellowship Program: Authority to Use Appropriated Funds for Costs Associated with Education and Training of Foreign Officials

- U.S. Code, Title 10, Section 2249d, Distribution to Certain Foreign Personnel of Education and Training Materials and Information Technology to Enhance Military Interoperability with the Armed Forces

- U.S. Code, Title 10, Section 2350m, Participation in Multinational Military Centers of Excellence

- U.S. Code, Title 10, Section 4344, Foreign Cadets Attending the Military Academy

- U.S. Code, Title 10, Section 4345, Military Academy Exchange Program with Foreign Military Academies

- U.S. Code, Title 10, Section 4345a, Military Academy Foreign and Cultural Exchange Activities

- U.S. Code, Title 10, Section 6957, Foreign Midshipmen Attending the Naval Academy

- U.S. Code, Title 10, Section 6957a, Naval Academy Exchange Program with Foreign Military Academies

- U.S. Code, Title 10, Section 6957b, Naval Academy Foreign and Cultural Exchange Activities

- U.S. Code, Title 10, Section 7046, Officers of Foreign Countries: Admission to Naval Postgraduate School

- U.S. Code, Title 10, Section 7234, Submarine Safety Programs: Participation of NATO Naval Personnel

- U.S. Code, Title 10, Section 9344, Selection of Persons from Foreign Countries, Air Force Academy

- U.S. Code, Title 10, Section 9345, Exchange Program with Foreign Military Academies

- U.S. Code, Title 10, Section 9345a, Foreign and Cultural Exchange Activities

- U.S. Code, Title 10, Section 9415, Inter-American Air Forces Academy

- Public Law 113-291, Section 5530, Authorized Duration of Foreign and Cultural Exchange Activities at Military Service Academies

- Public Law 113-291, Section 1268, Inter-European Air Forces Academy

- [U.S. Code, Title 22, Section 2347, International Military Education and Training]

- [U.S. Code, Title 22, Section 2347c, Exchange Training: Reciprocity Agreement]

- [U.S. Code, Title 22, Section 8422a, Authorization of Assistance: International Military Education and Training]

- [U.S. Code, Title 32, National Guard]

• Unit Train And Equip

- U.S. Code, Title 10, Section 2282, Authority to Build the Capacity of Foreign Security Forces, as amended by Public Law 114-92, Section 1206, One-Year Extension of Funding Limitations for Authority to Build the Capacity of Foreign Security Forces; Public Law 112-81, Section 1207, Global Security Contingency Fund, as amended by Public Law 113-291, Section 1201

- U.S. Code, Title 10, Section 408(C), Equipment and Training of Foreign Personnel to Assist in Department of Defense Accounting for Missing United States Government Personnel

- Public Law 110-417, Section 943, Authorization of Noncon- ventional Assisted Recovery Capabilities, as amended by Public Law 114-92, Section 1271, Two-Year Extension and Modification of Authorization for Nonconventional Assisted Recovery Capabilities

- [U.S. Code, Title 22, Section 2349aa-10, Antiterrorism Assistance]

- [U.S. Code, Title 22, Section 8422b, Authorization of Assistance: Foreign Military Financing Program]

• Equipment and Logistics Support

- U.S. Code, Title 10, Section 127d, Allied Forces Participating in Combined Operations: Authority to Provide Logistic Support, Supplies, and Services (Global Lift and Sustain)

- U.S. Code, Title 10, Section 2249e, Prohibition on Use of Funds for Assistance to Units of Foreign Security Forces That Have Committed a Gross Violation of Human Rights

- U.S. Code, Title 10, Section 2341, Authority to Acquire Logistic Support, Supplies, and Services for Elements of the Armed Forces Deployed outside the United States

- U.S. Code, Title 10, Section 2342, Cross-servicing Agreements

- U.S. Code, Title 10, Section 2350c, Cooperative Military Airlift Agreements: Allied Countries

- U.S. Code, Title 10, Section 2350d, Cooperative Logistic Support Agreements: NATO Countries

- U.S. Code, Title 10, Section 2350f, Procurement of Commu-nications Support and Related Supplies and Services

- U.S. Code, Title 10, Section 2539b, Availability of Samples, Drawings, Information, Equipment, Materials, and certain services

- U.S. Code, Title 10, Section 2562, Limitation on Use of Excess Construction or Fire Equipment From Department of Defense Stocks In Foreign Assistance or Military Sales Programs

- U.S. Code, Title 10, Section 2667, Leases: Non-Excess Property of Military Departments and Defense Agencies

- U.S. Code, Title 10, Section 4681, Surplus War Material: Army Sale to States and Foreign Governments

- U.S. Code, Title 10, Section 7227, Foreign Naval Vessels and Aircraft: Supplies and Services

- U.S. Code, Title 10, Section 7307, Disposals of Naval Vessels to Foreign Nations

- U.S. Code, Title 10, Section 9626, Aircraft Supplies and Services: Foreign Military or Other State Aircraft

- U.S. Code, Title 10, Section 9681, Surplus War Material: Air Force Sale to States and Foreign Governments

- Public Law 109-163, Section 1208, Reimbursement of Certain Coalition Nations for Support Provided to U.S. Military Operations, as amended by Public Law 114-92, Section 1212, Extension and Modification of Authority for Reimbursement

of Certain Coalition Nations for Support Provided to U.S. Military Operations

- Public Law 110-252, 122 Stat. 2398, Coalition Readiness Sup-port Program, as amended by Public Law 113-291, Section 1222

- Public Law 110-181, Section 1233, Coalition Support Fund, as amended by Public Law 113-291, Section 1222

- Public Law 110-181, Section 1234, Logistical Support for Coali-tion Forces Supporting Operations in Iraq and Afghanistan, as amended by Public Law 113-291, Section 1223, One-Year Extension of Logistical Support for Coalition Forces Support-ing Certain United States Military Operations, as amended by Public Law 114-92, Section 1201

- Public Law 111-383, Section 1234, Report on Department of Defense Support for Coalition Operations

- Public Law 112-239, Section 1276, Department of Defense Participation in European Program on Multilateral Exchange of Air Transportation and Air-to-Air Refueling and Other Exchange Services (ATARES)

- Public Law 113-291, Section 1207, Cross Servicing Agreements for Loan of Personnel Protection and Personnel Survivability Equipment in Coalition Operations

- Public Law 113-291, Section 1210, Provision of Logistic Support for the Conveyance of Certain Defense Articles (in Afghanistan) to Foreign Forces Training with the U.S. Armed Forces

- Public Law 113-291, Section 1211, Biennial Report on Programs Carried Out by the Department of Defense to Provide Training, Equipment, or Other Assistance or Reimbursement to Foreign Security Forces

- Public Law 114-92, Section 1202, Strategic Framework for Department ofDefense Security Cooperation

- Public Law 114-92, Section 1207, Authority to Provide Support to National Military Forces of Allied Countries for Coun- terterrorism Operations in Africa

- [U.S. Code, Title 22, Section 2761, Sales from Stocks]

- [U.S. Code, Title 22, Section 2751, Need for International Defense Cooperation and Military Export Controls]

- [U.S. Code, Title 22, Section 2762, Procurement for Cash Sales]

- [U.S. Code, Title 22, Section 2302, Utilization of Defense Articles and Defense Services]

- [U.S. Code, Title 22, Section 2318, Special Authority (Drawdown)]

- [U.S. Code, Title 22, Section 2321h, Stockpiling of Defense Articles for Foreign Countries]

- [U.S. Code, Title 22, Section 2321i, Overseas Management of Assistance and Sales Programs]

- [U.S. Code, Title 22, Section 2321j, Authority to Transfer Excess Defense Articles]

- [U.S. Code, Title 22, Section 2753, Eligibility for Defense Services or Defense Articles]

- [U.S. Code, Title 22, Section 2763, Credit Sales]

- [U.S. Code, Title 22, Section 2767, Authority of President to Enter Into Cooperative Projects with Friendly Foreign Countries]

- [U.S. Code, Title 22, Section 2769, Foreign Military Construction Sales]

- [U.S. Code, Title 22, Section 2770a, Exchange of Training and Related Support]

- [U.S. Code, Title 22, Section 2776, Reports and Certifications to Congress on Military Exports]

- [U.S. Code, Title 22, Section 2796, Leasing Authority]

- [U.S. Code, Title 22, Section 8422b, Authorization of Assistance: Foreign Military Financing Program]

• Research, Development, Test, and Evaluation (RTD&E)

- U.S. Code, Title 10, Section 2350a, Cooperative Research and Development Agreements: NATO Organizations; Allied and Friendly Foreign Countries

- U.S. Code, Title 10, Section 2350l, Cooperative Agreements for Reciprocal Use of Test Facilities: Foreign Countries and International Organizations

- U.S. Code, Title 10, Section 2358, Research and Development Projects

- U.S. Code, Title 10, Section 2360, Research and Development Laboratories: Contracts for Services of University Students

- U.S. Code, Title 10, Section 2365, Global Research Watch Program

- U.S. Code, Title 10, Section 2531, Defense Memoranda of Understanding and Related Agreements

- [U.S. Code, Title 22, Section 2796d, Loan of Materials, Supplies, and Equipment for Research and Development Purposes]

• Intelligence Sharing and Exchange

- U.S. Code, Title 10, Section 443, Imagery Intelligence and Geospatial Information: Support for Foreign Countries

- U.S. Code, Title 10, Section 454, Exchange of Mapping, Charting, and Geodetic Data with Foreign Countries, International Organizations, Nongovernmental Organizations, and Academic Institutions

Existing Mission-Based Authorities

• Humanitarian Assistance/Health

- U.S. Code, Title 10, Section 401, Humanitarian and Civic Assistance (HCA) Provided in Conjunction with Military Operations

- U.S. Code, Title 10, Section 402, Transportation of Humani-tarian Relief Supplies to Foreign Countries

- U.S. Code, Title 10, Section 404, Foreign Disaster Assistance

- U.S. Code, Title 10, Section 407, Humanitarian Demining Assistance: Authority; Limitations

- U.S. Code, Title 10, Section 2557, Excess Nonlethal Supplies: Availability for Homeless Veteran Initiatives and Humanitarian Relief

- U.S. Code, Title 10, Section 2561, Humanitarian Assistance

- U.S. Code, Title 10, Section 182, Center for Excellence in Disaster Management and Humanitarian Assistance

- U.S. Code, Title 10, Section 2649, Civilian Passengers and Commercial Cargoes: Transportation on DoD Vessels, Vehicles, and Aircraft, as amended by Public Law 111-383, Section 352, Revision to Authorities to Transportation of Civilian Passengers and Commercial Cargoes by DoD When Space Unavailable on Commercial Lines

- Public Law 114-92, Section 1205, Monitoring and Evaluation of Overseas Humanitarian, Disaster, and Civic Aid Programs of the Department of Defense

- [Public Law 108-25, United States Leadership Against HIV/ AIDS, Tuberculosis and Malaria Act of 2003 (Title 22, for the President's Emergency Program for AIDS Relief)]

• Defense Institution Building

- Public Law 112-81, Section 1081, Authority for Assignment of Civilian Employees of the Department of Defense as Advisers to Foreign Ministries of Defense, as amended by Public Law 113-66, Section1094

- Public Law 113-291, Section 1047, Inclusion of Regional Orga-nizations in Authority for Assignment of Civilian Employees of DoD Advisers to Foreign Ministries of Defense

- Public Law 114-92, Section 1055, Authority to Provide Training and Support To Personnel of Foreign Ministries of Defense

- Public Law 113-291, Section 1206, Training of Security Forces and Associated Security Ministries of Foreign Countries to Promote Respect for the Rule of Law And Human Rights

• Counternarcotics

- U.S. Code, Title 10, Section 124, Detection and Monitoring of Illegal Drugs

- [U.S. Code, Title 22, Section 2291, International Narcotics Control]

- Public Law 101-510, Section 1004, Support for Counterdrug Activities, most recently amended by Public Law 113-291, Section 1012, Extension and Modification of DoD Authority to Provide Support for Counterdrug Activities and Other Governmental Agencies

- Public Law 105-85, Section 1033, Additional Support for Counterdrug Activities, amended by Public Law 111-84, Section 1014, Support for Counterdrug Activities of Certain Foreign Governments and Public Law 113-291, Section 1013, Additional Support for Counterdrug Activities of Certain Governments

- Public Law 108-375, Section 1021, Use of Funds for Unified Counterdrug and Counterterrorism Campaign in Colombia, most recently amended by Public Law 113-291, Section 1011, Unified Counterdrug & Counterterrorism Campaign in Colombia, Extension of Authority

- Public Law 108-136, Section 1022, Authority for Joint Task Forces to Provide Support to Law Enforcement Agencies Conducting Counterterrorism Activities, amended by Public Law 113-291, Section 1014, Extension of Joint Task Force to Support Law Enforcement Agencies

• Cooperative Threat Reduction and Nonproliferation

- Public Law 113-66, Section 1204, Authority to Conduct Activities to Enhance the Capability of Foreign Countries to Respond to Incidents Involving Weapons of Mass Destruction (to Respond to Syrian WMD), as amended by Public Law 114-92, Section 1273, Extension of Authorization to Conduct Activities to Enhance the Capability of Foreign Countries to Respond to Incidents Involving Weapons of Mass Destruction

- Public Law 113-291, Section 1321, Authority to Carry Out Department of Defense Cooperative Threat Reduction Program (No Expiration)

- [U.S. Code, Title 22, Section 5901, Demilitarization of Independent States of Former Soviet Union]

- [U.S. Code, Title 22, Section 5952, Authority for Programs to Facilitate Cooperative Threat Reduction]

- [U.S. Code, Title 22, Section 5853, Nonproliferation and Dis-armament Activities in Independent States]

- [U.S. Code, Title 22, Section 5854, Nonproliferation and Dis-armament Fund]

- [U.S. Code, Title 22, Section 2349bb-2a, International Non- proliferation Export Control Training]

- [U.S. Code, Title 22, Section 2301, Nonproliferation and Export Control Assistance: Authorization of Assistance]

- [U.S. Code, Title 50, Section 2333, International Border Security]

- [U.S. Code, Title 50, Section 2334, Interdiction of Weapons of Mass Destruction and Related Materials: Training Program]

- [U.S. Code, Title 50, Section 353, Matters Relating to the International Materials Protection, Control, and Accounting Program of the Department of Energy]

- [U.S. Code, Title 50, Section 2562a, Initiative for Proliferation Prevention Program]

- [U.S. Code, Title 50, Section 2569, Acceleration of Removal or Security of Fissile Materials, Radiological Materials, and Related Equipment at Vulnerable Sites Worldwide]

- [U.S. Code, Title 50, Section 2912, Authority to Provide Assistance to Cooperative Countries]

- [U.S. Code, Title 50, Section 3711, Authority to Carry Out Department of Defense Cooperative Threat Reduction Program]

- [Public Law 111-84, Section 3101, National Nuclear Security Administration]

- [Public Law 104-201, Section 1501b, Specification of Cooperative Threat Reduction Programs, as amended by Public Law. 113-291, Section1301, Specification of Cooperative Threat Reduction Programs]

• Counterterrorism

- Public Law 108-375, Section 1208, Support of Special Operations to Combat Terrorism, as amended by Public Law 114-92, Section 1274, Modification of Authority for Support of Special Operations to Combat Terrorism

- Public Law 113-291, Section 1510, Counterterrorism Partnership Fund

• Cooperative Ballistic Missile Defense

- U.S. Code, Title 10, Section 223, Ballistic Missile Defense Programs: Program Elements

- Public Law 105-85, Section 233, Cooperative Ballistic Missile Defense Program

- Public Law 105-261, Section 233, Limitation on Funding for Cooperative Ballistic Missile Defense Programs

• Maritime Security

- [U.S. Code, Title 6, Section 945, Container Security Initiative]

- Public Law 114-92, Section 1263, South China Sea Initiative

- [Public Law 107-295, Maritime Transportation Security Act of 2001]

• Cybersecurity

- U.S. Code, Title 10, Section 1051c, Multilateral, Bilateral, or Regional Cooperation Programs: Assignments to Improve Education and Training in Information Security, Established by Public Law 112-81, Section 951, Activities to Improve Multilateral, Bilateral, and Regional Cooperation Regarding Cybersecurity

Existing Partner-Based Authorities

- Public Law 110-181, Section 1513, Afghanistan Security Forces Fund, as amended by Public Law 113-291, Section 1532

- Public Law 111-383, Section 1216, Authority to Use Funds for Reintegration Activities in Afghanistan, as amended by Public Law 113-291, Section 1232, One-Year Extension

- Public Law 111-383, Section 1217, Authority to Establish a Program to Develop and Carry Out Infrastructure Projects in Afghanistan, Public Law 113-66, Section 1215, One- Year Extension and Modification of Authority for Program to Develop and Carry Out Infrastructure Projects in Afghanistan

- Public Law 112-239, Section 1222, Authority To Transfer Defense Articles And Provide Defense Services to the Military and Security Forces of Afghanistan; as amended by Public Law 113-291, Section 1231, as amended by Public Law 114-92, Section 1215, Extension of Authority to Transfer Defense Articles and Provide Defense Services to the Military and Security Forces of Afghanistan

- Public Law 109-163, Section 1202, Commanders' Emergency Response, as amended by Public Law 114-92, Section 1211, Extension and Modification of Commanders' Emergency Response

- Public Law 113-291, Section 1236, Authority to Provide Assistance to Counter the Islamic State of Iraq and the Levant (Known as Iraq Train and Equip Fund), as amended by Public Law 114-92, Section 1223, Modification of Authority to Provide Assistance to Counter the Islamic State of Iraq and the Levant

- Public Law 112-81, Section 1215, Authority to Support Operations and Activities of the Office of Security Cooperation in Iraq, as amended by Public Law 113-291, Section 1237, Extension and Modification of Authority to Support Operations and Activities of the Office of Security Cooperation in Iraq

- Public Law 113-59, Section 1209, Authority to Provide Assistance to the Vetted Syrian Opposition, as amended by Public Law 114-92, Section 1225, Matters Relating to Support for the Vetted Syrian Opposition

- Public Law 113-66, Section 1207, Assistance to the Government of Jordan for Border Security Operations

- Public Law 113-272, Section 6, Ukraine Freedom Support Act of 2014, Increased Military Assistance for the Government of Ukraine

- Public Law 114-92, Section 1250, Ukraine Security Assistance Initiative

- Public Law 114-92, Section 1251, Training for Eastern European National Military Forces in the Course of Multilateral Exercises

- Public Law 113-291, Section 1535, European Reassurance Initiative (Transfer of Funding for Specific Activities)

- Public Law 111-172, Lord's Resistance Army Disarmament and Northern Uganda Recovery Act of2009 (amends Title 22)

- Public Law 113-66, Section 1206, United States Security and Assistance Strategies in Africa

- Public Law 113-66, Section 1208, Support for Foreign Forces Participating in Counter-LRA Operations

- Public Law 113-291, Section 1253, Military-to-Military Engagement with the Government of Burma

- Public Law 114-92, Section 1261, Strategy to Promote United States Interests in the Indo-Asia-Pacific Region

- Public Law 114-92, Section 1279, United States-Israel Anti- Tunnel Cooperation

- [U.S. Code, Title 22, Section 2271, Central America Democracy, Peace, and Development Initiative]

- [U.S. Code, Title 22, Section 2295, Support for Economic and Democratic Development of the Independent States of the Former Soviet Union]

- [U.S. Code, Title 22, Section 8422d, Authorization of Assistance: Exchange Program Between Military And Civilian Personnel of Pakistan and Certain Other Countries]

### SC---Excludes SA---AT: “We Change Funding”---2NC

#### To “increase” means expanding already-existing cooperation.

Buckley ’6 [Jeremiah S, Joseph M. Kolar; November 13; partners at Buckley Kolar LLP; Westlaw, Brief of Amici Curiae for “Mortgage Insurance Companies of America and Consumer Mortgage Coalition,” WL 3309503]

First, the court said that the ordinary meaning of the word “increase” is “to make something greater,” which it believed should not “be limited to cases in which a company raises the rate that an individual has previously been charged.” 435 F.3d at 1091. Yet the definition offered by the Ninth Circuit compels the opposite conclusion. Because “increase” means “to make something greater,” there must necessarily have been an existing premium, to which Edo's actual premium may be compared, to determine whether an \*26 “increase” occurred. Congress could have provided that “adverse action” in the insurance context means charging an amount greater than the optimal premium, but instead chose to define adverse action in terms of an “increase.” That definitional choice must be respected, not ignored. See Colautti v. Franklin, 439 U.S. 379, 392-93 n.10 (1979) (“[a] definition which declares what a term ‘means' … excludes any meaning that is not stated”).

Next, the Ninth Circuit reasoned that because the Insurance Prong includes the words “existing or applied for,” Congress intended that an “increase in any charge” for insurance must “apply to all insurance transactions - from an initial policy of insurance to a renewal of a long-held policy.” 435 F.3d at 1091. This interpretation reads the words “existing or applied for” in isolation. Other types of adverse action described in the Insurance Prong apply only to situations where a consumer had an existing policy of insurance, such as a “cancellation,” “reduction,” or “change” in insurance. Each of these forms of adverse action presupposes an already-existing policy, and under usual canons of statutory construction the term “increase” also should be construed to apply to increases of an already-existing policy. See Hibbs v. Winn, 542 U.S. 88, 101 (2004) (“a phrase gathers meaning from the words around it”) (citation omitted).

### SC---Excludes SA---AT: Predictability---2NC

#### The vast majority of legislative authorities for security cooperation are Title 10, even if there are some Title 22 outliers

RAND Institute ’19 [RAND Research on Security Cooperation: 2006-2019, “Taking Stock of RAND's Security Cooperation Research,” studies highlighted and synthesized here were sponsored by the U.S. Army, the U.S. Air Force, and the Office of the Secretary of Defense and conducted in three federally funded research and development centers managed by RAND: RAND Arroyo Center, Project AIR FORCE, and the National Defense Research Institute, <https://www.rand.org/ard/topics/security-cooperation.html>]

The term security cooperation refers to the broad category of activities undertaken by the U.S. Department of Defense (DoD) "to develop partnerships that encourage and enable partner nations to act in support of US strategic objectives" A variety of other programs and activities (and associated terms) spanning the strategic, operational, and tactical levels fall under the umbrella of security cooperation. These include efforts to build partner capacity, security force assistance, and defense institution building. Security cooperation activities range from the expensive and visible—training, equipping, and exercising together—to low-key but valuable bilateral talks, workshops, personnel exchanges, professional military education, and efforts to achieve interoperability with partners in terms of processes and equipment.

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?

The RAND Corporation has studied the field of security cooperation extensively over the past two decades. By pulling together RAND's security cooperation research in one collection and highlighting what we have learned about the enterprise in this document, we seek to help answer these questions. The bulk of the works in this summary focus on DoD security cooperation, although a few studies also look at the security sector assistance activities of other agencies and departments, including the U.S. Department of State. Notably, in recent years, resources and authorities for security cooperation have shifted toward DoD and away from other agencies. The large number of security cooperation actors, programs, and activities across departments and agencies presents a number of challenges, particularly in measuring the effects of a specific program that is part of a broader U.S. engagement strategy.

This brief introduction discusses the main findings from RAND research in the main areas of security cooperation. The first section addresses the < href="#authorities-and-planning">literature on security cooperation authorities and planning. The second section focuses on security cooperation activities aimed at building partner capacity, security force assistance, and defense institution building, while the third distills the findings from research on security cooperation activities aimed at enhancing interoperability. The fourth section discusses RAND work on the relatively new area of assessing, monitoring, and evaluating security cooperation activities. In conclusion, the final section highlights lessons learned and best practices in security cooperation.

Jump To

Security Cooperation Authorities and Planning

Building Partner Capacity and Security Force Assistance

Security Cooperation Activities Aimed at Enhancing Interoperability

Assessing, Monitoring, and Evaluating Security Cooperation

Lessons Learned and Best Practices in Security Cooperation

Security Cooperation Authorities and Planning

One thread of RAND research has focused on how to improve security cooperation authorities, prioritization, and planning. Although sometimes overlooked, the issue of authorities is essential to the execution of security cooperation activities and one that continues to create challenges. There are a large set of potentially overlapping authorities that security cooperation planners need to navigate.

A 2016 study entitled From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation analyzed legislative authorities for security cooperation and found 160 total authorities, 123 of which are under Title 10. The report identified 106 "core" statutes that directly authorize activities and 17 supporting ones that legislate the transfer of funds or mandate reports to Congress. Dozens of interviews and focus group sessions revealed frustration and confusion about perceived gaps, overlaps, and ambiguities surrounding these authorities, a need for greater flexibility in addressing multifaceted or emerging threats, and a desire to improve on this patchwork that has developed over many years.

The study created a framework to organize authorities into several categories: authorities focused on particular activities (e.g., exercises), particular missions (e.g., counterterrorism), and particular partners (e.g., Pakistan). The study also identified opportunities for consolidating and revising existing authorities, starting by reducing the 106 core authorities to 91. Although the U.S. government has made recent progress in clarifying and reducing security cooperation authorities, much still needs to be done to better integrate Title 10 and Title 22 authorities, assess the effect of appropriations on security cooperation, and align notification and reporting requirements.

#### Security cooperation excludes security assistance programs

Gwinn ’22 [Jeremy; April 19; U.S. Army infantry officer currently in the Office of Security Cooperation–Iraq, Ph.D. in international relations from the Fletcher School of Law and Diplomacy; War on the Rocks, “Sweeter Carrots and Harder Sticks: Rethinking U.S. Security Assistance,” <https://warontherocks.com/2022/04/sweeter-carrots-and-harder-sticks-rethinking-u-s-security-assistance/>]

The What, Why, and How of Security Assistance

“Security assistance” refers to a specific set of programs authorized by the Foreign Assistance Act and Arms Export Control Act. These programs are overseen by the State Department in cooperation with the Department of Defense. “Security cooperation” describes separately authorized Defense Department-led activities such as “global train and equip” programs. The Ukraine Security Assistance Initiative, which has provided military aid to that country since 2016, is one such example of these programs run by the Pentagon. I will use the more common term here, security assistance, in reference to either type. When security assistance works well, it gives partner nations the tools to address internal instability and deter and defend against external adversaries, reducing the likelihood that direct U.S. intervention will be called for in the future. It also helps to ensure that the United States maintains access, basing, and overflight privileges, strengthens interoperability, and accrues the less tangible benefit of military-to-military personal relationships.

#### The DOD defines security coop as the authorities governed by Title 10 of US Code

Anderson ’19 [Melissa Dalton and James Anderson; April 25; Director of the Cooperative Defense Project at the Center for Strategic and International Studies; Assistant Secretary of Defense for Strategy, Plans and Capabilities Dr. James Anderson, served for three years as the vice president for academic affairs at the Marine Corps University, doctorate in international relations and master of arts in law and diplomacy from the Fletcher School at Tufts University; CSIS Keynote Address, “Shifting the Burden Responsibly: Oversight and Accountability in U.S. Security Sector Assistance,” https://www.csis.org/analysis/shifting-burden-responsibly-oversight-and-accountability-us-security-sector-assistance-0]

JAMES ANDERSON: Good afternoon. I want to start by thanking Melissa Dalton for the invitation to speak here today. I have had the pleasure of working with Melissa and am very appreciative of her research efforts and her team regarding security cooperation. It is an honor to speak here at CSIS where many of my current and former colleagues have come from.

This report could not be more timely. I have been briefed on the report’s main findings, and I appreciate the thorough CSIS review of oversight and accountability in the U.S. security sector assistance. This report reminds me of the important role that our friends in the think tank community play, especially when the department is embracing a new approach to the topic.

I’ve had the pleasure to serve in my current capacity as assistant secretary of defense for strategy, plans and capabilities since last fall. Our SPC office casts a wide net to include policy oversight of security cooperation, our National Defense Strategy, the plans necessary to implement the strategy, as well as nuclear deterrence and missile defense.

Security sector assistance is a vast enterprise, and it one of the U.S. governments most effective tools in shaping U.S. foreign policy outcomes. At DOD we represent a key component of that effort that we call security cooperation: the authorities governed by Title 10 of the U.S. Code, which relate to engaging with allied and partner militaries to affect outcomes related to our mutual security.

I want to focus my remarks here today on how we are reforming security cooperation within the department and creating a more holistic, strategic security – (audio break) – major lines of efforts for DOD as we implement our National Defense Strategy. The security interests of the United States and allies are best addressed together cooperatively. The United States has a critical leadership role in encouraging allies to be more militarily capable, interoperable, and lethal.

With these principles in mind, I’d like to proceed along the following path. I’d like to talk about where we are coming from and how the FY ’17 reforms, the security cooperation, and the National Defense Strategy are changing the way we are doing business. I would also like to talk about some of the gaps in our execution and highlight with some examples some places where we are successfully executing our mission and creating security through cooperation.

The United States has realized that the primary security challenge of our generation – great power competition – requires a strong network of allies and partners. At the same time, this administration feels strongly that allies and partners need to contribute their fair share towards common security interests.

Security cooperation is one of the best tools for our growing ally and partner capacity to contribute more militarily. With smart, limited investments in our partners, we can amplify military effects to deter aggression.

Today the United States is an exporter of security cooperation. However, as a young republic – or even before we became a republic, we were the recipient of security cooperation. For all the noble ideas the United States was founded upon, ideas cannot hope to make up for a shortage of gunpowder. The first thing that might be considered a foreign military sale the United States conducted was an important purchase: gunpowder covertly supplied by our friends, the French. And that arms transfer made a difference. Our first act of foreign military sale helped to win – helped us to win at Saratoga and turn the tide of the Revolutionary War.

Clearly things have changed greatly in the post-Cold-War environment. The reality is today that we are confronted by an array of emerging requirements and ever-present risks. Because of this, operating by, with, and through allies is not simply a goal; it is a necessity. It is the only path to sustainable progress in combating terrorism or countering any other international security threat including the reemergence of great power competition.

The release of the National Defense Strategy in 2018 marked a turning point for the whole of DOD. We live in an increasingly complex global security environment and, after many years without an update to our fundamental strategic guidance, the time had come to acknowledge changes in the international security environment and the priorities for the Department of Defense. The NDS emphasizes the need to shift the weight of our security cooperation resources from countering terrorism, which has of course been the primary focus of the department’s efforts over the past – nearly the past two decades to a renewed focus on deterring and potentially responding to threats from near-peer competitors.

Security cooperation relates to all three lines of effort in the National Defense Strategy. One, building lethality. Security cooperation allows us to improve our effectiveness in coalition efforts, to cover down on gaps in our posture, and to ensure that our partners pack a punch in the first few hours of conflict, or days of conflict, if it comes to that.

Two, strengthening U.S. alliances and partnerships. Security cooperation is the primary tool for ensuring our alliances and partnerships are fruitful, meaningful, and that our relationships are a net security contributor, not a detractor.

Three, reforming how the department does business. Security cooperation is evolving with the department to become more strategic, more efficient, and more effective. In FY ’19, we dedicated the greatest amount of funding – nearly 25 percent of the total funding in the security cooperation account – to challenges in the Indo-Pacific area of responsibility – nearly $260 million. This is an increase of nearly 75 percent over what we notified in the year prior, and this does not include regional initiatives such as the Maritime Security Initiative, which I will say more about in a few minutes. Consistent with the NDS, we also increased EUCOM’s allocation by nearly 25 percent from FY ’18 to approximately 250 million (dollars).

While CENTCOM continues to rely on separate authorities, in particular the Counter-ISIS Train and Equip Fund and the Afghan Security Forces Fund, we reduced its FY ’19 Section 333 allocation by 30 percent from the FY ’18 Level. AFRICOM, NORTHCOM, and SOUTHCOM, for their part, combined received about 30 percent of the total funding.

The NDS specifies clear priorities, and our security cooperation resource allocations reflect and will continue to reflect those priorities. All that said, I’d like to note at this point that Title 2 funding is still providing robust tools for engagement and financing of our partner militaries, even in those regions that are not prioritized in the NDS.

With all the changes in the last few years, the question arises, how do we explain security cooperation? How do we define it? I think a good way to look at security cooperation in terms of where we are going is to consider all activities conducted by the Department of Defense aimed at enhancing the capability and willingness of U.S. partners and allies to operate in coalition with – or in lieu of – U.S. forces in response to shared security challenges. This formulation is largely consistent with how we think Congress envisions our future role in security sector assistance.

DOD has always had a robust role in security sector assistance enterprise, but until FY ’17 reforms, it was spread across the department. There were many purse holders, many different executors, and dozens of legal authorities scattered in a patchwork-like fashion across the U.S. Code that overlapped, sometimes acted independently, and weren’t looked at holistically.

Sometime security cooperation doesn’t get a lot of attention. Luckily, CSIS has some of the finest minds in the security cooperation business at work here, and I’m most grateful for the work of Melissa, Kath, Tommy, and others for their efforts on this topic.

Security cooperation is often behind the news we read at night but rarely the frontline story. Luckily we’re also blessed with another influential group that cares deeply about security cooperation – the Congress. In FY ’17 Congress undertook the largest, most sweeping, and most substantial reforms to security cooperation in our nation’s history. The FY ’17 NDAA consolidated dozens of authorities into a narrow band of activities in Chapter 16. It set up requirements for human rights vetting, institutional capacity building, and assessment monitoring and evaluation.

With lots of work in the trenches by both DOD and Congress, this all hit at once, and it was welcome. Implementing an ambitious vision remains a challenge, particularly for those activities that were funded out of service accounts or regional initiatives. Many security cooperation activities were not being looked at holistically across the spectrum. Programs were siloed and oversight sometimes limited.

Congress believed that the entire system needed oversight from a single executor with visibility across all the authorities and all the different pots of money. This is how we got the Title 10, Chapter 16, Section 382 in the U.S. Code. The notion that the secretary’s designee, the undersecretary of defense for policy – my immediate boss – shall have, quote, “the responsibility for the oversight of strategic policy guidance and the responsibility of overall resource allocation for security cooperation programs and activities of the Department of Defense.” End quote.

This is where we are trying to go with security cooperation: a holistic DOD-wide enterprise with visibility across the spectrum of security cooperation activities, administered with policy oversight, and aligned tightly to strategy.

How we define security cooperation is changing as well. At one point security cooperation meant – basically meant train and equip programs. We’re moving away from that. Security cooperation enterprise now encompasses everything from equipment, to training, to conventional arms sales, to exercises with both high-end and developing partners.

Meanwhile, we are prioritizing interoperability and making arms sales quicker and more efficient. In the last 10 years the department has reduced the average time to process foreign military sales by 30 percent. And I know our colleagues at DSCA are working hard to streamline things even more.

We are also trying to move off of year-to-year planning. My office has been involved in a push over the last two years to align security cooperation planning with planning, programming, budgeting, and execution cycle as well as the global force management cycle, planning two years out from the current fiscal year.

#### CRS agrees.

Serafino ’16 [Bolko J. Skorupski and Nina M. Serafino; August 23; Research Assistant; Specialist in International Security Affairs; Congressional Research Service, “DOD Security Cooperation: An Overview of Authorities and Issues,” https://sgp.fas.org/crs/natsec/R44602.pdf]

Terminology: Security Assistance and Security Cooperation

“Security assistance” and “security cooperation” are two terms that refer to U.S. activities to train, equip, and otherwise assist foreign partners. The term security assistance is a generic term used throughout the U.S. government to describe assistance provided to foreign military and security forces, regardless of the agency providing that assistance. However, DOD uses the term security assistance to refer specifically to assistance provided under Title 22 authority, funded with monies appropriated to the State Department and managed by the Defense Security Cooperation Agency (DSCA), an agency under the Office of the Secretary of Defense, Policy.3

DOD defines “security cooperation” as a broad set of activities undertaken by DOD to encourage and enable international partners to work with the United States to achieve strategic objectives. Included in the definition are DOD interactions with both foreign defense and foreign nonmilitary security establishments. Security cooperation includes all DOD-administered security assistance programs that (1) build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities; (2) develop allied and friendly military capabilities for self-defense and multinational operations; and (3) provide U.S. forces with peacetime and contingency access to host nations.4 According to DOD, security assistance is a subset of DOD’s security cooperation portfolio.

Authority for DOD to conduct security cooperation activities is enacted in two primary places: Title 10 (Armed Forces) U.S.C. and National Defense Authorization Acts.

### SC---Excludes SA---Violation---2NC

#### Title 22 programs excluded: IMET, counter-narcotics, FMF, and humanitarian assistance

Stark ’20 [Alexandra; Oct 26; PhD from the government department at Georgetown University, a research fellow at the Middle East Initiative of the Harvard Kennedy School’s Belfer Center for Science and International Affairs, and Minerva/Jennings Randolph Peace Scholar at the United States Institute of Peace; New America, “Managing U.S. Security Partnerships: A Toolkit for Congress,” <https://www.newamerica.org/political-reform/reports/tools-congress-manage-us-security-partnerships/>]

Title 22 authorities fall under State Department auspices, while Title 10 authorities are controlled by the Department of Defense (DoD).26

For each program, this report includes a short description of what it does, the stated purpose of the program, how the program is authorized, which agencies are involved in implementation of the program, and Fiscal Year 2020 (FY20) funding levels.

The Washington Office on Latin America’s (WOLA) Defense Oversight Research Database provides an up-to-date guide on all authorities and programs through which the United States provides assistance to foreign military, police, or paramilitary forces.27

Key Title 22 Security Cooperation and Assistance Programs:

International Military Education and Training (IMET):

Description: IMET provides training and education on a grant basis to students from allied and security partner countries.28 IMET funds training for non-U.S. personnel at U.S. facilities and outside of the United States for professional military education and technical training.29

Purpose: IMET is intended to strengthen partner forces’ capabilities and enhance interoperability for joint operation, enhance mil-mil relations, provide professional military education, increase understanding and communication between the United States and its security partners, and provide training to foreign personnel around human rights and the importance of democratic values such as the military’s role in a civilian-led government.30

Authorization/Implementation: Authorized by Section 541 of the Foreign Assistance Act (FAA) of 1961. The State Department determines which countries will have IMET programs, but programs are implemented by DoD.31

FY20 Funding: $100 million32

International Narcotics and Law Enforcement (INCLE):

Description: INCLE “provides equipment, training and services to foreign countries for counternarcotics and anti-crime efforts,” including law enforcement training and in limited instances, weaponry to provide defensive arms to aircraft used in counternarcotics operations, although a 15-day congressional notification is required in these instances. INCLE funds may also provide economic development assistance.33

Purpose: To support country- and global-level law enforcement programs to counteract transnational crime including money laundering, narcotics trafficking, and terrorism-related issues. INCLE funds support programs like the Partnership for East Africa Counterterrorism and the Trans-Sahara Counterterrorism Partnership.34

Authorization/Implementation: Authorized by section 481 of the FAA of 1961. Overseen by the State Department.

FY20 Funding: $945.35 million35

Foreign Military Financing (FMF) (see Part II for more):

Description: FMF provides other countries with grants and loans to make government-to-government purchases of U.S-made defense articles and defense-related services via the Foreign Military Sales (FMS) program (see Part II). FMF also less frequently funds Direct Commercial Sales (DCS) between other countries and private U.S. companies.36

Purpose: FMF is intended to enhance the military capabilities of security partners; promote coalition efforts, especially in counter-terrorism and enhance interoperability; and support the U.S. industrial base.37

Appropriation/Implementation: Authorized by the Arms Export Control Act, as amended. The State Department determines which countries have an FMF program; FMF is implemented by DoD’s Defense Security Cooperation Agency (DSCA).38

FY20 Funding: $5,370.9 million39

Peacekeeping Operations (PKO):

Description: Supports regional stability operations and multilateral peacekeeping that is not funded through the UN.40

Purpose: In spite of its name, this program is often used to support East African forces conducting counter-terrorism operations, for example against al-Shabaab in Somalia.41

Authorization/Implementation: Authorized under section 551 of the FAA.42

FY20 Funding: $291,435 million

Non-Proliferation, Anti-Terrorism, Demining & Related Programs (NADR):

Description: NADR provides support for U.S. security assistance efforts to police, military, and civilian government actors.

Purpose: NADR provides assistance in four areas: counter-terrorism, nonproliferation, regional stability, and humanitarian assistance. Programs supported by NADR include the Humanitarian Demining Program and the Antiterrorism Assistance Program, which provides CT training to law enforcement agencies in other countries.

Authorization/Implementation: Authorized by section 571 of the FAA;43 overseen by the State Department.44

FY20 Funding: $707.15 million45

## Security Cooperation---Other Neg Violations

### SC---Excludes Cyberspace---1NC

#### DOD doctrine classifies ‘security cooperation’ as distinct from ‘cyberspace operations’

Bilms ’21 [Kevin; January; career Department of Defense civilian serving in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict; War on the Rocks; “What’s in a name? Reimagining irregular warfare activities for competition,” https://warontherocks.com/2021/01/whats-in-a-name-reimagining-irregular-warfare-activities-for-competition]

Current Irregular Warfare Operations and Activities

Both the Irregular Warfare Annex to the National Defense Strategy and the Defense Department’s current directive define irregular warfare as a struggle to influence populations and affect legitimacy. They identify five core missions within irregular warfare: unconventional warfare, stabilization, foreign internal defense, counter-terrorism, and counter-insurgency. These documents also describe six enabling activities for population-focused arenas including military information support operations, cyberspace operations, counter-threat networks, counter-threat finance, civil-military operations, and security cooperation.

### SC---Excludes Hostilities---1NC

#### “Security cooperation” excludes post-hostilities action. The impact to legal precision is Russia War.

Fenell ’11 [Nathan; December 12; International Studies MA Candidate at the University of San Francisco, written after his second deployment to Iraq; the University of San Francisco, “Security Cooperation Poorly Defined,” <https://repository.usfca.edu/cgi/viewcontent.cgi?article=1020&context=thes>]

Background and Need for the Study

The precise use of words by Department of Defense officials is critical to formulating and executing military strategy.11 When developing a plan of action, loosely defined military terms can affect planners’ abilities to properly understand the actual capabilities resident in a proposed course of action.12 In Afghanistan, the misapplication of the military term security cooperation fostered a climate that caused the Department of Defense and State to underestimate the significant role of SC in fostering the diplomatic relationships that contribute to international peace and stability.

As a major in the Marine Corps, I planned and participated in a security cooperation exercise with Estonia. It was important to the United States European combatant commander and the commanding general Estonian Self Defense Force that communication with the media specifically addressed our operation as a security cooperation exercise. Eighteen countries participated in the exercise, to include the United States and Estonia, and sixteen other countries that are part of the North Atlantic Treaty Organization (NATO). However, this exercise, named BALTIC OPERATIONS, was not officially a NATO exercise.

This distinction between security cooperation exercise and NATO exercise may seem like nothing more than semantics. However a misunderstanding of the semantic nuances had potential negative strategic consequences. Estonia shares a border with Russia and former Soviet military forces occupied Estonia prior to the 1991 Singing Revolution. Diplomatic tensions between Estonia and Russia remain tense and Estonia is constantly defending its territorial waters in the Baltic Sea against Russian naval vessels. During the exercise a Russian frigate and a Russian submarine attempted to violate Estonia’s territorial water. In response, Estonia deployed a small portion of its Navy to block the Russian vessels and force a return to internationally recognized neutral waters shared by countries bordering the Baltic Sea. This level of international tension between Estonia and Russia is constant. If the participants of a security cooperation exercise were to describe the event as a NATO exercise, it would be interpreted by Russia as a signal that NATO forces, led by the United States, were rehearsing air, land, and sea strategies in the Baltic Sea that would support an amphibious assault against the Russian city of St. Petersburg. This instance and many others like it demonstrate that the improper use of military terminology can have unintended negative consequences.

According to the authors of a paper written for USAID, the reconstruction strategy in Afghanistan, is often mislabeled as security cooperation, and designed to support the withdraw of United States military forces from Afghanistan.13 This example demonstrates the tendency to confuse Afghan reconstruction with SC. SC is a prehostilities strategy to effectively and peacefully resolve emerging problems prior to the eruption of violence and the need to commit U.S. forces to a contingency operation.14 This is contrasted with reconstruction, a term that describes aid provided during and after military conflict. This contrast highlights the need to protect the integrity of the SC and the importance of identifying operations where SC is confused. Indeed one of the basic assumptions under which I will proceed with this thesis is that SC, properly defined, occupies a critical role in the overall strategy to prevent the United States from entering into armed conflict rather than a strategy employed after hostilities have commenced.

Military doctrine, national strategy, and specialized dictionaries for military professionals and government policy makers, present a precise definition of and specific criteria for the strategic application of security cooperation.15 Yet a review of case studies by organizations like the United States Agency for International Development and the Woodrow Wilson School of Public and International Affairs that focus on Provincial Reconstruction Teams in Afghanistan, demonstrates that the current application of security cooperation is inconsistent with its doctrinal definition.16 Moreover, my professional military experience with the doctrinal application of security cooperation and Provincial Reconstruction Teams provides a first hand account that reinforces the observation that doctrinal definition and contemporary practical application of Security cooperation are inconsistent.

### SC---Excludes Training/Interoperability---1NC

#### Security cooperation excludes ‘training’ and ‘interoperability’---the DoD conducts tose under Operations and Managements funds under EUCOM

Bowne ’18 [Andrew; 2018; Major and Judge Advocate in the United States Air Force, Contract and Fiscal Law Professor, The Judge Advocate General's School, United States Army; Military Law Review, “Defending the New Fulda Gap: Deterring Russian Aggression Against the Baltic States Through Fiscal Legislation, 226 Mil. L. Rev. 147, lexis]

IV. Current U.S. Contributions to NATO

Despite bipartisan criticism of the perceived lack of funding from other NATO members, the United States still recognizes that its leadership in the Alliance is vital to its own national security. 78 There are clear benefits to combined defense in terms of national security, foreign relations, and the economy, 79 placing U.S. funding of NATO at the intersection of foreign and domestic policy. While the President has constitutional authority in defense, as the Commander-in-Chief, and to enter into agreements with foreign states, 80 Congress can affect both defense and foreign affairs through its power of the purse. 81 Accordingly, this section analyzes the reflection of U.S. foreign and defense policies through Congressional authorizations and appropriations that affect the implementation of Operation Atlantic Resolve's lines of operation, particularly in increasing interoperability and improving the defense capacity of the Baltic States. 82

A. Congress's Role in Funding NATO Operations

Congress's power to authorize expenditures through legislation is instrumental in national security and foreign relations, as it determines the amount and purpose for which expenditures are authorized. 83 Because military activities and foreign assistance require expenditures of funds, the United States cannot implement its strategic goals in Eastern Europe without fiscal authority. 84 The constitutionally provided power of the purse therefore places Congress as the cornerstone of the United States' participation in NATO operations. While U.S. funding for deterring Russian aggression is complex and lacks clarity, sources of funding generally fall within three categories: service component funds, the European Reassurance/Deterrence Initiative, and security cooperation.

B. Building Better Allies through Funding Resources

1. Service Operations & Maintenance Funds

As the Unified Combatant Command with an area of responsibility covering Europe and Russia, EUCOM is tasked with managing theater requirements, to include supporting NATO operations and meeting U.S. national security objectives. 85 While EUCOM has authority over the conduct of operations within this region, it is the military services that receive direct funding from Congress through Operations and Maintenance (O&M) funds. 86 Like all Unified Combatant Commands during the budget planning phase, EUCOM is limited to providing inputs to influence the armed services, and sets priorities for funding, but Congress may appropriate different amounts and purposes than requested by the combatant commander. 87

To the extent an expense is necessary, fits within EUCOM's mission, and funds are authorized and appropriated, O&M funds are available for the expenditure, 88 unless the expense is covered by a more specific appropriation. 89 Another caveat is that the expenditure of funds must be for the primary benefit of the United States. 90 These two limitations to the use of service O&M funds obfuscate the analysis of how to fund operations in support of the NATO mission properly. First, it is unclear which agency's funds can be used. Under the Foreign Assistance Act, the Department of State (DoS) is the agency responsible for coordinating all foreign development activities. 91 An exception to the Foreign Assistance Act is when Congress specifically authorizes the Department of Defense (DoD) to obligate defense funding for the benefit of a foreign state, military or population, or if the funding is for "little t" training. 92 Because "little t" training, which protects U.S. forces by promoting safety, familiarization, and interoperability with foreign forces, does not constitute security cooperation, such activities are funded by O&M. However, a second issue arises because most efforts to build NATO ally and partner capacity likely will exceed the parameters of "little t" training and will fall under the umbrella of foreign assistance. Accordingly, funding for such security cooperation programs will come from more specific appropriations, as described below.

### SC---Excludes Troop Withdrawals---1NC

#### “Security cooperation” excludes troop withdrawals.

Fenell ’11 [Nathan; December 12; International Studies MA Candidate at the University of San Francisco, written after his second deployment to Iraq; the University of San Francisco, “Security Cooperation Poorly Defined,” <https://repository.usfca.edu/cgi/viewcontent.cgi?article=1020&context=thes>]

Purpose of the Study

Words have meaning and the unique ideas that are transmitted through the use of military vocabulary demand that the author and the orator communicate with specificity and clarity. In the case of security cooperation, my research indicates that military professionals, government officials, and academics appear to be equally guilty of failing to limit their use of the term to its correct context. Most egregiously, the term is being improperly used as an important element that describes the United States exit strategy from Afghanistan.21 An example of the recent comments made by the Secretary of State as she described the current state of affairs in Washington, D.C. and Afghanistan, that the State Department convened an interagency team, including DOD, USAID, and the NSC and held discussions that resulted in an agreement that included strong commitments on economic/social development, democratic institution-building, human rights, anticorruption, and other important long-term reforms. Mrs. Secretary follows up on this statement by saying; “Ambassador Crocker and General Allen are still working through some of the security cooperation issues with President Karzai”.22 To place these comments into context, the Honorable Mrs. Clinton was incorrectly describing the peace process in Afghanistan and the withdraw of U.S. forces as security cooperation.

Doctrinally, security cooperation is unrelated to a military withdraw from a country at the conclusion of armed conflict.23 I was caught by surprise; therefore, to discover that despite the efforts of the Department of Defense to accurately articulate its professional lexicon via a dictionary of military terms and doctrine, basic concepts and their associated framework of action were being misused. 24 Initially I thought that I was encountering isolated instances of misuse, but further reading led me to believe that the misapplication of this particular term was wide spread.25

### SC---9 Budget Categories---1NC

#### “Security cooperation” currently only fits into 9 categories.

Defense ’21 [Office of the Secretary of Defense; May 2021; “Fiscal Year (FY) 2022 President’s Budget: Justification for Security Cooperation Program and Activity Funding,” https://open.defense.gov/Portals/23/Documents/Security\_Cooperation/Budget\_Justification\_FY2022.pdf]

Title 10, Chapter 16, Section 301 of the U.S. code defines security cooperation as “any program, activity (including an exercise), or interaction of the Department of Defense with the security establishment of a foreign country to achieve a purpose as follows:

• To build and develop allied and friendly security capabilities for self-defense and multinational operations

• To provide the armed forces with access to the foreign country during peacetime or a contingency operation.

• To build relationships that promote specific United States security interests.

The Department has made significant reforms to align strategic guidance with resource allocation; establish an assessment, monitoring, and evaluation (AM&E) program; and create a comprehensive, common picture of the Department’s budget for security cooperation activities as well as related programs that engage foreign partners. This budget display is representative of the Department’s progress to date in achieving security cooperation reform and realizing congressional intent in Title 10, Chapter 16 security cooperation.

Section 381(a) of Title 10, U.S. Code, requires a consolidated budget of security cooperation programs and activities be included annually along with the President’s Budget request to Congress. The consolidated budget display is intended to enhance planning and oversight of security cooperation programs and related activities across the DoD. This fourth annual budget display demonstrates how DoD plans, programs, and budgets for programs and activities to align with the Department’s strategic objectives.

This budget display includes the $6.5 billion requested by the Department for FY 2022 to conduct security cooperation programs and activities. It focuses primarily on the funding requested for programs and activities that will be executed under the authorities in Chapter 16 of Title 10, U.S. Code. It also includes funding requests for non-Chapter 16 programs and activities that include some elements or activities that are consistent with the security cooperation definition, including the Coalition Support Funds, the DoD Cooperative Threat Reduction (CTR) Program, Ukraine Security Assistance Initiative (USAI), Afghanistan Security Forces Fund (ASFF), and the CounterIslamic State of Iraq and Syria (ISIS) Train and Equip Fund (CTEF). This display excludes classified programs, such as programs authorized under Section 127e of Title 10, U.S. Code, “support of special operations to combat terrorism.” The budget display also excludes Drug Interdiction and Counter-Drug activities authorized under Section 284(c) of Title 10, U.S. Code, “Support for counterdrug activities and activities to counter transnational organized crime.”

In identifying the specific funds allocated to security cooperation, the Department focused on costs that could be directly tied to security cooperation or similar activities. Many DoD activities, especially in the Military Services, could be viewed as security cooperation. However, for the purposes of this display, the Department focused on the situations where a security cooperation program is expected to incur an additional cost above and beyond what the Department would already be doing. For example, if U.S. forces are planning to conduct a training event and two observers from a partner nation are expected to attend, the Department would not reflect the costs of that exercise in this budget display. However, if DoD paid for the travel, lodging and subsistence of those observers to support attendance, then those costs would be captured in this display.

Changes from FY 2021 Justification for Security Cooperation Program and Activity Funding book include:

• Realigned the Defense Institute for International Legal Studies (DIILS) and Institute for Security Governance (ISG) from Category 4, Capacity Building, to Category 6, Management, Infrastructure and Workforce development to better align these Program / Activities with the category objectives.

• Realigned Border Security from Category 4, Capacity Building, to Category 3, Support to Operations, to better align with this Program / Activity with the category objectives.

• Added the Regional Defense Fellowship Program (RDFP) to Category 5, Educational and Training Activities. Consistent with the FY 2021 defense appropriations bill, RDFP has been realigned as a standalone program.

• Created Category 9, Cooperative Threat Reduction, and realigned the DoD Cooperative Threat Reduction Program from Category 4, Capacity Building, to the new category to reflect the program’s distinct authorities and mission.

Categories of Security Cooperation Programs and Activities

This budget display groups security cooperation programs and related activities and the respective authorities through which they are executed into nine (9) categories. Categories 1-5 mirror the subchapters in Chapter 16 of Title 10. The budget display also includes Categories 6-9 as follows: requests that fund the reforms to management and oversight inside the Department (Category 6), humanitarian and assistance activities (Category 7), and partner security forces funds for counterterrorism activities and combating insurgencies (Category 8), and cooperative threat reduction efforts aimed at preventing the proliferation of weapons of mass destruction (Category 9).

The nine security cooperation and related activities categories of this display are summarized below:

Category 1: Military to Military Engagements – Security cooperation programs and activities related to the interaction between U.S. military personnel and the national security forces of friendly foreign countries, including the exchange of military personnel, payment of incremental expenses, and bilateral and regional cooperation programs.

Category 2: Training with Foreign Forces – Security cooperation programs and activities related to training with military and non-military security forces of friendly foreign countries, as well as the payment of related training and exercise support.

Category 3: Support to Operations – Security cooperation programs and activities that provide logistic support, supplies, services, specialized training, loan of equipment, and reimbursements to support the conduct of operations in which the U.S. military may or may not be directly participating.

Category 4: Capacity Building – Security cooperation programs and activities that build the capacity of a friendly foreign country’s security forces through the provision of defense articles and services, including institutional capacity building efforts with international partners.

Category 5: Educational and Training Activities – Security cooperation programs and activities related to the participation of foreign personnel in DoD-sponsored education and training programs, including the Regional Centers for Security Studies.

Category 6: Management, Infrastructure, and Workforce Development – Activities that encompass the administration, management, and oversight of security cooperation programs, to include personnel, information technology, facilities, and costs associated with ensuring a qualified security cooperation workforce, such as the establishment of a certification program.

Category 7: Humanitarian Assistance Activities – Security cooperation programs and activities associated with humanitarian and/or civic assistance for friendly foreign countries.

Category 8: Partner Security Forces Funds – Security cooperation programs and activities associated with the professionalization, cultivation, and sustainment of partner security forces in Afghanistan to counter local insurgency and transnational terror organizations, as well as in Iraq, and Syria with a focus on preventing the reemergence of ISIS.

Category 9: Cooperative Threat Reduction Activities – Title 50 activities focused on working with partner civilian and military departments to reduce the threat of weapons of mass destruction (WMD) and WMD-related materials to U.S. national interests.

### SC---AT: 9 Budget Categories---2AC

#### Requiring the aff to fit into the nine categories is illogical. They just added a new category last year!

Defense ’21 [Office of the Secretary of Defense; May 2021; “Fiscal Year (FY) 2022 President’s Budget: Justification for Security Cooperation Program and Activity Funding,” <https://open.defense.gov/Portals/23/Documents/Security_Cooperation/Budget_Justification_FY2022.pdf>]

Changes from FY 2021 Justification for Security Cooperation Program and Activity Funding book include:

• Realigned the Defense Institute for International Legal Studies (DIILS) and Institute for Security Governance (ISG) from Category 4, Capacity Building, to Category 6, Management, Infrastructure and Workforce development to better align these Program / Activities with the category objectives.

• Realigned Border Security from Category 4, Capacity Building, to Category 3, Support to Operations, to better align with this Program / Activity with the category objectives.

• Added the Regional Defense Fellowship Program (RDFP) to Category 5, Educational and Training Activities. Consistent with the FY 2021 defense appropriations bill, RDFP has been realigned as a standalone program.

• Created Category 9, Cooperative Threat Reduction, and realigned the DoD Cooperative Threat Reduction Program from Category 4, Capacity Building, to the new category to reflect the program’s distinct authorities and mission.

## Security Cooperation---Aff

### SC---Conditional---2AC

#### Congress can reallocate authority and funding for SC broadly, especially for emerging tech operations with allies

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]

Congressional Role

Congress provides the authority and funding for SC programs. Title 10 SC activities fall under the jurisdiction of the armed services committees, while Title 22 (DOS) SA activities are under the jurisdiction of the Senate Foreign Relations and House Foreign Affairs committees. Although the armed services committees are responsible for the authorizing legislation for Title 10 SC programs, both committees exercise oversight of SC activities and the management of SC policy, including the level of coordination between DOD and DOS. Funding for Title 10 SC programs and activities is provided through annual appropriations bills, which originates in the appropriations committees, specifically the defense subcommittees.

Primarily (but not solely) through these six committees,

Congress plays critical roles in the design and oversight of SC programs and in ensuring that SC activities are aligned with and meeting U.S. national security and foreign policy objectives. Pursuant to statutory authorities, the executive branch must notify relevant committees on a regular basis about some, but not all, SC activities. Congress can exercise oversight roles in numerous ways, including determining how the executive branch makes decisions for the export of military and dual-use items, using annual authorizing legislation to establish temporary authorities or modify the U.S. Code on an enduring basis, reviewing proposed arms transfers and planned SC/SA activities and funding obligations, mandating reports, and holding relevant hearings. The Senate also influences SC through its advice and consent to the ratification of relevant treaties. DOD’s FY2021 SC Budget Request,

Authorizations, and Appropriations

The final FY2021 NDAA (P.L. 116-283) mostly maintained funding levels from DSCA’s FY2021 SC budget request, although some provisions identify SC priority areas. In establishing the Pacific Deterrence Initiative (PDI), the NDAA requires DOD activities, including SC, to prioritize the Indo-Pacific region. The creation of PDI also indicates that the Indo-Pacific will remain a priority for years to come. Other NDAA provisions include a requirement for DOD to identify ways to enhance SC in African countries, as well as amplify SC requirements from the Women, Peace, and Security Act of 2017. The bill also amended DOD’s main train and equip program (10 U.S.C. §333) to add “air domain awareness operations” and “cyberspace security and defensive cyberspace operations” as authorized areas for support.

The final FY2021 Defense Appropriations bill (P.L. 116- 260) increased funds for DSCA’s base budget and slightly decreased its Overseas Contingency Operations budget. The bill provides significant increases for SC in both Africa Command’s and Southern Command’s areas of responsibility (funds for both have declined since FY2017) and cuts funding to both CTEF and ASFF (see Table 1).

#### Congress can increase conditional security cooperation

Stark ’20 [Alexandra; Oct 26; PhD from the government department at Georgetown University, a research fellow at the Middle East Initiative of the Harvard Kennedy School’s Belfer Center for Science and International Affairs, and Minerva/Jennings Randolph Peace Scholar at the United States Institute of Peace; New America, “Managing U.S. Security Partnerships: A Toolkit for Congress,” <https://www.newamerica.org/political-reform/reports/tools-congress-manage-us-security-partnerships/>]

2. Use the Power of the Purse

Congress can use the power of the purse to place restrictions on the accounts it funds and may fund certain accounts while defunding others.

Place Conditions and/or Restrictions on Security Assistance: Congress can restrict or place conditions on how U.S. security assistance is used by allies and security partners. Such conditions can discourage allies or security partners from pursuing certain policies.

Defund the Authorizations for the Use of Force (AUMFs): Congress has the discretion to appropriate funding for deployments related to AUMFs. Congress has appropriated more than $2 trillion in funding for operations in Afghanistan and Iraq as well as other operations related to the Global War on Terror (GWOT) through emergency supplemental bills since 9/11, namely the Overseas Contingency Operations (OCO) fund, which is operated jointly by the DoD and State Department on top of their annually appropriated base budgets.9

Increase Funding for End-Use Monitoring Programs: Recipients of U.S. defense articles and services must agree to use them only for their intended purposes, to not transfer the title without the written consent of the U.S. government, to provide the same degree of physical security to the articles as the U.S. government does, and to allow U.S. officials to verify compliance with these terms. Congress appropriates funding for end-use monitoring programs to ensure that U.S. defense articles are used according to the terms of the transfer agreement. Congress can increase funding for end-use monitoring programs to monitor whether weapons are used for agreed-upon purposes or are transferred to unauthorized actors.

Condition Future Arms Sales on Past Behavior: Congress could informally commit to condition future arms sales on the past behavior of recipient countries. For example, Congress could block sales to regimes that have been credibly found to commit violations of international humanitarian law or of end-use agreements. A robust end-use monitoring system could also expose violations of transfer agreements, providing Congress with leverage to hold security partners to the terms of end-use monitoring agreements and to potentially limit or block future arms sales.

Shift Focus from Equipment to Training: While building partner capacity is a primary goal of U.S. security assistance, U.S. policy tends to emphasize arms sales and the provision of materiel over training. Training may be relatively more effective in professionalizing partner militaries and ensuring that they actually have the technical capability to use the weapons they acquire effectively, as well as discouraging human rights violations. In order to shift emphasis towards training, Congress can appropriate more funding to International Military Education and Training (IMET) rather than Foreign Military Financing (FMF), and can include line-items in appropriations bills requiring assistance to be non-lethal or focused on training.

### SC---Includes Security Assistance---2AC

#### Security coop entails transferring defense articles, mil-to-mil exercises, military education, and building partner capacity. Both DOD-implemented Title 22 and DOD-administered Title 10 programs are topical.

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]

Security Cooperation (SC) Overview

The Department of Defense (DOD) uses the term security cooperation (SC) to refer broadly to DOD interactions with foreign security establishments. SC activities include

• the transfer of defense articles and services;

• military-to-military exercises;

• military education, training, and advising; and

• capacity building of partner security forces.

SC programs are intended to encourage and enable partner nations (PNs) to work with the United States to achieve strategic objectives. They are considered a key tool for achieving U.S. national security and foreign policy objectives. These activities are executed through both DOD-administered SC programs (authorized under Title 10, U.S.C.) and DOD-implemented State Department (DOS) security assistance (SA) programs (authorized under Title 22, U.S.C). Beyond grant-based programs, SC encompasses the Foreign Military Sales program and enables U.S. and PN collaboration on defense articles. The following sections focus on DOD “Title 10” activities.

SC: Policy and Objectives

SC activities aim to achieve particular objectives in support of U.S. national security and defense strategies. Specifically, SC may build defense relationships that promote U.S. security interests, enhance military capabilities of U.S. allies and partners, and provide the United States with access to PNs. Under the overarching goal of furthering U.S. national security and foreign policy interests, SC emphasizes partnerships, aiming to be mutually beneficial for the United States and its partners. SC activities aim to develop and strengthen a PN’s ability to provide internal security, contribute to regional security efforts, combat shared threats, and increase military interoperability with the United States.

The 2018 National Defense Strategy (NDS) signaled the Trump Administration’s intention to shift SC activities from nearly two decades of prioritizing counterterrorism toward “great power competition” (GPC) with Russia and China. The shift raised questions as to how SC should be realigned to meet this objective and what the implications could be for scaling down counterterrorism-focused SC activities in Africa and the Middle East, especially as Russia and China increase their influence. Some DOD officials and defense analysts have suggested that rather than a shift, counterterrorism, as well as irregular warfare, should remain priorities within GPC. The Biden Administration has yet to release a new NDS; however, its Interim National Security Strategic Guidance broadly identifies authoritarianism and strategic competition as priority threats that require coordination and cooperation with allies and partners.

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.

Table

Description automatically generated with low confidence

Table

Description automatically generated

Title 10 SC Reforms from the FY2017 NDAA

The post-9/11 period saw the rapid and piecemeal expansion of DOD SC activities, mainly as temporary authorities that required annual renewal in the National Defense Authorization Act (NDAA). The FY2017 NDAA (P.L. 114-328) consolidated and codified existing Title 10 SC authorities into 10 U.S.C. §§301-386. Other provisions aimed to make improvements to the SC programs and themselves, as well as improvements in the management and oversight of those programs. Key reforms from the FY2017 NDAA included requirements for the following:

• A consolidated DOD budget request for Title 10 SC programs and activities (10 U.S.C. §381); the first was released for FY2019.

• Harmonized congressional notification requirements for most DOD train and equip programs (10 U.S.C. §333).

• Institutional capacity building programs to strengthen partner defense institutions (10 U.S.C. §332).

• A DOD SC Workforce Development Program to manage a professional workforce in support of SC programs and activities (10 U.S.C. §384).

• A program of assessment, monitoring, and evaluation (AM&E) to be informed and supported by strategic evaluations on initial PN assessments, monitoring of implementation, and the efficiency and effectiveness of SC programs and activities (10 U.S.C. §383).

#### Their ev is outdated---recent NDAA’s redefined security cooperation as including Title 10 programs

Maginnis ’21 [Robert and Michael Prater; September 2; contractor with Sigmatech Inc. supporting DASA (DE&C) as a global strategist, retired U.S. Army officer who recently completed 18 years with HQDA G-3/5/7 working security cooperation policy and training, M.S. in management science from the Naval Postgraduate School, B.S. in engineering from West Point; principal adviser to the DASA (DE&C) for global security assistance and armaments cooperation and brings to the position 17 years of defense-related experience, primary interface with the Army staff regarding security assistance and armaments cooperation and contributes to Army strategies, campaign plans, policies and operational orders; U.S. Army Acquisition Support Center, “Security Cooperation Refresh,” <https://asc.army.mil/web/news-security-cooperation-refresh>]

Until 2018, a significant shortfall in the Army’s international engagement strategy was a self-imposed division of labor between conventional forces’ exercise-centric security cooperation and the materiel-focused security assistance enterprise, which resulted in less than optimal outcomes. Congress helped the U.S. Army rethink this synergy of effort by issuing new guidance via the Fiscal Year 2017 National Defense Authorization Act, which promises to result in better designed capability that meets U.S. and partner shared security goals.

DIVISION OF LABOR

The Army’s operational forces conducted security cooperation through troop exercises, information sharing and key leader engagements for decades. Meanwhile, the Army security assistance enterprise worked out of the limelight, remaining mostly materiel-focused and tethered to the State Department’s 22 U.S. Code, Subchapter II—Foreign Military Sales authorizations. The bifurcated foreign engagement activities infrequently overlapped, missing the Army’s true potential for helping prepare foreign partners to defend themselves as well as strengthen U.S. Army units for coalition operations and reach the aspirational outcome of robust interoperability—a stretch goal for Army commanders and our best foreign partners.

The Army’s division of security cooperation labor is the result of a decision made decades ago to split into two international engagement entities previously housed under the deputy undersecretary of the Army for international affairs.

The first entity in this division of labor is the Army secretariat represented by the deputy assistant secretary of the Army for defense export and cooperation (DASA (DE&C)) under the authority of the assistant secretary of the Army for acquisition, logistics and technology. DASA (DE&C) oversees the transfer of materiel, engineering activities and related training for foreign partners such as servicing foreign military sales cases and armaments cooperation agreements to leverage foreign technologies and capabilities that support Army readiness, modernization and interoperability goals.

The balance of international engagement activities was assumed by the Army’s chief of operations, the assistant chief of staff G-3/5/7, which oversees the day-to-day maneuver-related engagements with foreign partners. That partition of effort can result in conflicting messages to foreign partners and less than optimal outcomes for the Army’s contribution to DOD’s strategic goals of building partner capabilities and preparing for global coalition operations.

REDEFINING EFFORTS

Fortunately, those too often disjointed outcomes are now collapsing into a far more synergistic endeavor thanks to the National Defense Authorization Act of 2017, and in particular the codification of Title 10, Chapter 16, Security Cooperation.

Congress redefined nearly everything DOD does with a foreign partner as “security cooperation.” That definition includes not just exercises and information sharing—which is the traditional forte of operational forces—but the Army’s support of State Department-approved foreign military sales cases, direct commercial sales, the training provided to foreign partners at our schoolhouses and other programs as defined by Title 22 Security Assistance, a State Department authority executed by DOD.

#### Security coop includes DOD-administered security assistance

Rand ’15 [Dafna and Stephen Tankel; August; former Deputy Director of Studies and the inaugural Leon E. Panetta Fellow at CNAS; Assistant Professor in the School of International Service at American University, and an adjunct fellow in the Asia-Pacific Security program at CNAS; “SECURITY COOPERATION & ASSISTANCE: Rethinking the Return on Investment,” https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report\_Security-Cooperation\_FINAL.pdf]

PART II: DEFINING SECURITY ASSISTANCE AND COOPERATION

Security assistance and cooperation activities

encompass a range of different U.S. efforts in disparate countries. These activities differ in terms of how they are deployed and why, what types of local partners participate, how they are authorized legally and legislatively, their geographic scope, who is responsible for their budgets and implementation, and their relative importance to critical U.S. national security goals. Over the past decade, Congress has approved myriad new authorities, such as Building Capacity of Foreign Security Forces (Section 2282) and the Global Security Contingency Fund (GSCF), without a consonant overall reorganization or strategy regarding how to deploy the growing toolkit. As a result, there is some confusion about the purposes and types of programs that exist.

• Security assistance refers to programs through which the United States provides defense articles, military training, defense institution-building efforts, and other defense-related services by grant, loan, credit, cash sales, or lease, in furtherance of U.S. policies and objectives. Security assistance programs include Foreign Military Financing (FMF), Foreign Military Sales (FMS), International Military Education and Training (IMET), Global Peace Operations Initiative, and the Excess Defense Articles (EDA) program. The State Department has overall responsibility for many of these programs, including FMF, FMS, and IMET, but they are primarily implemented by the Defense Security Cooperation Agency (DSCA) at DoD. DoD has responsibility for other security assistance programs.

• Security cooperation encompasses all DoD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a host nation. (Access is the U.S. military’s term for the willingness of a host nation to allow U.S. forces on its ground and in its airspace.6 ) Security cooperation includes DoD-administered security assistance. Additional security cooperation programs include joint military exercises such as Operation Bright Star, normally held every two years with Egypt; training, counterproliferation, and nonproliferation programs; defense institution-building; defense and military contacts; information-sharing and intelligence cooperation; and logistics support. Security cooperation programs are budgeted and implemented directly by DoD.

• Security sector assistance, as defined by Presidential Policy Directive 23, refers to policies, programs, and activities used to engage with foreign partners and help shape their policies and actions in the security sector – both civilian and military institutions. PPD 23 outlined the need for a coordinated effort synchronizing programs across U.S. government agencies – including State, DoD, the Department of Justice (DOJ), and the U.S. Agency for International Development (USAID) – to help foreign partners build and sustain the capacity and the effectiveness of civilian and military institutions to provide security, safety, and justice for the civilian population.7 Many of these programs are significant; for example, the Obama administration included over $2.1 billion in its Fiscal Year (FY) 2016 budget request for two foreign assistance funds that primarily work with civilian security institutions: the international narcotics control and law enforcement (INCLE) and the nonproliferation, anti-terrorism, demining, and related (NADR) funds.8 (To avoid confusion, unless referring to it specifically, this report nests security sector assistance within the broader rubric of security assistance and cooperation.)

#### Security cooperation includes both Title 10 and Title 22 programs

Kelly ’10 [Terrence K. Kelly, Jefferson P. Marquis, Cathryn Quantic Thurston, Jennifer D. P. Moroney, Charlotte Lynch; 2010; RAND Institute; research described in this report was sponsored by the United States Army under Contract No. W748H-06-C-0001, “Security cooperation organizations in the country team: options for success,” ISBN 978-0-8330-4911-7]

Security assistance, as it is currently in law and practice, reflects an approach that is adequate in a stable environment in which efforts can be planned, resourced, and executed without major changes, but not sufficiently agile for a world in which challenges are more dynamic and flexibility is essential for success. To address this issue, the U.S. Army asked RAND to do a "quick turn" assessment of security assistance and propose alternatives for improving it. This technical report is the result of that project.

This research considers the missions and structure of security assistance organizations in U.S. Missions around the world and presents three options for improving the functionality of security assistance organizations based on best practices and what is known about the tasks they are likely to take on. This project was undertaken as a quick-turnaround study for the Army's Office of the Deputy Chief of Staff for Operations and Plans. The research took place from February to April 2008, with some adjustments based on input from Headquarters, Department of the Army, and from reviewers after this period ended.

Summary

The United States conducts a wide range of security cooperation missions and initiatives that can serve as key enablers of U.S. foreign policy efforts to assist and influence other countries. For a relatively small investment, security cooperation programs can play an important role by shaping the security environment and laying the groundwork for future stability operations with allies and partners.

Security cooperation, in the form of noncombat military-to-military activities, includes "normal" peacetime activities, such as building the long-term institutional and operational capabilities and capacity of key partners and allies, establishing and deepening relationships between the United States and partner militaries, and securing access to critical areas overseas. Security cooperation also can include conducting quasi-operational efforts, such as helping U.S. partners and allies manage their own internal defense.

However, current national security challenges both create significant demands for U.S. security cooperation programs and deplete the resources needed to carry out these missions. The wars in Iraq and Afghanistan are occupying the regular, reserve, National Guard, and Special Forces trainers and advisors who would normally be called on to train and advise mili-tary counterparts. Furthermore, U.S. allies, who often complement the efforts of U.S. advisors and trainers, are also stretched thin by their own deployments to Iraq and Afghanistan.

In an effort to find ways to improve security cooperation planning, coordination, and execution, the U.S. Army's Office of the Deputy Chief of Staff for Operations and Plans asked RAND Arroyo Center to conduct an assessment of key facets of U.S. security cooperation—specifically, the missions, capabilities, and structure needed in the security assistance organizations (SAOs)2 that coordinate the military aspects of U.S. foreign relations, including security cooperation activities, at U.S. Missions around the world.

In its assessment, the RAND research team identified three levels of players that plan, coordi-nate, execute, and oversee U.S. security cooperation efforts. However, a number of challenges exist at each level that can inhibit the effectiveness of SAO efforts.

Washington, D.C., Level

At the federal government level in Washington, D.C., anywhere from thousands to billions of dollars are allocated for security cooperation efforts in a given country through various pro-grams. Executive Branch agencies, particularly the departments of Defense and State, work together to ensure that funds are allocated according to the wishes of Congress and the Presi-dent. At the same time, Congress plays a pivotal role in these processes through its annual authorizations and appropriations bills, as well as its oversight and approval of the statutory framework that governs security cooperation.

At this level, two main funding authorities govern security cooperation:

• Title 22 funds are appropriated to the State Department, which often transfers them to DoD, which in turn manages and executes most security assistance programs. Title 22 includes Foreign Military Sales programs. Title 22 is less flexible in some ways, mainly because Congress authorizes and appropriates these funds on a by-country and by- program basis, and requires congressional notification and permission to move funds from one effort to another.

• Title 10 funds are appropriated to DoD and are intended for operations and maintenance of the U.S. military. These funds are often used to fund international participation in U.S. joint exercises, military personnel exchanges, or military-to-military contacts as a way to enhance the relationships between partner militaries and U.S. forces.

Because of the differences in funding authorities for Title 10 and Title 22, there is a general separation between the two, resulting in distinct organizations and cultures and leading to stovepiped approaches to working with foreign countries.

#### SC entails all DOD interactions with foreign defense establishments---it’s inclusive of security assistance

Tankel ’18 [Stephen; Nov 20; associate professor at American University, an adjunct senior fellow at the Center for a New America Security, a senior editor and War on the Rocks, and the author of With Us and Against Us: How America’s Partners Help and Hinder the War on Terror; Policy Roundtable: The Pros and Cons of Security Assistance, “Introduction: The Future of Security Assistance,” <https://tnsr.org/roundtable/policy-roundtable-the-pros-and-cons-of-security-assistance/>]

Security Assistance and Cooperation: A Brief Overview

Security cooperation and security assistance are terms often used without always being defined — or sometimes even understood — by the people writing about them. Without getting too in the weeds, it’s helpful to briefly describe these concepts and delineate where they come from.

Security assistance refers to programs through which the United States provides arms and other defense materials, military training, defense institution-building efforts, and other defense-related services. The State Department has overall responsibility for many of the largest and longest-standing of these programs, which fall under Title 22 authority, including foreign military financing, foreign military sales, and international military education and training. However, it is the Department of Defense that actually implements many of them. It also administers the Section 333 authority, which consolidated many of the Title 10 capacity-building authorities created since 9/11 into one.

Because of its focus on allied and partner militaries, security assistance is largely synonymous with military assistance. Indeed, the two are often used interchangeably. However, the United States also provides security sector assistance to civilian institutions through programs such as the International Narcotics Control and Law Enforcement.3 For our purposes, it is helpful to nest security sector assistance within the broader rubric of security assistance.

Security cooperation encompasses all Department of Defense interactions with foreign defense establishments. This includes all Defense Department-administered security assistance, as well as joint military exercises, defense institution-building, defense and military contacts, information-sharing and intelligence cooperation, and logistics support. The United States currently engages in security cooperation with 224 countries and international organizations around the world.4

The United States spends billions on security assistance and cooperation to achieve various objectives. The most obvious goal is to build the capacity of partners’ military and police forces, as well as their defense and law enforcement institutions so they can confront shared security threats and contribute to international missions. Many of the new security assistance and cooperation authorities created after 9/11 have focused on capacity building specifically for counterterrorism purposes. Capacity building and joint exercises also increase the interoperability of partner forces with the U.S. military. Although capacity building generally focuses on operational and tactical capabilities, it also may (and should) include professionalization of partner forces and institutions.

Another aim is to build or maintain relationships with partner countries in order to secure access — to bases or transit routes — and increase U.S. influence with the host nation government. That influence may be used to yield specific outcomes, such as encouraging recipients to buy arms from the United States as opposed to a competitor or to contribute to an international coalition. In other cases, the purposes of gaining influence are fuzzier, and may include balancing against a regional competitor, or simply generating goodwill. Critically, whether for access or influence, security assistance and cooperation are being used as incentives, which may lead to them being deployed in ways that are inconsistent with capacity-building needs in a given country.

### SC---Includes JCS Categories---2AC

#### “Security cooperation” includes at least these categories.

JCS ’17 [Joint Chiefs of Staff; May 23; publishing with the Army, Marine Corp, Air Force, Navy, and Coast Guard; Security Cooperation, Joint Publication 3-20, “Appendix A: Security Cooperation: Related Programs and Authorities,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf]

Security Cooperation Categories with Related Programs and Authorities

|  |  |
| --- | --- |
| Security Cooperation Category | Related Programs and Authorities |
| Military-to-Military Contacts | Title 10, USC, Section 312 African Partnership Station (Navy) Southern Partnership Station (Navy) African Partnership Flight (Air Force) American, British, Canadian, Australian, and New Zealand Armies' Program (US Army) |
| Personnel Exchanges | Title 10, USC, Section 311 Military Personnel Exchange Program Defense Personnel Exchange Program |
| Combined Exercises and Training | Title 10, USC, Sections 321-322 Joint Combined Exchange Training Combatant Commanders Exercise and Engagement Training Transformation (OSD P&R) |
| Train-and-Equip/Provision of Defense Articles | Title 10, USC, Section 333 Foreign Military Financing Program (FMF; Title 22, USC, Sections 2763-4) Foreign Military Sales Peacekeeping Operations (Foreign Assistance Act, Section 2348) |
| Defense Institution Building | Title 10, USC, Section 332 Defense Institution Reform Initiative Wales Initiative Fund Ministry of Defense Advisors Defense Institute for International Legal Studies |
| Operational Support | Title 10, USC, Section 331 Acquisition and Cross-Servicing Agreements Coalition Support Fund Coalition Readiness Support Program Personnel Recovery |
| Education | International Military Education and Training (IMET; Title 22, USC, Section 2347) Combatting Terrorism Fellowship Program (Title 10, USC, Section 345) Regional Centers for Security Studies Western Hemisphere Institute for Security Cooperation |
| International Armaments Cooperation | Acquisition and Cross-Servicing Agreements Engineer and Scientist Exchange Program Information Exchange Program Test and Evaluation Program |
| Humanitarian Assistance and Disaster Relief | Humanitarian and Civic Assistance (Title 10, USC, Section 401) Overseas Humanitarian, Disaster, and Civic Aid (Title 10, USC, Sections 401 and 2561) Continuing Promise Commanders Emergency Response Program (Title 10, USC, Section 2333) Defense Health Programs |

Legend FMF foreign military financing OSD Office of the Secretary of Defense P&R Personnel and Readiness USC United States Code

Figure A-1. Security Cooperation Categories with Related Programs and Authorities

### SC---Includes Title 22---2AC

#### NATO cooperation over emerging tech can be either Title 10 or Title 22---and even if the status quo authority is confusing, the plan can clarify it

Bowne ’18 [Andrew; 2018; Major and Judge Advocate in the United States Air Force, Contract and Fiscal Law Professor, The Judge Advocate General's School, United States Army; Military Law Review, “Defending the New Fulda Gap: Deterring Russian Aggression Against the Baltic States Through Fiscal Legislation, 226 Mil. L. Rev. 147, lexis]

However, funding non-Article 5 activities contingent upon the demonstrated commitment to defense spending and collective security can promote NATO member spending and influence increased defense spending across the Alliance. 208 Such conditions would demonstrate the prioritization of collective defense. Conditioning foreign assistance on matters unrelated to defense capabilities can encourage allies to increase their own defense spending in order to maintain or improve their status with the United States. While maintaining the paramount importance of deterrence strategy through collective defense in NATO, the United States should tie some of its foreign assistance spending in Europe for non-Article 5 activities to a country's defense spending. Examples of such activities include counterterrorism training, refugee support, or even trade incentives.

Congress already places conditions on the appropriation of authorized funds on foreign assistance; however, it has not utilized this powerful foreign policy tool to influence NATO member defense spending. When drafting future conditional authorizations, Congress should look to its own example in the FY17 NDAA, for its specific and technical conditions imposed on Ukraine in the Extension and Enhancement of Ukraine Security Assistance Initiative. 209 While $ 350 million was authorized to be appropriated in Fiscal Year 2017, Congress made available not more than $ 175 million in funds to be used for the authorized purposes. The Secretary of Defense, in coordination with the Secretary of State, certified that Ukraine "ha[d] taken substantial actions to make defense institutional reforms, in such areas as civilian control of the military"; increased transparency and accountability in defense procurement; improved transparency to decrease corruption; and sustained improvements of combat capability, among other requirements. 210 By limiting the amount of assistance, and placing measurable requirements on the beneficiary as a condition to receiving a portion of the funding, Congress is able to maintain some control over the purpose and amount of spending that, absent such conditions, are within the exclusive purview of the recipient.

Congress can use similar conditions on future authorizations towards NATO members to influence the amount and purpose of ally defense expenditures. One possibility is to condition some or all Title 10 and Title 22 funding going to each NATO member on their certification, through its annual reporting requirements to the NATO Secretary General, that they have increased their defense spending, or met both defense spending and spending on military equipment targets. Absent certification, the Secretary of Defense can waive the conditions based on his determination that such waiver is in the best interest of the national security of the United States. 211 Another possibility is to focus conditions on the NATO members' commitment to improving combat capability through its spending on research and development or even buying specific weapon systems that promote interoperability with other members of the Alliance, such as cyber defense or intelligence, reconnaissance, and surveillance platforms that are important in countering Russia's hybrid warfare capabilities.

Conditional authorizations for funding foreign aid recognize the reality that there are many other issues, both internal and external, impacting NATO members. The refugee crisis, incidents of terrorism, and nationalism erode the foundations of the European Union. This could lead to decreased military spending and lack of political will to spend precious resources to come to the aid of another NATO member, placing the principles of Article 5, and indeed the very purpose of the Alliance, in question. 212 Fairly leveraging those threats is a prudent course of action that Congress can take to offer support to U.S. allies, albeit with strings attached, in order to refocus NATO on Article 5 deterrence and boost defense spending. Certain NATO members may see less of a need to meet the NATO defense spending targets, particularly those in the south or the west that have less to fear from Russian aggression than the Baltic States or Poland. Those members would face receiving little to no support from the United States in their respective efforts to manage an influx of refugees from the Syrian conflict or train counterterrorism security forces. 213 By using a carrot to entice additional defense spending throughout the Alliance, Congress can reinforce a diplomatic truism: that supporting causes, such as the defense of the Baltic States' sovereignty from Russian aggression will earn goodwill from the rest of the Alliance--or more simply, supporting NATO results in NATO support. 214

In the FY17 NDAA, Congress hinted that it may consider individual NATO member contributions in future foreign assistance authorizations. It decided against expressing the sense of Congress that NATO allies' investments in developing and employing security capabilities should "meet or exceed U.S. efforts in this regard." Instead, Congress directed the Secretary of Defense to present to the armed services and foreign relations committees an accounting of European investment in security capabilities and efforts to contribute to global security outcomes. 215 This requirement, along with the reforms to the security cooperation framework that also require country-specific reporting, 216 indicates Congress may consider implementing conditional funding for NATO members, as they did with Ukraine.

Conditional spending provisions from Congress could also create secondary effects that positively impact the amount of defense spending throughout NATO. It is reasonably foreseeable that the European community could exert its own diplomatic pressure on an ally failing to meet the Wales Summit targets, especially if the loss of U.S. dollars consequently causes a state to struggle to contain their non-Article 5 security threats within their borders. This would serve as a secondary line of influence towards increasing defense spending. For example, if the Czech Republic, a NATO member that consistently spends less than one percent of its GDP on its defense, 217 were to lose the millions of dollars it receives from the United States in foreign assistance, 218 and fail to effectively manage internal security threats, neighboring NATO members, such as Germany or Poland, may exert their own diplomatic pressures on the Czech Republic to increase defense spending.

The United States' national security interest is better served when its NATO allies focus on discrete capabilities to defend and deter Russian aggression than if it were to encourage each of the Baltic States to be independently capable of defending against Russia. Given their size and resources, it is impossible to expect any of the Baltic States to match the strength of the Russian forces aligned on their eastern borders on their own. By influencing their defense spending, Congress can better ensure that the Baltic States' forces provide complementary and integrated capabilities, rather than incompatible or duplicative ones. 219 By avoiding the duplication of systems and capabilities between multiple allies, limited resources are better managed. Thoughtfully crafted conditions on security cooperation authorities can also leverage existing capabilities, such as encouraging Estonia to build upon their already sophisticated cyber defense capabilities. 220[220]In 2007, Estonia suffered weeks of cyberattacks from Russia, directed at Estonian government, businesses, and media outlets. Benjamin Oreskes, Why Trump Makes this Small Country so Nervous, POLITICO MAG. (Dec. 10, 2016), http://www.politico.com/magazine/story/2016/12/trump-russia-worries-estonia-214511. As a result, Estonia focused considerable efforts towards cyber defense and is on the cutting edge of cyber security.Id. Tallinn is also the host of its own brain-child, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), dedicated to enhancing the capability, cooperation, and information sharing among NATO, NATO nations, and partners in cyber defense. NATO, CCDCOE HISTORY, https://ccdcoe.org/about-us/ (last visited Feb. 12, 2019)[End Footnote 220] Such influence will improve interoperability as Congress can ensure strategic oversight and leadership remains within the purview of the DoD.

Carefully drafting funding authorizations to maximize U.S. influence in improving NATO's defense capability, through conditional foreign aid and other economic incentives, will encourage defense spending and strengthen individual NATO member ties to the United States. 221 The resulting increase in ownership of collective security by the European contingent of NATO should improve individual defense capabilities. However, to create a meaningful deterrent to Russia and effectively counter its A2/AD capabilities in Eastern Europe, the whole of the Alliance must be greater than the sum of its parts. By focusing on improving NATO member forces, networks, and weapon systems, Congress can positively influence interoperability within NATO as well as ensure that U.S. dollars spent on defending NATO allies are effective.

### SC---AT: Excludes Cyber---2AC

#### Security coop is extremely broad---cyber coop can utilize Cyber Command strategy and apply it to allied engagement

Bilms ’21 [Kevin; January; career Department of Defense civilian serving in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict; War on the Rocks; “What’s in a name? Reimagining irregular warfare activities for competition,” https://warontherocks.com/2021/01/whats-in-a-name-reimagining-irregular-warfare-activities-for-competition]

Merge “Civil-Military Operations” and “Security Cooperation” Into “Security Partner Engagement”

Civil-military operations and security cooperation are similar, but each term contains ambiguity that prevents non-practitioners from fully understanding how they fit in competition. For example, “civil-military operations” risks confusion with “civil-military relations,” the study of the dynamic between the military and civil society writ large. As a term, “security cooperation” is broad enough to encompass virtually anything involving a partner.

Both activities specifically emphasize the use of military forces to establish, maintain, influence, and leverage security relationships through increased defense interactions. Recent history exemplified the importance of non-standard (i.e., non-military) security partners to consolidate strategic gains, and the ability to manage complex and non-traditional security relationships could yield even greater impact in great-power competition. Concerted security engagements before conflict help align U.S. efforts with allies and partners, provide invaluable access and placement in event of crisis, and facilitate U.S. campaign and contingency plans. Both conventional forces and special operators are capable of engaging partners and allies to not only increase interoperability, but also enhance U.S. influence, as a low-cost contribution in competition below armed conflict.

“Security partner engagement” acknowledges the importance of security partnerships and ensuring that regular engagements will secure U.S. influence and preserve the United States as the preferred partner of choice. This terminology adapts U.S. Cyber Command’s concept of “persistent engagement,” where regular engagement helps to get ahead of problems and forestall opponents’ abilities to gain advantage. Applying this logic to civil-military security engagements acknowledges that the influence and advantages afforded by a deep network of security partners are neither predetermined nor indefinite, and require concerted effort to deter opponents that seek to make headway or generate fissures among partners and allies. Reshaping “security partner engagement” in this fashion could account for one way that the department operationalizes its Guidance for Development of Alliances and Partnerships, which looks to maintain and sustain this asymmetric advantage in all stages of competition.

### SC---AT: Excludes Training/Interoperability---2AC

#### Training and exercise programs are literally security coop

Fraser ’15 [Douglas; October 21; General (Retired), LLC, Former Commander of United States Southern Command; Statement of General Douglas M. Fraser before the House Armed Service Committee on Security Cooperation, https://www.hsdl.org/?view&did=789068]

Close Relationship Between Security Cooperation and Security Assistance Mr. Chairman, while this hearing is focused on security cooperation, from my experience, I think it is important to acknowledge the close relationship between Department of Defense security cooperation programs and Department of State security assistance programs. During my time in U.S. Pacific Command and U.S. Southern Command, both commands worked closely with the Department of State and the respective U.S. Embassies to coordinate security cooperation and security assistance programs. Training and exercise programs conducted through security cooperation meshed closely with the education and equipping programs conducted through security assistance programs. In fact, in many cases, more funding assistance to a country was provided through Department of State programs to enhance the capability of a nation’s armed forces, like Foreign Military Financing, than came from Department of Defense programs.

#### Congress granted the DOD authority to pursue training and interoperability as security cooperation with NATO

Bowne ’18 [Andrew; 2018; Major and Judge Advocate in the United States Air Force, Contract and Fiscal Law Professor, The Judge Advocate General's School, United States Army; Military Law Review, “Defending the New Fulda Gap: Deterring Russian Aggression Against the Baltic States Through Fiscal Legislation, 226 Mil. L. Rev. 147, lexis]

The lack of clarity for EDI authorities notwithstanding, efforts to build defense capacity in the Baltic States were bolstered by the overhaul of the security cooperation regime in the FY17 NDAA. In an attempt to simplify the quagmire that security cooperation authorities had become over the past fifteen years, Congress streamlined the dozens of various temporary and permanent sources of authority and codified them under one chapter in Title 10 of the U.S. Code. 125 Congress noted the increasingly more important role security cooperation plays in DoD operations, 126 and the below discussion of how EUCOM can leverage these new authorities to augment EDI demonstrates the potential utility such activities can have within NATO's deterrence strategy.

3. Defense Security Cooperation and the Baltic States

Since the terrorist attacks of 11 September 2001, Congress granted more authority to the DoD to engage in security cooperation with foreign militaries, a mission originally conducted by the DoS. Over that time, security cooperation became an integral part of the DoD's mission and is considered an important tool for executing its national security responsibilities. 127 The FY17 NDAA overhauled the previously unwieldy patchwork of authorities that made up the security cooperation regime and provides authority for the DoD to enhance interoperability and increase defense capability of friendly foreign militaries. As building partner capacity with newer NATO members is one of the five lines of effort under EDI, 128 these new authorities should be leveraged to the maximum extent possible by EUCOM in the Baltic States to ensure sufficient capability exists in that vulnerable region to deter Russia aggression. However, as discussed below, the source of funding for these authorities and whether they can be used in conjunction with EDI funds remains ambiguous.

a. Building Defense Capacity

Key among the changes is the replacement of 10 U.S.C. § 2282 on "Authority to Build the Capacity of Foreign Security Forces" with a new permanent authority that widens the scope of security cooperation the DoD can provide. 129 While the scope of Section 2282 was limited primarily to counterterrorism and stability operations, 130 broadens the scope of authorized foreign capacity building to include, among other purposes, training, and equipping for border security and operations or activities that contribute to an international coalition operation that is in the national interest of the United States. 131 Moreover, 10 U.S.C. § 333, Section 2282's replacement, will permit the DoD to provide lethal equipment on a global scale, which it was unable to do under Section 2282. 132 Finally, Section 333 allows the DoD to support the sustainment of previously provided equipment to foreign partners, whereas such sustainment was previously under the exclusive purview of the DoS through its Foreign Military Financing account. 133 This bureaucratic anachronism resulted in equipment at risk of disrepair, misuse, and inoperability by the foreign recipient. 134

Under the definitions section of the Security Cooperation chapter, security cooperation programs, such as those authorized by Section 333, include building and developing allied security capabilities for self-defense and building relationships that promote specific U.S. security interests. 135 The DoD should utilize these new authorities to build capacity in the security forces of the Baltic States in a way that it was unable to do so under the previous law. However, because Section 333 did not become law until the final days of Fiscal Year 2017 when it replaces Section 2282, 136 the utility of this new authority was largely unknown in FY17 and remains little used due to the complexity of funding Section 333 activities. Section 333 provides the sole source of funding shall come out of amounts authorized and appropriated for such fiscal year for O&M, Defense-wide, and available for the Defense Security Cooperation Agency. 137 However, Section 1241 of the FY17 NDAA adds additional sources of funding for Fiscal Year 2017 relevant to the Baltic States, including O&M Defense-wide, available for the Defense Security Cooperation Agency as specified in the funding table in Section 4301 of the FY17 NDAA, 138 as well as for the same line of items in the OCO O&M funding table in Section 4302. 139 The dual funding sources, O&M and OCO O&M, highlight the potential overlap between Section 333 capacity building, which are funded by O&M, and EDI capacity building, which is funded by OCO O&M. To avoid obligating funds from the wrong account, commanders must know whether the activity falls under EDI, and whether security cooperation funds can be used in addition to EDI or exclusively. Clarifying legislation can help resolve this confusion. 140

b. Operational Support to Foreign Forces

In addition to the replacement of Section 2282, the FY17 NDAA greatly expands the authority to provide support for conduct of operations to friendly foreign countries, replacing Section 1207 from the Fiscal Year 2016 NDAA, which was limited to providing support to African countries conducting counterterrorism activities. 141 Section 1245 of the FY17 NDAA, codified at 10 U.S.C. § 331, greatly expands the scope of the previous authority by eliminating geographic limitations. 142 This new authority provides funding of logistic support, supplies, and services to security forces in a friendly country, as well as small-scale construction projects to facilitate friendly country participation in U.S.-supported operations. 143

One provision that, if utilized by EUCOM, could meaningfully assist improving the defense capability in the Baltic States is the special procurement authority that allows the DoD to procure equipment "for the purpose of the loan of such equipment to the military forces of a friendly foreign country participating in a U.S.-supported coalition or combined operation." 144 This is "to enhance capabilities or to increase interoperability with [U.S. forces] and other coalition partners." 145 Because the intent of the authority is that the friendly country will reimburse the United States for the procurement, or the U.S. forces can to reuse the equipment, there is no limitation on the value of the procurement. 146

The DoD should utilize this authorization to procure an excess quantity of U.S.-used systems to ensure friendly forces use and train on the same equipment as U.S. forces. Use of equipment, coupled with training and exercises will increase familiarity and interoperability with U.S. forces and provide friendly foreign forces with confidence in operating weapon systems alongside the United States. A successful loan may influence the friendly force's procurement decisions, leading to more effective use of defense spending by the friendly force at no real cost to the United States, as the equipment is returned at the end of the loan period. However, it remains unclear as to what limitations on the type of procurement there are, if any. For example, the law is silent as to whether this section authorizes procurement for loaning weapon systems. 147 Nor does it provide the maximum duration of any loan. Nonetheless, the DoD should leverage the seemingly broad authority granted by Congress to procure equipment for the purpose of loaning such equipment to its allies to improve interoperability and bolster the defense capability of its allies in Eastern Europe.

c. Training and Exercises

Finally, perhaps the best way the DoD can maximize the operational readiness of its NATO partners is through extensive training and exercises. 148 Training of NATO members near Russia is essential to ensure those members, such as the Baltic States and Poland, can cope with hybrid warfare that may not trigger Article 5. 149 Moreover, frequent military exercises with U.S. forces can enhance those armed forces' capabilities. Wide-scale multinational exercises on NATO's eastern flank would also serve a dual purpose of reassuring allies and warning foes. 150 Recognizing the importance of multinational training and exercises, Congress sought to provide broader authority for commanders of combatant commands and service secretaries to authorize payment of certain expenses for friendly foreign countries resulting from participating in training and exercises with U.S. general forces. 151 This expands the previous authority, which was limited to payment of only incremental expenses to developing countries when authorized by the Secretary of Defense. This was only after a determination that "the participation by such country is necessary to the achievement of the fundamental objectives of the exercise and that those objectives cannot be achieved unless the United States provides the incremental expenses incurred by such country." 152 The new authority requires only the determination by the Secretary of Defense that support of the friendly foreign force is in the national security interest of the United States to do so, and expands the scope and type of payment for training and exercise expenses. 153 It allows a commander of a combatant command to authorize payment for expenses associated with training, exercises, deployment to such events, incremental expenses, and small-scale construction directly related to the effective accomplishment of such events, with the prior approval of the Secretary of Defense. 154

Beyond the benefit of paying for expenses to attract participation by other countries, this authority also appears to permit foreign forces to develop new capacity by allowing for training to improve the capacity of foreign forces beyond minimal level necessary to achieve interoperability, safety, or familiarization with U.S. forces in preparing for combined military operations." 155 While the new law states that the primary purpose of the training and exercises is to train U.S. forces, 156 there is no limiting language, such as restricting the training of foreign forces to only safety and interoperability. Thus, so long as U.S. forces are receiving the benefit of the training and exercises, the participation by other friendly forces and use of this authority for funding is permitted. Granting the DoD this authority allows it to better program more robust exercises and training focused on capacity building of the Baltic States' forces.

Consistent with the intent of EDI and RAP, EUCOM should use this authority to the fullest extent practicable to integrate multinational forces, particularly in command and control, intelligence, surveillance, reconnaissance, and cyber defense, where interoperability is critical to defending against Russian aggression. 157 Moreover, this authority's provision for small-scale construction permits to building necessary infrastructure within Eastern Europe that would otherwise be challenging for approval. Provided the project does not represent a foreign assistance program, structures built in support of U.S. military personnel participating in overseas training and exercises need not be temporary structures. 158 The explicit limitation on such military construction is that no one project may exceed $ 750,000 in costs, 159 and the implicit limitation comes from the absence of any authority for the maintenance of such construction projects after the completion of the exercise. Nonetheless, this authority appears to permit the United States to fund and build in a friendly foreign country, and the beneficiary can then decide to keep and maintain the project for its own future use. The resulting infrastructure will provide training and exercise opportunities where there may have been none absent this authority.

### SC---AT: Excludes Hostilities---2AC

#### SC is not exclusively peacetime---SA and SC can be used to support major combat operations

Smith et al. ’17 [Kevin, Mark Lauber, and Lt. Cl. Matthew Robbins; April 1; Senior Analyst in the Joint Center for International Security Force Assistance at Joint Staff J7 Joint Force Development; Senior Special Operating Forces Analyst in the Joint Center for International Security Force Assistance; Joint Doctrine Development Officer in the Joint Doctrine Analysis Division at the Joint Staff J7 Joint Education and Doctrine Division; Joint Force Quarterly, “Joint Publication 3-20, Security Cooperation: Adapting Enduring Lessons,” 85]

Today’s security environment demands that the Department of Defense (DOD) employ a robust strategy and assortment of capabilities across the entire range of military operations and in support of America’s national security interests. A preponderance of these activities falls under the umbrella of security cooperation (SC) in which few, if any, U.S. forces participate directly in combat operations. As DOD continues to develop the “four plus one” threat baseline described by the Chairman of the Joint Chiefs of Staff, the Joint Force Development Directorate has taken steps to better align joint doctrine with the National Military Strategy as part of an approach that emphasizes the need for adaptive doctrine.1 Within this effort, the need to synergize U.S. capacity and capabilities with those of its partners remains paramount.2

To this end, ongoing efforts to adapt the disparate entities and authorities associated with SC into a unified strategy serve as an important next step. In 2008, DOD published a directive that elevated the requirement for DOD expertise for SC activities to the same level as other “integral [conventional] DOD activities.”3 To achieve parity, the Joint Doctrine Development Community (JDDC) identified the need to incorporate the topic of SC into the joint publication library as Joint Publication (JP) 3-20, Security Cooperation. The approval of JP 3-20 is a major step toward the joint force recognizing SC as a way to apply the military instrument of national power in support of partner nations (PNs) around the globe to achieve strategic objectives and to help shape the operational environment for current and future operations. This article outlines the continued adaptation of SC and the inextricable doctrinal security force assistance (SFA) principles discussed in JP 3-20 that are applicable to the joint force.

JP 3-20 defines security cooperation as “all DOD interactions with foreign security establishments to build security relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a partner nation.”4 These three categories, however, only hint at the true breadth and complexity of activities that make up the universe of security cooperation. Some SC activities are simple engagements between U.S. and PN defense officials, while others are complex and may include multibillion-dollar arms negotiations brokered at the highest levels of government through DOD-administered and Department of State–led security assistance (SA) programs under U.S. Code Title 22 authority. These examples bracket the more common theater security cooperation exercises routinely conducted within each geographic combatant command’s area of responsibility. While the recent and formal incorporation of SC into joint doctrine may appear new, the United States has used various adaptations of SC to protect and advance its vital interests abroad for decades.

Historical Overview

In 1971, the Secretary of Defense established the Defense Security Assistance Agency (DSAA) to direct, administer, and supervise the execution of approved SA plans and programs, such as military assistance, international military education and training, and foreign military sales.5 In November 1997, the Defense Reform Initiative transferred additional responsibility for program management of humanitarian assistance and demining, armaments cooperation, export loan guarantees, and foreign comparative testing functions, along with their associated personnel and resources, to DSAA. In October 1998, SC officially entered the DOD lexicon, accommodating the scope of these additional functions beyond DSAA’s traditional SA missions. This expansion of mission necessitated a name change, hence DSAA’s redesignation as the Defense Security Cooperation Agency.6 This consolidation of similar programs from five dissonant agencies into one stand-alone entity reflected efforts to improve efficiency and reduce administrative redundancy.

However, SC did not appear in mainstream joint doctrine until manifested in a 2004 revision of JP 3-07.1, Joint Tactics, Techniques and Procedures for Foreign Internal Defense (FID). As the JDDC struggled to refine doctrinal treatment of SC, amended versions of then–JP 1-02, Department of Defense Dictionary of Military and Associated Terms, revealed continuing efforts to clarify myriad SC activities. Though not retained in the current JP 1-02, the meaning behind the original definition of SC activity prevails:

Military activity that involves other nations and is intended to shape the operational environment in peacetime. Activities include programs and exercises that the U.S. military conducts with other nations to improve mutual understanding and improve interoperability with treaty partners. They are designed to support a combatant commander’s theater strategy as articulated in the theater security cooperation plan.7

Today, SC more broadly supports the combatant command’s entire theater campaign plan.

Subsequent developments in SC further expanded its scope by adding authorities from U.S. Code Title 10 for programs such as multinational exercises—a move designed to gain synergy by coordinating peacetime Title 10 activities with Title 22 activities. Amended in the reformative aftermath of the Vietnam War, these Title 22 programs specifically precluded the United States from employing its forces in harm’s way using SA funds. This contributed to a misunderstanding of both SA and SC as exclusively peacetime activities. This inaccurate conclusion led to confusion regarding when and how SA and SC authorities and programs could and should be used. Originally designed to limit American participation in conflict, modern versions of the vintage U.S. Lend-Lease program, as the precursor to what we now know as SA, continue to evolve, but still contribute to the development of our foreign partners’ security force capacities and capabilities across the entire range of military operations.

The term security force assistance entered the DOD lexicon to provide greater depth to the SC pillar of developing PN capabilities. SFA was coined (after early efforts in Iraq failed to create a viable security force) to provide U.S. forces with applicable means for developing the capacity and capabilities of PN forces and their supporting institutions. The training of foreign security forces is a primary role of U.S. special operations forces. However, special operations forces were stretched to their limits conducting counterterrorism and counterinsurgency operations throughout the Iraq and Afghanistan theaters of operation and elsewhere. In response, significant numbers of conventional forces were indoctrinated to conduct SFA activities and further doctrine was developed. The initial incorporation of SFA into the 2010 replacement for JP 3-07.1, known after as JP 3-22, Foreign Internal Defense, defined it as DOD “activities that contribute to unified action by the U.S. Government to support the development of the capacity and capability of foreign security forces and their supporting institutions.” Essential to SC, this streamlined definition established the enduring relevance of SFA, and subsequently SC, in all circumstances where U.S. military forces must develop foreign security force (FSF) capabilities.

SC and SFA in the Current and Future Operating Environment

While SC and SFA remain important to steady-state operations, they are equally valuable in support of major combat operations because they can facilitate operational access and improved military relations and interoperability. Whether considering their preemptive use to shape the operational environment, provide trained and ready forces to participate in operations, or create a postconflict application to lay the foundations for lasting peace and regional stability, SC and SFA present irreplaceable mechanisms for achieving conditions conducive to U.S. national interests.

### SC---AT: Excludes NATO---2AC

#### Security coop entails all DOD interactions with foreign security establishments, including NATO

Davids ’19 [Douglas; December; Center for Army Lessons Learned; News from the Front, “The Front of Military Education and Security Cooperation: Defense Security Cooperation University,” https://usacac.army.mil/sites/default/files/publications/17981.pdf]

Security cooperation is defined as "all Department of Defense (DOD) interactions with foreign security establishments to build security relationships that promote specific U.S. security interests, develop allied and partner-nation military and security capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to allied and partner nations."1 Security cooperation is a multifaceted effort that requires more than just planning to develop the skills of a foreign security force. In 2017, the National Defense Authorization Act (NDAA) created the DOD Security Cooperation Workforce Development Program (SCWDP) to develop and manage supporting security programs, improve the quality of the security cooperation workforce, and ensure personnel have the appropriate level of expertise and experience to perform their missions.2

The 2017 NDAA directed the Defense Security Cooperation Agency (DSCA) to manage the SCWDP's training and education standards, as well as identify and define training and certification requirements. Specifically, DSCA was required to "establish and maintain a school to train, educate, and certify the security cooperation workforce ... ." To meet this obligation, DSCA established the Defense Security Cooperation University (DSCU) in September 2019, to educate and certify 20,000 U.S. government employees' security cooperation and standardize their training.

Purpose

This article provides a brief description of the threat environment security cooperation must work within, an overview of the new DSCU, a discussion of the legal requirements emplaced on the DSCU, and an example course from DSCU and how this course meets the legal requirements.

The Threat and Environment

The threats the U.S. faces worldwide are vast and at times, overwhelming. They include both irregular and major power threats. Prior to 11 September 2001, irregular threats such as terrorist activities, piracy, trafficking of illegal drugs and illegal arms, and human smuggling already endangered U.S. and international security. However, today these entities are major nonstate actors that can threaten free societies across entire regions and even present transcontinental threats. Irregular forces do not have borders, uniforms, or rules, and will take advantage of any weakness found in the global system. The 2018 National Military Strategy states that "transnational threat groups, from jihadist terrorists to transnational criminal organizations, are actively trying to harm Americans."3 However, these numerous irregular threats are too vast for the U.S. to handle alone and require the help of allies and partners.

The reemergence of a great power competition with Russia and China has also added to the need for effective security cooperation, and, as stated in the 2018 National Military Strategy, "represents the most difficult challenges facing the Joint Force."4

The hard reality is that major powers like Russia and China are very much involved in the effort to gain greater influence around the world while diminishing the U.S.'s position. The 2017 National Security Strategy states that "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity."5 Threats like the Islamic Republic of Iran cannot be taken lightly either, and the situation with North Korea, despite peace talks, is still unpredictable. Both are "determined to destabilize regions, threaten Americans and our allies, and brutalize their own people."6 Major powers are trying to secure alliances, minerals, or bases of support with neutral territories in order to diminish U.S. influence in the region. Without robust security cooperation efforts to unify U.S. efforts with those of its allies and partners, adversaries could gain a position of relative advantage.

" ... by strengthening the militaries of our allies and partners, you actually strengthen your own security."

Security cooperation builds the capacity of foreign security forces to meet today's challenges, supporting and advancing the interests of the U.S. and partner nations. Aside from long-term allies and cohorts, the U.S. has new partners in the global security system, many of which need assistance. Not only is Eastern Europe no longer a satellite of the old Soviet Union power, but many of its nations are now members of the North Atlantic Treaty Organization (NATO). This has tipped the balance of power away from Russia. Russia has executed actions, such as in Ukraine and the Black Sea, to regain its position of power. In Asia, the U.S. has incorporated former adversaries, such as Vietnam, as part of the U.S.'s security cooperation efforts to keep China's aggressive expansion at bay. Security cooperation is a growing industry in the strategic efforts of the U.S., and this is not likely to change in the near future. Security cooperation is a necessary activity that helps the U.S. respond to irregular and conventional threats.

### SC---AT: JCS Categories Only---2AC

#### Not true. The categories are common examples of “security cooperation.”

JCS ’17 [Joint Chiefs of Staff; May 23; publishing with the Army, Marine Corp, Air Force, Navy, and Coast Guard; Security Cooperation, Joint Publication 3-20, “Appendix A: Security Cooperation: Related Programs and Authorities,” https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf]

This appendix describes DOD and DOS programs that have been used to support a variety of SC activities. This appendix is not all inclusive and provides only an overview of the programs. In most cases, planners should consult with legal advisors to identify the proper USC section, regulation, or directive prior to any expenditure of resources. As a matter of fiscal law, funds may only be expended for the purpose for which they were authorized. Consequently, the planners and appropriate commander must ensure any expenditure of funds for an SC activity complies with the associated fiscal mandates. Failure to do so can result in a violation of the Anti-Deficiency Act.

### SC---AT: Only DOD---2AC

#### “Security cooperation” could use any of the USFG.

Zaccor ’5 [Albert; August; Colonel in the US Army and Atlantic Council Senior Fellow; the Atlantic Council of the United States, “Security Cooperation and Non-State Threats: A Call for an Integrated Strategy,” https://www.files.ethz.ch/isn/46290/2005\_08\_Security\_Cooperation\_and\_Non-State\_Threats.pdf]

It is an oft-repeated mantra that in order to defeat transnational terrorism, and by extension other related non-state threats, the United States must apply all the elements of national power, including diplomatic, informational, military, and economic.34 The OSD SCG directs that DOD Security Cooperation “will be integrated with other elements of national power…in order to achieve national security, defense, and foreign policy objectives.”35 This formulation, while helpful, obscures two key facts. First, Security Cooperation includes activities that by their very nature involve the simultaneous application of more than one element of national power. Security Cooperation at a minimum requires the combination of diplomatic relations, military assistance, military-to-military contacts, and public diplomacy. In other words, Security Cooperation is itself an application of at least three of the classic elements of national power.36 Second, DOD is not the only entity in the USG that interacts with foreign governments to achieve the stated objectives: relationships, capabilities, information and intelligence, and access. The Department of State, the Intelligence Community, and to a lesser extent, other departments and agencies, conduct activities aimed at the accomplishment of these objectives, broadly understood. There is, however, no common USG, or interagency, definition or concept of Security Cooperation.37 We will return to this issue in the final section of this paper. For the purposes of the present discussion, this paper offers the following working definition of Security Cooperation:

Footnote 37.

37 Even within DOD there are programs, notably directed against WMD proliferation, that are not covered under the rubric of Security Cooperation. See the discussion of the WMD Proliferation Prevention Initiative, below.

Footnote 37 ends. The article continues.

Security Cooperation refers to all USG assistance provided to foreign law enforcement, security, and defense establishments in support of national defense, security, and foreign policy objectives.38

Footnote 38.

38 The application of the Security Cooperation paradigm to the entire USG requires a precise definition of security. Defined too broadly, Security Cooperation would simply be a surrogate for foreign policy. Limiting the objectives to specific enumerated defense and security objectives and assistance to foreign establishments playing a role in national security or defense is necessary to circumscribe the issue adequately.

Footnote 38 ends. The article continues.

This expanded definition of Security Cooperation will help us to see how the USG may leverage its programs and activities to fight terrorism and related non-state threats.

The role of Security Cooperation in countering non-state threats is clearly reflected in U.S. strategy. The NSS states that the U.S. will cooperate with nations to counter terrorism and WMD proliferation, assisting those that are willing but unable, and persuading those that are able but not willing.39 The National Military Strategy (NMS) develops the concept of forward defense, or “Countering Threats Close to Their Source.”40 This is the recognition that the United States’ first line of defense is abroad, and that it is necessary to “patrol strategic approaches” and extend U.S. defensive capabilities beyond our borders to create an active “defense in depth.”41 In this context, Security Cooperation is best understood as a set of tools that can shape the strategic battlespace by creating the conditions necessary to accomplish U.S. security and defense objectives.42 As the NMS’s focus on forward defense indicates, these activities are by their nature anticipatory, preparatory, and defensive.43 They are best used as part of a long-term comprehensive strategy to put in place the relationships, capabilities, information and intelligence, and access to facilitate future offensive and defensive actions to counter non-state, as well as more traditional, threats.

Security Cooperation Goals

Before turning to a detailed discussion of the contribution that Security Cooperation can make to fighting non-state threats, let’s briefly examine the four main goals of security cooperation in that context.

Relationships

Fighting strategic criminals will require the cooperation of a variety of governments, including those outside our established alliance relationships. We are not capable of compelling the kind of “willing and competent cooperation” that we need.44 Security cooperation provides powerful tools to persuade foreign governments to work with the U.S. in support of common objectives. Senior U.S. commanders, notably current and former Geographic Combatant Commanders, regularly stress the critical contribution that Security Cooperation activities make to building the kinds of relationships with foreign leaders that set the stage for successful U.S. operations. The example most often cited is the role that US Central Command (CENTCOM) Security Cooperation activities played in persuading Central Asian leaders, notably in Uzbekistan and Kyrgyzstan, to support U.S. military operations in Afghanistan by granting access to bases and overflight rights.45 In addition to granting access, good relationships aid in building a common threat perception, which is a necessary precondition for any substantial cooperation. Relationships with foreign defense leaders can also provide the U.S. with influence over the policy direction of key partner states, including efforts at defense reform and the shape of force structure changes. Finally, good relationships make it more likely that foreign governments will share information with the U.S., including, in the extreme case, early warning of potential attack.46

Intelligence and Information Sharing

Relationships built on trust and mutual interests are also necessary to obtain cooperation from foreign governments in the area of Intelligence and Information. It is useful to separate the distinct, but related, issues of Intelligence Sharing and Intelligence Security Cooperation. Intelligence Sharing is a critical element in the fight against non-state threats, or strategic crime. By its nature, however, such sharing involves sensitive sources, methods and arrangements, normally in the context of a bilateral relationship. Its sensitivity requires delicate handling in highly restrictive channels. Intelligence sharing, in practice, falls outside the scope of Security Cooperation. Intelligence Security Cooperation, on the other hand, involves the development of interoperable and cooperative intelligence systems and processes designed to enhance the ability of one partner to work with one or several other partners. The core activities in Intelligence Security Cooperation are analytical and expertise exchanges, familiarization, training, and traditional Security Assistance. Both Intelligence Sharing and Intelligence Security Cooperation are mutually supporting. It is clear that the quality and reliability of intelligence we get from our partners depends on the competence, capability, professionalism, and trustworthiness of their national intelligence services and how compatible their operations are with ours. Intelligence Security Cooperation provides the tools to develop long-range relationships with foreign partners to improve both the quality of the intelligence we share and our ability to work together.

Access

The National Defense Strategy stresses the requirement to secure strategic access and retain global freedom of action for U.S. forces.47 This includes obtaining permanent and deployment basing and overflight. Security Cooperation directly supports access by developing relationships with foreign partners based on trust and mutual interests. Senior officer and other official visits contribute to this by demonstrating U.S. commitment to a defense relationship and staying abreast of host nation priorities, concerns, and requirements. Some Security Cooperation activities directly support access by improving host nation infrastructure, notably airbases, ports, and troop facilities, to support U.S. forces during operational and training deployments. Other activities improve host nation capabilities through training, equipping, and exercises. The NMS recognizes that access has an informational dimension that goes beyond the purely physical access to a partner’s territory, facilities or airspace:

“…theater security activities with multinational partners provide access to information and intelligence critical to anticipating and understanding new threats.”48

This insight is important in determining the contribution Security Cooperation can make to countering non-state threats. While DOD and the military services remain understandably focused on the physical dimension of access and its support to current and future operations, the fight against strategic criminals requires that we pay greater attention to securing strategic access to information and information networks controlled by our partners, allies, and adversaries. In some cases “virtual access” to databases, data flows, raw and finished intelligence, sensor data, and other forms of information may be more critical to the success of military operations than the ability to access an airfield, port or overflight corridor. Security Cooperation tools can also support the attainment of this non-traditional form of access.

### SC---AT: Only DOD---1AR

#### The DOD definition is bad.

Lenze ’17 [Major Anthony Lenze; 2017; Judge Advocate in the United States Army; Military Law Review, “Traditional Combatant Commander Activities: Acknowledging and Analyzing Combatant Commanders' Authority to Interact with Foreign Militaries,” vol. 225]

Security cooperation is now a term that encompasses “any program, activity (including an exercise), or interaction of the [DoD] with the security establishment of a foreign country to achieve a [strategic] purpose ... [.]”85 The DoD assigns such strategic importance to security cooperation that, with the help of Congress, it created the Defense Security Cooperation Agency (DSCA) to direct and guide the execution of all DoD security cooperation programs.86 The DSCA helps administer security cooperation, now a multi-billion dollar industry within the annual Defense appropriation.87 With all the money and strategic brainpower pouring into security cooperation, newcomers to the field may presume fully-vetted, standardized terms and definitions. However, this could not be further \*656 from reality.

Members of the DoD frequently mischaracterize security cooperation or outright disagree with respect to its doctrinal definition.88 For example, the 2010 National Security Strategy (NSS) used the term security cooperation to include rebuilding damaged infrastructure and establishing conditions necessary to end military operations in Afghanistan.89 With the exception of combat operations, it would seem that almost any military action could fit under the 2010 NSS's version of security cooperation.90 Nevertheless, if security cooperation is in fact an evolving term in the DoD, making sense of the authorities under which the military executes security cooperation events is even more troublesome.91 This is especially true when authorities are based upon a set of specific terms. Hence, with doctrine lagging behind and accompanied by undefined terminology, no authority in the realm of security cooperation is more ambiguous than the authority for military-to-military contacts.92 With ambiguity surrounding military-to-military contacts, planners and lawyers should defer to commanders to decide the best way to employ these strategic interaction events. The fate of 10 U.S.C. §168 and its ultimate repeal is illustrative of this point.

#### The 2NC cited the definition FROM the Department of Defense, which doesn’t define the word broadly.

Zaccor ’5 [Albert; August; Colonel in the US Army and Atlantic Council Senior Fellow; the Atlantic Council of the United States, “Security Cooperation and Non-State Threats: A Call for an Integrated Strategy,” https://www.files.ethz.ch/isn/46290/2005\_08\_Security\_Cooperation\_and\_Non-State\_Threats.pdf]

Lack of Doctrine

Part III of this paper offered a definition of Security Cooperation that could be common to the entire USG, not just the Department of Defense. The USG interagency has no such common definition because it lacks a common conceptual understanding of how to translate higher level strategic guidance into specific programs designed to accomplish strategic objectives.

The Department of Defense, despite its size, its diversity, and the scope of its Security Cooperation activities, has such a common understanding. DOD’s process is not without its flaws.113 During the late 1990s and the early 21st century, however, the department has successfully established a rational set of procedures for translating the strategic guidance in the National Security, Military, and, now, Defense Strategies, into specific programs executed by the military commands, services, and defense agencies.114 This process promotes discipline by forcing subordinate organizations to demonstrate that their Security Cooperation activities directly support specific objectives in the higher-level strategies. Efforts are under way to discipline the process further by establishing an assessment mechanism to provide feedback on the effectiveness of programs and activities.115 One reason for the success of the DOD program is OSD’s publication of periodic Security Cooperation Guidance. This document, in addition to providing authority for subordinate organizations’ Security Cooperation activities (see more below), serves the purpose of an informal doctrine, stipulating not only the “what,” but the “how” and the “why” of Security Cooperation.116

Footnote 113.

113 For example, there are still failures to coordinate and inadequate integration among DOD managed programs. Amy Chou, OSD Strategy Office, interview by the author, 14 Jan 05.

Footnote 113 ends. The article continues.

In order for the USG interagency to plan and execute Security Cooperation programs and activities in an integrated and synergistic manner, a doctrine, or common conceptual framework, for Security Cooperation is necessary. Such a doctrine would have to define what Security Cooperation is, and, what it is not.117 It would have to define precisely which departmental and agency programs qualify as Security Cooperation and outline a procedure for combined interagency planning, programming, and execution. Armed with such a common conceptual framework, executive branch officials and program managers will be better equipped to engage in integrated planning and program execution. True success in this effort, however, will depend on the resolution of the other problems of authority, funding, and process and organization.

Footnote 117.

117 As has been suggested here, activities to improve foreign partners’ security capabilities conducted by any department or agency would qualify as Security Cooperation. In contrast, general foreign development assistance, although related to security and part of broader U.S. foreign policy, would probably not. Even within DOD, this is not totally clear. Officials in OSD’s Counter-proliferation Policy office refused to admit that activities intended to improve the maritime security capabilities of Azerbaijan and Kazakhstan in support of counter-proliferation would be included under the definition of Security Cooperation and declined to integrate their program formally with other DOD Security Cooperation efforts.

Footnote 117 ends. The article continues.

Unclear Authority

The USG lacks a clear authoritative basis for guidance of Security Cooperation programs and activities. This is rooted in the lack of overall strategic planning in the USG and the ad hoc and department-specific nature of the planning that does occur. 118 There is no equivalent of the OSD Security Cooperation Guidance for the interagency to guide the programmatic activities of executive branch departments and agencies. The strategy documents, such as the NSS or National Strategy for Combating Terrorism, provide overall strategic intent, goals, and objectives, and suggest broad means for accomplishing them. The strategies successfully link the various non-state threats by cross-referencing them and demonstrating the interconnected nature of terrorism, WMD proliferation, narcotics trafficking, and transnational organized crime. This high-level strategic guidance does not result in integrated strategies, however, because the goals and objectives are too broad to drive implementation at the program level and because there is no requirement for departments and agencies to develop integrated plans.

#### DOD has a history of security cooperation, but “security cooperation” as an overarching term depends on its content.

Maroney ’13 [Jennifer D. P. Moroney and David E. Thaler; 2013; International Relations PhD at the University of Kent-Canterbury; Master of International Affairs from Columbia University; RAND, “Review of Security Cooperation Mechanisms Combatant Commands Utilize to Build Partner Capacity,” https://www.rand.org/pubs/research\_reports/RR413.html]

Security cooperation (SC) is an overarching term that defines “those activities conducted with allies and friendly nations to build relationships that promote specified U.S. interests, build allied and friendly nation capabilities for self-defense and coalition operations and supporting institutional capacity, [and] provide U.S. forces with peacetime and contingency access.”1 Examples include training and combined exercises, operational meetings, contacts and exchanges, security assistance, medical and engineering team engagements, cooperative development, acquisition and technical interchanges, and scientific and technology collaboration. The Department of Defense (DoD) has a long history of conducting SC activities with partner countries for a variety of purposes, including building partner capacity (BPC), which is a primary focus of this report.

### SC---AT: Congress Says DOD Only---2AC

#### Wrong, Congress defined “security cooperation…OF the department of defense.”

US Code ’18 [United States Code Annotated; last amended Aug. 13, 2018; Title 10: Armed Forces, Subtitle A: General Military Law, Part I: Organization and General Military Powers, “Security Cooperation,” Chapter 16]

(7) The term “security cooperation programs and activities of the Department of Defense” means any program, activity (including an exercise), or interaction of the Department of Defense with the security establishment of a foreign country to achieve a purpose as follows:

(A) To build and develop allied and friendly security capabilities for self-defense and multinational operations.

(B) To provide the armed forces with access to the foreign country during peacetime or a contingency operation.

(C) To build relationships that promote specific United States security interests.

## With

### With---Excludes Subsets---1NC

#### “With” refers to the total.

Oxford ’89 [Oxford English Dictionary; 1989; English Dictionary, second edition; Oxford English Dictionary Online, “with, prep., adv., and conj,” accessed through the University of Michigan]

b. Comprising in the whole number or total; including.

#### Limits and ground -- subsets unlock endless reshuffling of member states and unpredictable configurations designed to evade negative generics.

### With---Not Unilateral---1NC

#### “With NATO” requires other allies to participate in crafting and enforcing the plan---unilateral policy shifts by the US are excluded

Gregory ’15 [Roger; Aug 19; Judge, United States Court of Appeals, Fourth Circuit; States v. Bollinger, 798 F.3d 201]

The second textual limitation - the fact that commerce must be "with foreign Nations" - requires a nexus between [\*\*30] the United States and a foreign country. See Goodno, supra, at 1202 (observing that dictionaries contemporary to the Constitutional Convention defined "with" as "noting the means" or "noting connection" (internal quotation marks omitted)). The use of the word "with" in the foreign clause, instead of the word "among" as used in the interstate clause, merely suggests the obvious: Congress cannot regulate commerce "among" foreign nations because other nations do not submit their sovereignty to our regulatory powers

### With---Not Unilateral---2NC

#### “With” requires that the other country be a participant

Merriam-Webster’s ’22 [Online Dictionary, “with”, http://www.merriam-webster.com/dictionary/with]

2 a —used as a function word to indicate a participant in an action, transaction, or arrangement <works with his father> <a talk with a friend> <got into an accident with the car>

b —used as a function word to indicate the object of attention, behavior, or feeling <get tough with him> <angry with her>

c : in respect to : so far as concerns <on friendly terms with all nations>

d —used to indicate the object of an adverbial expression of imperative force <off with his head>

e : over, on <no longer has any influence with them>

f : in the performance, operation, or use of <the trouble with this machine>

#### Cooperation is coordinated action of two or more States under a legal regime

Karimova ’16 [Tahmina; 2016; Legal Officer at the International Labor Organization, Ph.D. from the Graduate Institute of International and Development Studies, Geneva; Human Rights and Development in International Law, p. 122-124]

Edward McWhinney observes that as a term of art of international law, ‘cooperation’ emerged after World War II.2 No treaty or international decision defines the notion or the term ‘cooperation’, though. Wolfrum defines cooperation as ‘the voluntary coordinated action of two or more States which takes place under a legal regime and serves a specific objective’ and to ‘this extent marks the effort of States to accomplish an object by joint action, where the activity of a single State cannot achieve the same result’ or mutual benefit.3 What follows is that the duty to cooperate would lead to an obligation to enter into such an action to achieve a specific goal. In terms of substance, cooperation per se has no independent content;4 it must be tied to a specific area to acquire a specific meaning.

#### “With” indicates who the cooperation is with.

Dean ’85 [Robert Dean, Thomas Cane, Daniel Larocque; May 14; Judges on the Court of Appeals of Wisconsin; Westlaw, “Engel v. Engel,” 125 Wis. 2d 568]

Their father's participation in the action as vendor does not give the trial court jurisdiction to partition. Their father may not bring the action because he does not hold the property in common with his sons. See sec. 700.18, Stats. Moreover, the preposition ‘with’ in sec. 842.02(1) is used as a function word to indicate a person who shares in an action, transaction or arrangement. Webster's New Collegiate Dictionary 1346 (1977). Only Werner, Sr., qualifies as a person having an interest in the real property. He therefore does not have an interest ‘with’ anyone.

#### “With” means NATO must share in the arrangement.

Lautenschlage ’3 [Peg; July 8; Attorney General of the State of Wisconsin; Westlaw, “Respondent-Respondent Berge's Brief and Appendix” in *Wisconsin v. Berge*, 2003 WL 23837809]

Moreover, the use of the preposition “with” is significant. The preposition “with” is “used as a function word to indicate one that shares in an action, transaction, or arrangement.” Webster's Third New International Dictionary 2626 (3d ed. 1986); see also Village of Menomonee Falls v. Falls Rental World, 135 Wis. 2d 393, 397, 400 N.W.2d 478 (Ct. App. 1986) (stating that it is proper for courts to look to dictionary definitions to determine the plain meaning of words.) Given “with's” plain meaning in this context, all correspondence either from Garrett to Ms. Spoo (a/k/a Diane Brice), or from Ms. Spoo (a/k/a Diane Brice) to Garrett, is suspended. If Garrett wanted to challenge the suspension of that privilege, he should have appealed to the warden within 10 days of Boughton's June 26, 2002, memorandum. The return is devoid of any indication that he did that. The circuit court's decision should be affirmed.

#### “With” means NATO must accompany the US in cooperation.

Grey ’15 [Ellery Gray, Marty Jackley, and Mark Vargo; March 3; Attorneys; Westlaw, “Appellant's Reply Brief” in *South Dakota v. Eagle*, 2015 WL 3610506]

In its holding, the Viramontes court announced that the holding (or restraining) was unlawful because it was “for” the purpose of abandonment. This shift grammatically conflates the legality of the holding with the legality of the proscribed purpose. However, the Arizona kidnapping statute, like the South Dakota kidnapping statute, uses the preposition “with.” Prepositions, though often short words, are very powerful. Take for example the following: “My mother is at the hospital” and “My mother is in the hospital.” The shift in language by the court above was an even larger shift than the preceding example. Both words have multiple definitions, each dependent upon context. The Merriam-Webster dictionary provides several distinct uses of both “with” and “for.” Concerning “with” the dictionary has, in part, this to say: “'with... 4

a - used as a function word to indicate combination, accompaniment, presence, or addition <heat milk with honey> <went there with her> <his money, with his wife‘s, comes to a million> (http://www.merriam-webster.com/dictionary/with) This is the same use of “with” that both the Arizona and South Dakota kidnapping statutes use. In both cases, the unlawful holding is required to “accompany” the proscribed purpose. Concerning “for” the dictionary has, in part, this to say: “‘for’ 1

### ‘With’ Modifies Noun---1NC

#### “With” modifies security cooperation.

Davis ’9 [Robert; April 30; Judge on the United States Court of Appeals for Veterans Claims; Westlaw, “Smith v. Shinseki,” No. 07-1646, 2009 WL 1204792]

The second and third alternatives also include the preposition “with.” In this instance, the preposition modifies a noun and expresses a relationship. “With” indicates accompaniment. See WEBSTER'S 2626. Therefore, in order to receive a 100% schedular rating based on the second alternative, a veteran must show that cardiac involvement is accompanied by congestive heart failure. To receive a 100% schedular rating based on the third alternative, the alternative at issue in Ms. Smith's case, she must demonstrate that she has progressive pulmonary disease, and that the disease is accompanied by fever, night sweats, and weight loss despite treatment.

### ‘With’ Excludes Foreign-Only Action---1NC

#### “With” requires American action.

Hartz ’18 [Harris; August 29; Court of Appeals Judge on the Tenth Circuit, dissenting; Westlaw, “United States v. Durham,” 902 F.3d 1180]

The panel opinion suggests that the text of the Commerce Clause indicates that power under the Foreign Commerce Clause exceeds that under the Interstate Commerce Clause. See Maj. Op. at 1201–02. It notes that the Clause speaks of commerce “with foreign Nations” but “among the several States.” But the difference in prepositions indicates the opposite. If the Clause permitted regulation of commerce “among foreign nations”—so that the two clauses used the same preposition—then Congress would be empowered to regulate commerce among France, England, and Italy, even if the United States were not involved at all. Thus, use of the preposition with instead of the preposition among obviously limits the extent of the Foreign Commerce Clause. See Colangelo supra at 970–71 (explaining the difference between the uses of the two prepositions in the Commerce Clause).7

### With---Involves NATO---2AC

#### ‘With’ requires involving NATO in the creation of the plan

Colangelo ’10 [Anthony; September; Assistant Professor of Law, SMU Dedman School of Law; “ARTICLE: THE FOREIGN COMMERCE CLAUSE,” Virginia Law Review, 96 Va. L. Rev. 949]

It was precisely this general, national regulatory power that saved application of the federal Controlled Substances Act ("CSA") to homegrown medical-use marijuana in the Court's 2005 decision Gonzales v. Raich, 128 and that has constitutionally justified numerous federal laws designed to prevent various races to the bottom "among" the states. 129 The Foreign Commerce Clause contains no equivalent, globally-encompassing authority to regulate "among" foreign nations, only the power to regulate commerce "with" them. 130 The difference between the power to regulate among members of the domestic system, but only with members of the international system, suggests that Congress has no more power to regulate inside foreign nations than it has inside the several states.131 Indeed, as Section B explains in more depth - and [\*974] contrary to leading lower-court decisions - this textual difference actually deprives Congress of some of the more sweeping regulatory powers abroad that it enjoys at home.132 To preview the argument, Congress cannot independently create comprehensive global regulatory schemes over international markets or prevent races to the bottom among the world's nations the same way it can create comprehensive national regulatory schemes over domestic markets and prevent races to the bottom among the states. Because Congress lacks primary authority to create such global schemes, it cannot claim a derivative authority under the Necessary and Proper Clause to reach local foreign conduct that threatens to undercut those schemes the same way it can reach local intrastate conduct to [\*975] effectuate regulation "among the several States."133 Rather, for Congress to regulate local foreign conduct pursuant to a comprehensive international regulatory scheme, that scheme must be created "with foreign Nations."134 In this sense, the word "with" contemplates agreement or cooperation with foreign nations in establishing the scheme, without which Congress cannot extend U.S. law over local foreign conduct to effectuate that scheme.

### With---Membership---2AC

#### “With” denotes membership.

Collins 19 – Collins online Unabridged English Dictionary, American English section (not British). [With, carbon dated 1-4-19, https://www.collinsdictionary.com/us/dictionary/english/with]//BPS

a. as a member of

playing with a string quartet

## The North Atlantic Treaty Organization

### NATO---Collective Defense---1NC

#### NATO is a security treaty built around collective defense for member-states---topical plans must alter Article V conditions

Fukuyama ’22 [Francis; Jan 31; Olivier Nomellini Senior Fellow and director of the Ford Dorsey Master’s in International Policy program at Stanford University’s Freeman Spogli Institute for International Studies; “Dangerous Revisionism,” <https://www.americanpurpose.com/blog/fukuyama/dangerous-revisionism/>]

This doesn’t mean that NATO could or should have been expanded indiscriminately. As I argued in an earlier post, NATO is fundamentally a security treaty built around its Article V guarantee that an attack on one member would be considered as an attack on all. Countries that cannot actually be defended by the alliance should face a very high barrier to entry. This is not a matter of principle, but one of physical geography and military logistics. This is why I was opposed to offering eventual membership to Ukraine and Georgia back at the time of the Bucharest Declaration in 2008; there was no realistic way for the Article V commitment to be met if those countries faced a determined Russian attack.

#### Vote neg:

#### Ground---they wreck it by ensuring affs defend uncontroversial consultations and logistics meetings

#### Limits---opening up the topic to infinite new partnerships with non-NATO countries overstretches the neg research burden and undermines preparedness for all debates

### NATO---Collective Defense---2NC

#### NATO is exclusively a military alliance between member-states---prefer ev describing the essence of NATO

Fukuyama ’21 [Francis; December 14; Olivier Nomellini Senior Fellow and director of the Ford Dorsey Master’s in International Policy program at Stanford University’s Freeman Spogli Institute for International Studies; “Ukraine and NATO,” https://www.americanpurpose.com/blog/fukuyama/ukraine-and-nato/]

Saying this upsets many of my Georgian and Ukrainian friends, but there are very good reasons for shelving the NATO membership issue for the foreseeable future. My reasons have to do with the essence of NATO. The North Atlantic Treaty Organization is a military alliance, built around its Article 5 guarantee that an attack on one member would be considered as an attack on the whole alliance. Were NATO to accept Ukraine as a member today, its members would immediately be engaged in an ongoing war with Russia—a position no member of the alliance wants to be in.

#### NATO is defined by its collective defense principle between current member-states.

Iseminger ’18 [Russell; June 1; Major, USAF; Air Force Technical Report, “Conventional deterrence: the effect of U.S. airpower on Russian strategic calculus,” https://apps.dtic.mil/sti/pdfs/AD1107526.pdf]

NATO and the Russian Bloc

NATO is defined by the current 29 members of NATO, who are bound by the collective defense principle in Article 5 of the treaty where “an attack against one Ally is considered as an attack against all Allies.”41 The area of application as defined in the CFE Treaty includes all of Europe, so the forces in every NATO country will be counted with the exception of U.S. and Canadian forces that are not forward deployed to Europe. As depicted in figure 1, the Southeast portion of Turkey is excluded from the ATTU region. However, since that cut-out was generated primarily with ground forces in mind, for simplicity the combat aircraft in all of Turkey will be counted. NATO forces that were deployed outside of Europe were excluded from the totals.

#### NATO’s partner outreach programs aren’t core strategic interests---only pressuring NATO member-states to bolster defenses and capabilities constitutes “security cooperation with NATO”

Raitasalo ’15 [Jyri; July 2; Docent of Strategy and Security Policy at the Finnish National Defence University, (Lt. Col. (GS), Dr.Pol.Sc; War on the Rocks, “NATO Is Not A Real Military Actor,” https://warontherocks.com/2015/07/nato-is-not-a-real-military-actor/]

In addition, there are no separate strategic interests of NATO that could be fulfilled apart from the interests and actions of its member-states. The truth is that the Secretary General and the Chairman of the Military Committee — and a bunch of other NATO officials and actors — can persuade, plead and ask, but they cannot make any significant or binding decisions related to the use of military force within the territory of the Alliance, or elsewhere. It is the task of the member-states of NATO to bolster their own defenses and capabilities. This is the only way for NATO to retain the significance it once had in the arrangements of international security.

#### NATO is defined by its status as a defense pact with 30 member states: Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, and the U.S

Amadeo ’22 [Kimberly; March 6; expert on U.S. and world economies, with over 20 years of experience in analysis and business strategy; “What is NATO?,” https://www.thebalance.com/nato-purpose-history-members-and-alliances-3306116]

DEFINITION

The North Atlantic Treaty Organization (NATO) is an alliance of 30 countries that border the North Atlantic Ocean. The Alliance includes the United States, most European Union members, the United Kingdom, Canada, and Turkey.

Definition of NATO

The North Atlantic Treaty Organization is a national security alliance among the U.S., Canada, and their European allies. It was formed in the wake of World War II to keep the peace and encourage political and economic cooperation on both sides of the Atlantic Ocean.1

Acronym: NATO

While NATO is primarily a national security alliance, it does include an Economics Committee that seeks to provide a forum to discuss economics among members and to monitor economies within and outside of the Alliance. More broadly, NATO has been a stabilizing influence in Europe and North America, allowing the economies of its members to develop and flourish.2

Member Countries

NATO's 30 members are Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, and the U.S.3

Each member designates an ambassador to NATO as well as officials to serve on NATO committees and discuss NATO business. These designees could include a country’s president, prime minister, foreign affairs minister, or head of a defense department.

On December 1, 2015, NATO announced its first expansion since 2009, offering membership to Montenegro. Russia responded by calling the move a strategic threat to its national security. Russia is worried by the number of Balkan countries along its border that have joined NATO.

How Does NATO Work?

NATO's mission is to protect the freedom of its members and the stability of their regions. Its targets include weapons of mass destruction, terrorism, and cyber-attacks.

One key aspect of NATO is Article 5, which states that "an armed attack against one Ally is considered an attack against all Allies."4 In other words, an attack one NATO nation will cause all NATO nations to retaliate.

NATO has invoked Article 5 just once in its history, following the 9/11 terrorist attacks on the U.S.

NATO's protection does not extend to members' civil wars or internal coups. During a 2016 coup attempt in Turkey, for example, NATO did not intervene on either side of the conflict.5 As a NATO member, Turkey would receive its allies' support in the case of an attack, but not in case of a coup.

#### NATO is fundamentally a military alliance, organized around mutual defense and military consultation

Markert ’17 [Jennifer; July 1; Writer, citing U.S. treaty police and the Department of State; Curiousmatic, “U.S. Mutual Defense Treaties: Which Countries Has America Sworn To Protect,” <https://curiousmatic.com/u-s-mutual-defense-treaties-countries-america-sworn-protect>] \*Images omitted

Currently, the United States is involved with seven mutual defense pacts, tying the nation’s fate (and military) to a number of others.

1947 – Inter-American Treaty of Mutual Assistance (Rio Treaty)

Also known as the “Rio Treaty,” this [1947 agreement](http://www.oas.org/juridico/english/treaties/b-29.html) includes a total of 18 nations, the newest being the Bahamas which became a signatory in 1982. The pact stipulates that an attack against any of these nations, specific to the American hemisphere, is an attack against them all.

Mexico [withdrew](http://www.oas.org/OASpage/press2002/en/press2001/sept01/09007.htm) from the treaty in 2002 following the September 11 attacks (when the pact was first activated, [according to](http://web.archive.org/web/20150301023724/http:/unterm.un.org:80/dgaacs/unterm.nsf/8fa942046ff7601c85256983007ca4d8/d8814d2901e999d8852569fa000062b4?OpenDocument) the UN Terminology database), calling it obsolete and unnecessary. [A decade later](http://www.eluniversal.com/nacional-y-politica/120605/alba-countries-pull-out-of-hemispheric-mutual-defense-agreement) Bolivia, Nicaragua, Venezuela, and Ecuador retired as well.

1949 – North Atlantic Treaty Organization (NATO)

NATO is based on the [North Atlantic Treaty](http://www.nato.int/cps/en/natolive/official_texts_17120.htm), an international government military alliance signed by 28 nations, agreeing to mutual defense in response to any attack by outside parties.

Since it was formed in 1949, NATO’s [article five](http://www.nato.int/terrorism/five.htm), which states that an attack against one nation is an attack against all, has only been invoked only once – after the September 11, 2001 attacks – resulting in NATO [counter-terrorist missions](http://www.nato.int/docu/review/2011/11-september/10-years-sept-11/EN/index.htm).

Article 6 – which calls not for action, but military consultation, has been invoked three times by Turkey.

### NATO---Core Military Activities---1NC

#### ‘Substantially’ means in the main

Becker ‘14 [David S; Winter; Partner in the Litigation and Intellectual Property Practice Groups at Freeborn & Peters, LLP, J.D. from DePaul University College of Law, & John C. Hammerle, Associate in the Litigation Practice Group at Freeborn & Peters, LLP, J.D. from DePaul University College of Law; Committee News, “The Trouble With “Substantial Completion” in Construction Projects,” https://freeborn.com/assets/the\_trouble\_with\_substantial\_completion\_in\_construction\_projects-aba\_winter\_2014\_newsletter.pdf]

3 See, e.g., Kinetic Builder’s, Inc. v. Peters, 226 F.3d 1307, 1315 (Fed. Cir. 2000); Ocean Winds Corp. v. Lane, 556 S.E.2d 377, 379 (S.C. 2001) (citing statutory definition of substantial completion as “that degree of completion of a project, improvement, or a specified area or portion thereof . . . upon attainment of which the owner can use the same for the purpose for which it was intended”) (internal citations and emphasis omitted); Daugherty v. Bruce Realty & Dev., Inc., 892 S.W.2d 332, 335 (Mo. Ct. App. 1995) (“a building is substantially complete . . . when it has reached the state of its construction so that it can be put to the use for which it was intended, even though comparatively minor items remain to be furnished or performed to conform to the plans and specifications of the completed building”); E.R. Stone v. City of Arcola, 181 Ill. App. 3d 513, 526 (Ill. App. Ct. 1989) (acknowledging that a project is “substantially complete” at a given date where “it could be used for the purpose for which it was intended on that date”). See also Sorenson v. Dager, 601 N.W.2d 564, 570 (Neb. Ct. App. 1999) (\*fix this parenthetical); Evans & Assocs. v. Dyer, 246 Ill. App. 3d 231, 239 (Ill. App. Ct. 1993) (“Substantial performance . . . . means performance in all the essential elements necessary to the accomplishment of the purpose of the contract. ‘Substantial’ means in substance; in the main; essential, including material or essential parts.”)..

#### For US ‘coop’ with NATO, that means planning, doctrine, interoperability, and logistics---excludes NATO affs that aren’t tied to military planning

----even if it includes partners, it excludes ‘broad’ cooperation on issues like pandemic cooperation unrelated to preparing for an Article 5 contingency

Skaluba ’17 [Christopher; Nov 7; served as the principal director for European and NATO policy in the office of the secretary of defense from 2012 to 2015; War on the Rocks, “In Praise of NATO's Dysfunctional, Bureaucratic Tedium,” <https://warontherocks.com/2017/11/praise-natos-dysfunctional-bureaucratic-tedium/>]

A year after Donald Trump’s election to the presidency, the furor around his approach to transatlantic security has predictably calmed. Part of the reason is saturation. Like antibiotics, provocation of one’s allies loses its potency when used excessively. Part of the reason is that the president has found a more willing and compelling foil, in the form of Kim Jong Un, than those buttoned-up European leaders he accuses of freeloading. Certainly, part of the reason includes the administration’s Russia-related scandals and Robert Mueller’s investigation. The president’s hostility toward NATO has always felt more like a sop to Moscow than a matter of principle and thus not a good look with indictments swirling.

But much of it has to do with the nature of the alliance itself. NATO’s bread and butter is cooperation on activities like planning, doctrine, interoperability, and logistics — things which are uninteresting to the general public discourse and largely resistant to the rhetorical or policy whims of even the president of the United States. Cooperation in these areas, while camouflaged to all but the most intense NATO watchers, can move the needle to the benefit of the United States in concrete and practical ways. As Secretary of Defense Jim Mattis heads to Brussels for his third meeting of NATO defense ministers in ten months, it is precisely to ensure such work continues.

Perception Is Not Policy

If it is fair to stipulate, without a hint of irony or partisanship, that the president makes decisions based on a rather shallow understanding of the pertinent facts, then his initial posture towards NATO and Russia makes sense. In fact, as someone who watched an episode or two of The Apprentice, Trump’s embrace of Russia was predictable. Equipped with a disposition that necessarily invites competition between opposing factions, nerdy NATO with its committees and communiques never had a chance against a tiger-hunting former KGB agent who invades countries with impunity and without a shirt. Putin is ready-made television.

Yet, as others have ably pointed out, viewed through the lens of genuine policy, Trump’s complaints about European security and its key players have some basis in fact. And while it is tempting for policy professionals like me to seek some novel, far-reaching meaning from the impolitic veneer of his tweets and applause lines, the most remarkable thing about Trump’s censure of NATO is how quotidian it is as a matter of policy. Questions about NATO’s obsolescence date from at least the 1960s and have been a proverbial albatross for the alliance since the end of the Cold War. That the United States is over-invested in NATO relative to the Europeans and Canada is an acknowledged fact by nearly everyone working transatlantic issues. And while I grimaced at the graceless pluck of invoicing Angela Merkel for Germany’s pedestrian defense spending, if true, it was a gambit rooted in cause.

Even in tone, Trump’s complaints alternately echo Secretary Donald Rumsfeld’s grouchy demonization of “Old Europe” in 2003 and Secretary Robert Gates’ headmasterly admonition of European defense spending in 2011. Similarly, Trump’s flattery of Putin shares policy fingerprints with both President George W. Bush’s plumbing of the Russian leader’s soul and President Barack Obama’s unfulfilling reset, even if the “Pale Moth’s” growing rap sheet since those halcyon times makes the recent spectacle hard to stomach.

What is unique about the Trump era is the juxtaposition of his views on the allies and Russia. The natural correlation is something akin to the Cold War and Obama’s second term: The United States is harmonious with NATO and frosty with Moscow. Disagreements with France and Germany about the 2003 invasion of Iraq occasioned another possibility whereby the United States is at cross-purposes with both sides. Obama’s first term was characterized by a Medvedev-inspired bonhomie with Moscow that was palatable as long as relations with the allies were equally durable. Trump has introduced the final option: threatening estrangement with traditional allies while currying favor with a Russia clearly hostile to U.S. interests. It is this dynamic, among others, that is most responsible for the disconsolation of America’s foreign policy elite.

Yet this unusual state of affairs is more histrionics than a deliberate policy course correction. Even holding out the quixotic possibility that Putin is willing and able to support some of Trump’s foreign policy goals (or, heaven forbid, electoral aspirations), there is no reason this should come at the expense of cordial relations with the Europeans. Unless, the logic goes, that is the price of Russia’s help, or more sinisterly, that Putin can otherwise manipulate Trump’s actions. The former requires malice aforethought inconsistent with most evidence about how the president operates. The chances of the latter, however implausible, are non-zero, and should Mueller find hard evidence to suggest anything of the sort, we would find ourselves in a scandal so serious as to make these matters quaint. In any case, the Congress, a substantial portion of American public, and Trump’s post-Flynn national security officials have all resisted any quid pro quo with Moscow that undercuts our allies. Which leads me to the conclusion that Trump’s enigmatic stance toward NATO and Russia is unlikely to change unqualified American support for the alliance, even when his public actions suggest otherwise. That Mattis and Secretary of State Rex Tillerson have attended regular ministerial meetings, that NATO’s secretary general has visited the White House, and that Trump himself has shuffled off to Brussels like his predecessors before him lends credence to the theory that practical cooperation with the alliance continues apace — in ways often directly in conflict with Russian interests.

Vapid, Vexing, Valuable

As a young Pentagon staffer, I was seconded to Brussels for a few months in 2003 to work at the U.S. Mission to NATO. Naturally excited and looking to make a positive impression, I rushed to backbench a NATO committee meeting at the first opportunity. The topic, I vaguely recall, was related to NATO capability development. I remember the imposing conference room, the translation booths, the flags, and the bevy of well-tailored colleagues from around Europe. I can still conjure the anxious pride of sitting behind the placard stamped “United States” for the first time. This was a dream. About 20 minutes later, it literally became one. I had to repeatedly stab myself in the leg with a pen in order to prod my jet-lagged body into consciousness. I could not have imagined, until that moment, how detailed and dull the daily discourse of NATO often is. And lest you are unconvinced by this reminiscence, I highlight a former secretary of defense’s habit of doing crossword puzzles during NATO meetings or the Weekend at Bernie’s jokes, prominent among senior Obama officials in the Pentagon intended as a metaphor for an alliance seen as moribund.

Moreover, NATO, like any large institution (hello Pentagon!), is raft with dysfunction and internal contradictions. My particular hobby horse is NATO’s requirement for defense spending. Not that, infamously, only a handful of members will ever meet the 2 percent of GDP target, but that in spite of this obvious reality, NATO continues to promote the 2 percent goal as one of its core principles. In high school, I worked summers at a drugstore where the staff would take turns getting lunch for the group. One weekend, I arrived at the chosen spot, order in hand, to be told that because of a delivery issue, the establishment was not serving beef. Incredulous, I proclaimed, “but you’re Burger King.” I likewise imagine a generation of earnest transatlantic scholars staring at their textbooks, perplexed and mumbling, “but you’re the 2 percent people.” To brand your organization with a characteristic that it will never realize takes a chutzpah that Trump can appreciate, but is nonetheless marketing malpractice of the first order. Compounding this folly, Greece, whose military is antiquated, bloated, and oriented toward conflict with another NATO ally, is championed alongside the formidable militaries of the United States and the United Kingdom because it meets the 2 percent threshold. NATO crediting Greece for its military spending is tantamount to House Stark thanking House Frey for hosting the Red Wedding. There are better ideas out there.

Nevertheless, I come here to praise NATO, not to bury it. I detail the aforementioned grievances to assure anyone reading this that those of us experienced in the alliance’s mysterious arts are not ignorant of its problems. Much of our work, over many years, has been dedicated to fixing or mitigating them. And that same experience allows us to appreciate the benefits that NATO membership accrues to the United States. The cynical nature of our times and politics makes it easy to criticize an organization like NATO, whose day-to-day work does not translate readily to the masses. Even so, to have well-founded frustrations with an elaborate and esoteric bureaucracy is one thing. To conclude such an organization is unworthy of American participation or investment is another. Such a posture is at best impetuous and at worst antithetical to the cause of “America First” that NATO naysayers are intent on restoring.

At its core, NATO is a culture of intensive, banal cooperation. It is a swanky headquarters building with Euro-looking conference rooms and passable coffee where mundane meeting after mundane meeting takes place on logistics, standardization, and capability development. It is command centers and watch floors and training areas where alliance militaries practice the monotonous regimens so critical to the science of arms. It is the Alliance Command Transformation — A.K.A. the really boring part of NATO — where the agonizing particulars of interoperability and doctrine are worked out. It is the operational realization of the inane political aspiration to cram soldiers from 14 different nations into a single brigade. It is a collection of customs and habits that dictate how decisions will be made when the balloon goes up. It prescribes where to meet and the rules for discussion. It ensures that you can trust the colleague next to you because you’ve worked with her in such a setting a hundred times before. It structures discourse and operations such that, by ritualizing behaviors and in making a thousand minor decisions, you build the blocks of strategic dexterity that NATO sometimes demonstrates.

The most poignant example I can point to of NATO’s potential is its mission in Afghanistan. Over 15 years, and two distinct American administrations, the United States, through this tool called NATO, coaxed more than a quarter of the world’s countries to participate in a far-flung and elusive mission that had nearly nothing to do with their own national interests. That political feat, however, is rivaled by the operational one, where NATO allies and partners sustained overlapping security, capacity-building, and counter-insurgency missions across an enormous geographical expanse for nearly a decade and a half. The complexity of military operations is often undersold to the public in popular characterizations of war, not to say anything about war by a coalition of militaries measurably different in size, capability, and aptitude. That something the scope, scale, and duration of the International Security Assistance Force (ISAF) was ever realized is rather breathtaking. We could, and should, argue about the strategic success of ISAF, and the costs, and whether it would have been easier operationally had United States gone it alone, but those are different debates. To appreciate ISAF is to recognize the nameless technocrats and servicemen who, through muted craftsmanship, navigated cranky parliaments and inordinate logistical puzzles to achieve a political and operational tour de force. This NATO — obscured to the public and the politicians that charge it with obsolescence — substantiates a faith in the power of process that would make Sam Hinkie smile.

Fashionably Old-Fashioned

Ask some Middle East or Asian security experts about NATO and they inevitably roll their eyes. That old thing. But have a deeper conversation about how they are going about defense cooperation in their regions and you quickly recognize what they want, however impractical, is NATO in all its blessed, bureaucratic glory. Like vegetables to a child, NATO is never what you want, but usually what you need. If you are a purveyor of soft power, NATO should be your thing. Where else can you force common purpose and consensus on scores of dissimilar nations by wont of incessant badgering (i.e., pretty much the job of American officials at NATO)? If you are a hard-power type, I remind you again of ISAF and the fact of 52 militaries operating with solidarity to impose their martial will. In either case, you begin to understand Vladimir Putin’s hostility toward the alliance — of what it is and what it could be should it ever have occasion to turn its withering gaze to Moscow. Is Putin’s disdain not proof itself of NATO’s indomitable relevance and potency?

Ultimately, I suspect Putin’s paranoia is both about the methodical reach of alliance hard power into his perceived sphere of influence as well as the fact that that alliance nations, on the whole, aspire to live in a world defined by classic liberal values. Putin begrudges not only NATO’s endurance and adaptability, but the goody-two-shoes Western order it represents. He certainly delights in Trump’s anti-liberal tendencies and hopes they will weaken NATO, but recognizes they are unlikely to change its deep-rooted puritan culture. To wit, consider again the 2 percent issue. In a world obsessed with image and status, any number of European defense officials fight to maintain the target because it is useful for keeping pressure on their own parliaments and politicians for increased defense spending. That is, the alliance chooses to look impotent in an attempt to do the right thing rather than revise its blueprint to look better. NATO, bless its heart.

#### Any other interp unlimits the topic---joint science diplomacy, anti-corruption, arms control, intelligence coop, and every other collaborative policy becomes topical--- overstretches the neg research burden and undermines preparedness for all debates

### NATO---Core Military Limits---2NC

#### Here’s just a small sample of the broad areas they expand the topic to include:

NATO ’21 [North Atlantic Treaty Organization; Aug 25; “Partnerships: projecting stability through cooperation,” https://www.nato.int/cps/en/natohq/topics\_84336.htm?]

Through partnership, NATO and partners also pursue a broad vision of security:

integrating gender perspectives into security and defence;

fighting against corruption in the defence sector;

enhancing efforts to control or destroy arms, ammunition and unexploded ordnance;

advancing joint scientific projects.

Partnership has evolved over the years, to encompass more nations, more flexible instruments, and new forms of cooperation and consultation.

### NATO---Political/Military Alliance CI---2AC

\*Also AT: No Partnerships

#### NATO is both a political and military alliance with four core activities: consultations; operations; partnerships; and developing threat response

Weaver ’21 [John Michael; 2021; Associate Professor of Intelligence Analysis at York College of Pennsylvania (USA), a retired DOD civilian from the United States' Intelligence Community, and has served as an officer in the US Army (retiring at the rank of lieutenant colonel); *NATO in Contemporary Times: Purpose, Relevance, Future*, Palgrave Macmillan]

NATO is both a political and a military Alliance that exists to guarantee the security and freedom of its members with both political and military means. Politically, NATO seeks to promote democratic values and empower member states to consult and collaborate on both security and defense-related issues to solve problems, build trust, and prevent conflict in the long run (What is NATO, n.d.). Militarily, NATO is committed to peacefully resolving disputes. If diplomacy fails, NATO has the military power to commence crisis management procedures. These can be carried out under a United Nations mandate or Article 5, which is the collective defense clause of NATO's founding treaty. Military operations can be conducted alone or with other countries and international organizations (What is NATO, n.d.).

2.3 MISSION

NATO is an Alliance of countries from North America and Europe that serves as a link between the two continents. This enables cooperation and consultation in the areas of defense and security, and it has the ability to conduct multinational crisis management operations (What is NATO, n.d.).

2.3.1 North Atlantic Council (NAC)

NATO's North Atlantic Council (NAC) is the epicenter of the Alliance's decision-making body (NAC, n.d.). It is also responsible for helping to create strategic guidance in an imperfect world (Dorff 2014). Accordingly, the NAC unites representatives of each Alliance nation to discuss policy or operational questions that require collective decisions, to foster a forum for full range consultation among members on all issues that affect their peace and security (NAC, n.d.). As a political organization, NATO develops policy to respond to changing conditions in the political-military domains under political guidance (AJP-01 2017,1-1). Accordingly, policy is seen as prescriptive and can better assign or direct tasks and capabilities (AJP-01 2017, 1-1). Moreover, the Alliance's strategic framework helps link national power to the political system of international actors (under NATO), to support collective interests (AJP-01 2017, 1-3). It often does so through the application of the instruments of national power (diplomatic, information, military, and economic or D.I.M.E.) (AJP-01 2017, 1-3-1-4; M0ller 2014; Nissen 2014,159; Weaver 2018a; b; Weaver 2019; Weaver 2020a, b; Weaver and Johnson 2020).

Under D.I.M.E., diplomatic efforts look at the engagement of political entities and how effective they are at brokering agreements and negoti-ating terms with other countries (AJP-01 2017, 1-3). The information instrument is paramount for the decision-maker to have the facts and data necessary to make timely decisions and the synchronization of messaging is critical for the Alliance's legitimacy (AJP-01 2017, 1-3). The military instrument looks to the availability of armed forces of different nations (air, ground, sea, space, and Special Forces), to project power as necessary (AJP-01 2017, 1-4). Finally, the economic instrument turns to capital and trade to exercise monetary influence over state and non-state actors alike (AJP-01 2017, 1-4).

It is the ultimate authority that heads a network of committees and its discussions and decisions cover a host of NATO activities and are often based on recommendations and reports developed by subordinate committees, at the NAC's request (NAC, n.d.). Policies that are decided in the NAC represent the collective will of all member countries from within NATO because those decisions are made based on unanimity and common accord. Likewise, the Secretary General chairs the NAC; deci-sions taken by it have the same status and validity at whatever level it meets (NAC, n.d.). Most importantly, the NAC was the only body estab-lished by Article 9 of the North Atlantic Treaty and remains the only one with the authority to set up subsidiary bodies (NAC, n.d.).

2.3.2 Nuclear Planning Group (NPG)

Many of the nations in NATO possess nuclear weapons (France, United Kingdom, and the United States). This group is charged with discussing a specified policy that gravitates around nuclear forces in a changing world and serves as the senior body on nukes for the Alliance; specific emphasis is on arms control and nuclear proliferation and has existed since 1966 (NPG, n.d.). Though all NATO members are de facto members of the NPG, France has opted not to participate. The senior component charged with nuclear issues is the NPG High Level Group (HLG) and it is chaired by the United States. The HLG tends to the issues of NATO's nuclear policy, planning and force posture, as well as the security, safety, and the monitoring of the effectiveness of NATO's nuclear deterrence (NPG, n.d.).

2.4 NATO MILITARY ORGANIZATION AND STRUCTURE

NATO will always look for political solutions first. However, when NATO's execution of political decisions has military implications, there are several key actors. This includes its Military Committee (Johnston 2017, 60-61). This is comprised of the Chiefs of Defense of NATO member countries. It also includes the International Military Staff, and NATO's Military Committee's executive body (What is NATO, n.d.). Finally, the military command structure is made up of Allied Command Operations (ACO) and Allied Command Transformation (ACT). Accord-ingly, NATO can turn to the military structure to influence political outcomes (Hudson 2009).

It is important to note that NATO has very few permanent forces of its own (several of these will be covered in subsequent chapters). At such times when the NAC agrees to launch an operation, member nations voluntarily contribute military forces. These forces are then returned to their nations upon mission completion (What is NATO, n.d.).

2.5 NATO ACTIVITIES

The Alliance can be seen as a significant enabler (Jakobsen 2014). NATO is engaged in four basic activities. These include (1) decisions and consultations, (2) operations and missions, (3) developing partnerships, and (4) developing the means to respond to threats (What is NATO, n.d.). It is incumbent upon the political leaders to craft strategic narratives to come up with a shared meaning of politics to more aptly shape beliefs, perceptions, and behavior (Miskimmon et al. 2011).

The first of these is decisions and consultation. What is important to understand is that a decision by NATO is taken by consensus. Moreover, daily, member nations consult with one another and take decisions on issues of security on a wide mix of issues (What is NATO, n.d.).

NATO is involved in multiple missions and operations the world over. More pointedly, these include recent operations in Afghanistan and Kosovo (Shea 2014), air policing, humanitarian relief operations, pandemic support (COVID-19), its interest in securing the Mediter-ranean, and NATO's support to the African Union (Operations and Missions, n.d.; What is NATO, n.d.). Accordingly, it leads as a contrib-utor to peace and security on multiple continents. The Alliance is a crisis management organization with an ability to handle full spectrum opera-tions (Johnston 2017, 139; Operations and Missions, n.d.). These have increased substantially since the 1990s (Operations and Missions, n.d.).

NATO is engaged in building partnerships (What is NATO, n.d.). In addition to the 30 member nations, 40 others collaborate with the Alliance on a wide range of security and political issues and this has led to many non-NATO members contributing resources and troops to Alliance operations in many countries.

Finally, NATO is involved in developing capabilities to respond to threats (What is NATO, n.d.). Since the collapse of the Soviet Union and the subsequent end of the Cold War, it has turned to innovation and adapted to emerging conditions and subsequent threats. These include the likes of special operations, intelligence, cyber, and contingency contracting in recent years. Under the NATO Crisis Management Process (NCMP), NATO personnel staff and committees put together options for the NAC (AJP-01 2017, 3-5).

#### NATO is both a collective defense AND a collective security organization.

Krause and Singer ‘1 [Volker and David; 2001; Professor of Political Science at Eastern Michigan University; Professor of Political Science at the University of Michigan, Ph.D. from New York University; Federal Ministry of Defense of Austria, “Minor Powers, Alliances, And Armed Conflict: Some Preliminary Patterns,” p. 14]

Collective Defense and Collective Security

A formal military alliance usually has the purpose of collective defense, which means that its members pool their capabilities and attempt to make a collective effort to protect one another against possible military aggression by a clearly specified adversary outside the alliance. Very often, however, an alliance offers not only collective defense but also serves the function of collective security. Under collective security, allies protect one another against possible military aggression by any one potential adversary within the same alliance. The differentiation between collective defense and collective security may be illustrated by the example of NATO. During the Cold War, NATO was mostly associated with collective defense against possible military aggression led by the Soviet Union, a clearly specified adversary outside the North Atlantic alliance. It should also be noted, though, that NATO also provided, and still provides, collective security against possible military aggression by any one potential adversary among its signatories. Given that German armed aggression has culminated in two world wars, NATO has played a critical role in protecting its signatories against the possibility of renewed German militarism while at the same protecting the security interests of its member Germany.

### NATO---Informal Cooperation CI---2AC

#### US ‘cooperation with NATO’ includes informal channels for which there are explicit and purposefully created frameworks for deliberation, exchange, and joint action---that limits out unintentional norm diffusion---and it’s crucial to aff ground---any other interp is hopelessly outdated

Eilstrup-Sangiovanni ’14 [Mette; 2014; Lecturer in International Studies at the Department of Politics and International Studies at the University of Cambridge, UK; “Informal cooperation beyond the alliance,” in NATO’s Post-Cold War Politics, Palgrave Macmillan, London]

A large literature charts NATO's post-Cold War transformation from a close-knit, defensive alliance to a more versatile, multifaceted security organization. This literature focuses mainly on changes to the formal institutional makeup of the Alliance, such as the adoption of new Strategic Concepts, inclusion of new member states, and reform of command and decision procedures. Less analytical attention has been paid to changing patterns of informal cooperation within and around the Alliance. Indeed, while scholars have identified a growing tendency to supplement formal NATO cooperation with ad hoc, flexible forms of collaboration this tendency is often cited as a sign of disintegration of the Alliance (for example, Noetzel and Schreer 2009) rather than an integral part of NATO's post-bipolar institutional practice, which is conducive to the continued functioning of the Alliance.

This chapter focuses explicitly on forms of informal cooperation involving NATO members, but occurring beyond the official institutional boundaries of the Alliance. Perhaps the most visible instantiation of ad hoc, informal cooperation are the short-term 'coalitions-of-the- willing' that have brought together NATO and non-NATO countries to intervene militarily in places such as Afghanistan and Iraq. However, 'extramural' security cooperation also takes other, less visible forms, including Anglo-American special intelligence-sharing, the G8's informal Counter-terrorism Action Group or the US-led Proliferation Security Initiative (PSI). What characterises these initiatives is that they bring together prominent NATO members (often in concert with powerful third-party states) in order to address issues that fall generally within the institutional scope and mandate of NATO but that are nonetheless pursued outside the formal institutional boundaries of the Alliance.

In what follows, I adopt a broadly rational institutionalist approach to explore factors that may encourage greater reliance on informal cooperation among NATO members. Assuming that shifts in institutional design and practice are primarily explained by reference to the changing incentives of dominant member states, I focus mainly on the role of the US in initiating informal cooperation.

I advance three arguments. Firstly, growing reliance on ad hoc cooperation is driven by systemic changes in the post-bipolar strategic environment, which place more diverse and less predictable demands on military resources - especially those of the US - than was the case during bipolarity. These changes have generated demand for flexible forms of cooperation, which allow allies to enlist the capabilities and expertise of third-party states on a case-by-case basis. Secondly, a new strategic focus, combined with a rapid expansion of membership, has resulted in a broadening of NATO's institutional scope and mandate and in enhanced centralization of decision-making. This process of 'internationalization' and 'institutionalization' has in turn served to push some issues outside the formal boundaries of the Alliance where institutional constraints on decision-making remain low. Thirdly, the end of bipolar- ity has shifted the balance of power among NATO members further in favour of the US, thereby reducing Washington's incentives to provide institutionalized voice opportunities or assurances to European allies. This has reinforced the inclination by the US to evade NATO's formal institutional constraints.

To focus my analysis, I examine cooperation on non-proliferation as a lens through which to illuminate broader changes in cooperation within the Alliance. Non-proliferation is a central component of America's post- Cold War security strategy. Yet, Washington has shown considerable reluctance in channelling core aspects of its global non-proliferation policy through NATO. Instead, ad hoc initiatives such as the PSI and the Cooperative Threat Reduction Program have been focal points for cooperation between the America and its NATO allies. The rest of this chapter seeks to illuminate why this has been the case.

Formal and informal institutions in international relations

Although informal institutions have attracted growing attention from IR scholars, there is little agreement on what separates informal from formal structures. Often, informal institutions are defined simply as agreements that lack binding force (that is, 'soft law') or more broadly as agreements enforced by unwritten conventions or norms of behaviour (see Brie and Stolting 2011: 19-20). By contrast, formal institutions are generally characterized by being to some degree legalized. International lawyers define legalization in terms of 'obligation' (implying that actors are bound by a rule or commitment under international law), 'precision' (implying that rules are detailed and precise), and 'delegation' (meaning that third parties are granted authority to implement, interpret, and apply the rules of agreements as well as to resolve disputes) (Abbott et al. 2000). In practice, of course, few international agreements impose detailed legal obligations on states or delegate significant authority to institutional agents to implement agreements or adjudicate disputes. However, we may think of formal institutions as agreements and practices that are instituted according to rules and procedures, which are recognized as legal in clearly defined contexts (Brie and Stolting 2011: 19). Such agreements tend to be written down in detailed documents specifying the precise obligations of state parties.

Informal institutions or agreements, conversely, exhibit low levels of legalization. They are typically not constituted by treaty or executive degree, and the rules that govern interaction are neither legally nor pro- cedurally binding on states. Informal agreements may be unwritten. Even when written, rules and objectives tend to be stated in vague, general terms that make them open to broad interpretation. A further difference pertains to the mode of decision-making. While formal institutions are often configured as representative organizations where official votes are taken and majority rule may apply, informal institutions tend to rely purely on deliberation and consensus-seeking without formal voting taking place.

When conceptualizing informal cooperation, it is helpful to distinguish two views of informal institutions according to how they emerge and what their relationship is to formal institutions. The first describes informal institutions as indigenous to formal institutions. On this view, informal institutions comprise social interactions that occur 'alongside formalized interactions in international organizations' (Brie and Stolting 2011: 20; Helmke and Levitsky 2004: 726). These informal institutions (conventions, norms of behaviour, stable expectations) are not consciously shaped and controlled by actors but arise endogenously from exchanges within formal frameworks (Helmke and Levitsky 2004: 730). They tend to complement zand strengthen formal institutions by creating incentives to comply with formal rules.

The second conceptualization views informal institutions as exogenous to formal institutions. On this view, informal institutions comprise explicit rules, norms, and decision-making procedures (written or unwritten) that arise outside officially authorized channels. In contrast to indigenous informal institutions, this second kind of informal institution is deliberately created and maintained by actors for the purpose of achieving joint political objectives.

In this chapter, I am interested in the second kind. Thus, I define informal institutions as explicit and purposefully created frameworks for deliberation, exchange, and joint action. Such informal institutions may stand in different relationships to formal international organizations. Sometimes, informal institutions may arise alongside the official decision-making bodies of IOs in order to improve their functioning. An example is the exclusive 'negotiating clubs' that operate within many IOs, where powerful member states debate issues informally before they are considered jointly with other members (Conzelmann 2011: 221-222). Gegout (2002) describes how a 'Quint' consisting of the US, Britain, France, Germany, and Italy conduct unofficial negotiations on EU foreign policy issues before they are placed before the Council. Elsewhere in this volume, Mayer and Theiler draw attention to informal aspects of NATO cooperation, which include regular lunches dur-ing which national representatives conduct off-the-record discussions. Such 'negotiating clubs' are mostly complementary to official decision- making structures. Although they operate without a formal institutional mandate, and although they favour representation from larger states, informal negotiation clubs are a prerequisite for consensus-building and effective implementation in many large IOs. They provide the 'oil', so to speak, that makes the heavy machinery of formal organizations turn.

Informal institutions may also operate independently and partly in contradiction of existing IOs. In this case, rather than complementing formal frameworks for decision-making and implementation, informal frameworks may emerge with the explicit purpose of sidestepping or subverting formal decision processes. The coalitions of the willing that fought in Iraq and Afghanistan provide an example. Military action by these coalitions was not ancillary or complementary to official deliberation and action by NATO. Rather, these coalitions presented alternative sites for cooperation that bypassed NATO altogether.

### NATO---AT: “Only Article 5”---2AC/1AR

#### NATO isn’t just Article 5---Article 3 and 4 requirements require training and consultation, and emerging tech requires non-Article 5 activities

Brady ’13 [Colonel Brian H. Brady; October; Judge Advocate, U.S. Army assigned to the Defense Intelligence Agency Office of General Counsel Operations, former staff legal advisor (LEGAD) in the Office of the Legal Advisor, North Atlantic Treaty Organization (NATO), Allied Command Transformation, Joint Warfare Centre; 2013 Army Law. 4, “The North Atlantic Treaty Organization Legal Advisor: A Primer,” Department of the Army Pamphlet 27-50-485, lexis]

II. NATO Legal Authority

The North Atlantic Treaty Organization is a creation of international agreement. A mosaic of international agreements establishes the NATO Alliance, states its mission, and grants privileges and immunities to its subordinate elements. The next section provides an overview of some of these key agreements.

A. North Atlantic Treaty of 1949

The North Atlantic Treaty, also known as the Washington Treaty, establishes NATO legal authority, organization, and function. 11 NATO is both a political entity and a military entity. NATO's political leader is the Secretary General (currently Mr. Anders Fogh Rasmussen, a Danish citizen), while its military leader is the Supreme Allied Commander Europe (SACEUR) (currently U.S. Air Force General Philip M. Breedlove). The treaty establishes both a political and military role for the organization.

1. Core Mission and Article 5

Article 5 of the treaty states the core mission of NATO. 12 This mission is based upon article 51 of the UN Charter, which provides for collective self-defense. Article 5 states as follows:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. 13

NATO invoked the provisions of article 5 to the treaty for the first time in the aftermath of the 11 September 2001 attacks on the United States. 14 NATO Operation Active Endeavor (naval operations in support of 9/11 counterterrorism missions in the Mediterranean) was one of the first NATO operations authorized under article 5. 15

2. Non-Article 5 Activity

Not all NATO military activity can be justified under article 5 to the treaty. NATO member states 16 have an obligation to train and prepare for their defense. This is articulated in article 3 to the treaty. 17 The political aspect of NATO is reflected in the article 4 requirement that parties consult one another to resolve disputes or identify potential threats to the alliance. 18 These authorities have been interpreted to give NATO its own engagement activity (mirroring the activity of a U.S. combatant command), such as the Partnership for Peace and the Mediterranean Dialogue. 19 While article 5 is a good start point in articulating the legal basis for traditional NATO operations, the LEGAL) may also refer to underlying United Nations Security Council Resolutions (UNSCR) giving authority to engage in armed conflict under Chapter VII of the UN Charter. 20 In this light, NATO doctrine provides for operational responses beyond article 5 self-defense.

To address the multitude of security scenarios facing the alliance, NATO doctrine recognizes a category of activity known as Non-Article 5 Crisis Response Operations (NA5CRO). 21 Non-Article 5 operations cover contingencies that do not amount to a response to an armed attack on alliance territory. 22 The earliest example of this type of operation includes the NATO-lead of the Implementation Force (IFOR) in Bosnia-Herzegovina. 23 The doctrine states as follows:

NA5CRO range from support operations primarily associated with civil agencies through operations in support of peace, countering irregular threat activities, to combat . . . this could include, but is not limited to, extraction operations, tasks in support of disaster relief and humanitarian operations, search and rescue (SAR) or support to non-combatant evacuation operations (NEOs), freedom of navigation and overflight enforcement, sanction and embargo enforcement, support to stabilization and reconstruction activities, peace enforcement (PE), and counterinsurgency (COIN). 24

3. Organizational Authority Under Article 9

The North Atlantic Treaty establishes the North Atlantic Council (NAC). 25 All NATO entities owe their base authority to some action taken by the NAC. As part of NATO's basic functions, the NAC establishes subsidiary bodies which include political, military, and other organizational entities within NATO. On the military side, the NAC established the Military Committee (MC), which provides direction and guidance on military policy and strategy. 26 The MC is supported by its International Military Staff (IMS). Among other things, the NAC approves rules of engagement (ROE) and target lists for specified NATO operations. 27

The NAC is chaired by the Secretary General of NATO (Mr. Anders Fogh Rasmussen), who builds consensus within this political and military body. The Secretary General is supported by the International Staff (IS) who works NATO's political agenda.

The NAC is also empowered to establish a form of subsidiary body that is now known as a NATO Agency. 28 NATO Agencies are the executive body within a subsidiary body. 29 NATO agencies include such entities as the NATO Standardization Agency (NSA), NATO Mamtenance and Supply Agency (NAMSA), and the NATO Communications and Information System Services Agency (NCSA). 30 Soldiers who eat at a NATO dining facility on the NATO-operated part of Kabul International Airport (KAIA) eat meals that were contracted and paid for by a NAMSA.

#### “Defense-only” interps badly misunderstand NATO’s evolution over time---Article 5 is irrelevant---US coop with NATO on emerging tech is necessarily political, not military

Weaver ’21 [John Michael; 2021; Associate Professor of Intelligence Analysis at York College of Pennsylvania (USA), a retired DOD civilian from the United States' Intelligence Community, and has served as an officer in the US Army (retiring at the rank of lieutenant colonel); *NATO in Contemporary Times: Purpose, Relevance, Future*, Palgrave Macmillan]

The political aspects that the NATO diplomats bring is essential for the success of the Alliance; diplomacy itself is an instrument of power and one that is critical as a "soft" component to bring about influence in the world (Weaver 2018a; Weaver 2018b; Weaver 2020; Weaver and Pomeroy 2018; Weaver and Pomeroy 2019, 2020; Weaver and Johnson 2020). To be effective and to remain relevant, it must look to clearly articulate objectives to NATO commanders at all levels (Kruger-Klausen and Odgaard 2014). The Alliance also helps enable nations like the United States to leverage others to minimize the burden of being the sole bearer of the problem while adding legitimacy to the mission (Jakobsen 2014, 5). What's more, is that NATO can bring together a variegated mix of capabilities that single nations might lack (Jakobsen 2014, 60).

Similar to the United Nations, it is frequently quite challenging to come to commonly acceptable terms due to the disparate mix of nations each with their own agendas to help maintain their relevancy and position on the global stage (Geoana 2020). It is not easy to realize consensus and when looking at divides between individual nations, like the United States and France (cultural differences), Greece, and Turkey (a history of hostility), and divisions between larger members like the United States and the European Union, the United Kingdom and the European Union (over Brexit), and many NATO nations and Turkey (due to Turkey's move towards a closer relationship with Russia), and one can quickly see how challenges abound for the political leaders of the Alliance.

That stated, diversity is often a good thing. It brings in new experiences, leads to better problem-solving, and offers additional perspectives.

Working in diverse environments also promotes creativity and opens up the dialogue to innovative ideas. Looking at problems through different cultural lenses can add value, might assist in conflict avoidance, and even lead to greater legitimacy especially if there is a move afoot to gravitate toward the direction of armed conflict or intervention. The addition of more members and the collaboration of countries in recent years and into the future will further increase NATO's diversity, give NATO leaders more cultural lenses to look through, and help avoid groupthink.

Because NATO is a political organization first and foremost, the civilians that serve as the head of this Alliance are probably going to be more inclined to look to diplomatic efforts to help avoid the employment of military forces. NATO Deputy Secretary General Mircea Geoana (2020) underscored the importance of NATO's political influence in a panel discussion when he underscored the necessity of NATO to expand its political influence while trying to limit formal expansion to leverage (1) that no other alliance has a greater sharing of values than NATO, that (2) NATO countries possess 50% of the world's Gross Domestic Product (GDP), and that the Alliance holds over 50% of the world's military power. This is important because NATO (the NATO Command Structure or NCS) has few permanent military forces itself and this is a weakness. NATO depends on member countries to contribute military forces, if and when needed. While NATO does maintain some military equipment, most equipment is contributed by member nations to support their military personnel (NATO Troop Contributions 2018). This can directly correlate into issue resolution for NATO as a whole and reduce the costs associated with member nation contributions of troops at the individual nation level.

Another weakness is that NATO heavily relies on member contributions for funding, and it is not entirely balanced. Additionally, NATO provides political and financial oversight for any jointly funded projects among member nations. Some countries have to spend more in order to develop additional capabilities for which the Alliance asks (cyber, communications, stand-off weapons, etc.) (NATO Funding, n.d.). NATO also relies on the United States for some essential operations, such as ballistic missile defense, airborne electronic warfare, and air-to-air refueling. However, the United Kingdom, France, and Germany contribute more than 50 percent of the non-defense spending (NATO Funding, n.d.).

That stated, each country will probably not see the solution that they would like brought to fruition that they would prefer. Consensus is rarely possible when multiple parties from diverse backgrounds are involved. Compromise will likely occur with each NATO member advocating for their preferred course of action, and the actual decision becoming "watered down" because not all nations will agree with individual member recommendations. The ability of NATO members to keep an open mind, work together, and compromise is vital for NATO's success.

NATO leaders will have to continue to adapt to a quickly changing world. Having strong allies outside of NATO aids in foreign policy negotiations and helps reduce the risk of military conflict and this is an opportunity. The member nations will have to ensure they can form agreements within NATO and with its partners. For NATO to remain relevant, especially in the context of its burgeoning 30 member states, Alliance members will have to put aside differences and look to a utilitarian approach to solving problems at the top for this supranational organization to remain relevant in the future.

There are threats. When turning to cyber, issues regarding cyber network operations are burgeoning and becoming more problematic (Weaver and Johnson 2020). Cyberspace has been designated as its own military domain, separate from land, air, sea, and space (NATO 2020). The Deputy Secretary General stated that NATO agreed to create a Cyberspace Operations Center in the military command structure (NATO 2020); what is needed is a clear understanding of the effects that the NATO SECGEN wants to achieve so that it can be task organized accordingly. It has also been noted that some actors have been exploiting the COVID-19 crisis, and there has been an increase in malevolent cyber activity since it began (NATO 2020). NATO will have to explore its interpretation of whether or not cyber attacks constitute an Article 5 attack. Geoana (2020), also underscored the challenges confronting the expansion of cyber to include artificial intelligence and quantum computing in the years ahead. Moreover, NATO will have to come to understand advanced persistent threats (APTs), the Internet of Things (IOT), the use of "deep fakes" and more when looking at the topic of cyber (Weaver and Johnson 2020).

To achieve success will require partnerships and synchronization to remain relevant. More pointedly, NATO political leaders will have to work with military planners (Kruger-Klausen and Odgaard 2014). The threats facing the Alliance members have drastically changed since it was founded. A military attack from a hostile actor is less likely to occur now than during the Cold War, but Russia still is a concern (Geoana 2020). Other challenges are more in the realms of terrorism, and nuclear proliferation (Geoana 2020). NATO leaders will have to form a clear vision and a formidable strategy to remain relevant to survive (Shea 2014, 41).

Moving forward, NATO will have many challenges. More to the point, NATO Secretary General Jens Stoltenberg has underscored three points. These include (1) remaining strong as an Alliance to remain formidable and keep its edge, (2) looking at how NATO can enhance its political influence even though there will be disagreement at times among NATO member nations, and (3) looking to how NATO becomes even more relevant globally without expanding its formal membership (Geoana 2020). Direction and guidance must be clear. The Alliance must also come to terms with the political realities of what is truly possible and knowing what exceeds the political will of member countries. Once this is understood, NATO as a political entity, can move forward with identifying the ways, means, and ends necessary to achieve what the Alliance wants to accomplish. Finally, NATO should turn to its Emerging Security Challenges Division (ESCD) to look at future threats to the Alliance and determine the best way forward to address these (ESCD, n.d.).

#### Article 5 situations are incredibly rare---most NATO coop occurs under Article 4 and requires building effective partnerships with non-NATO allies

Matlary ’14 [Janne Haaland; 2014; Professor of International Politics at the University of Oslo and at the Norwegian Defence University College, Norway; “Partners versus Members? NATO as an Arena for Coalitions,” in NATO’s Post-Cold War Politics, Palgrave Macmillan, London]

If this is so, then NATO is important as an arena and increasingly so. But the main political dynamic is between the US, on the one hand, and remaining NATO members and partners, on the other. Moreover, if Article 5 contingencies remain unlikely as during the past two decades, then the boundary between members and partners will remain rather fuzzy. Even the border violations from June to November 2012 (of Turkey by Syria) have not resulted in Article 5 invocations by the former, which have twice called for consultations under Article 4. This was also the case when the Turkish border was violated in the 'spillovers' in the run-up to the Iraq war in 2003. At that time, the Turks asked for NATO assistance under Article 4, something which severely split the Alliance. Hence, Article 5 situations are very rare, with September 11, 2001 being an exception when the North Atlantic Council (NAC) declared it an Article 5 but was rebuffed by the US which wanted full control of its response.

My point is simply that absent the threat of inter-state war in the Euro-Atlantic area, most NATO cases will be under Article 4, and thus voluntary. This makes for a political dynamic where those who fight together, stay together. Moreover, the fact that both members and partners find it useful and perhaps necessary to contribute begs the question of why contribute.

The importance of partner contributions

Once, when a small NATO member repeatedly voiced criticism at the NAC, the US ambassador bent over and asked his British counter-part: 'So what do they contribute?'2 In the Alliance, the burden-sharing debate around risk-willingness is the key one after the Cold War, and influence is gained on a one-to-one basis: those that contribute, gain influence, hopefully in Washington, but certainly in a given operation. They may gain security through this, or prestige, or meet national interest needs. Like the partnership policy of the US is a key to American global politics, the same partner concept seems now to develop at NATO. It can be argued that the partners contribute, in order to gain military interoperability, political influence in NATO and political influence in Washington. One may add that this is also why members contribute (Matlary and Petersson 2013).

NATO after Afghanistan is an alliance where the fundamental security contract, Article 5, still underpins the alliance and keeps it together, but where the political dynamics of the alliance have changed in major ways. The realities of coalition warfare have become very clear in terms of the demands for risk-willing, significant military capacities. Some European allies participate in ISAF despite high costs in terms of life and treasure, but many more offer only token participation. States that want closeness to the US must contribute risk-willing, relevant military capacities to global operations. These states are part of the first tier of NATO, the inner circle. As stated, in NATO, states will first and foremost seek closeness to the US. Some states achieve this through their contributions to current operations. Others do not, who then are relegated to the second tier (hence the characterization of NATO as a 'two-tier' alliance).

### NATO---Includes Partners---2AC

#### Predictability---NATO literally defines partnership objectives as a part of ‘NATO’---all other interps are contrived and normative

NATO ’21 [North Atlantic Treaty Organization; Aug 25; “Partnerships: projecting stability through cooperation,” https://www.nato.int/cps/en/natohq/topics\_84336.htm?]

A flexible network of partnerships with non-member countries

Dialogue and cooperation with partners can make a concrete contribution to enhance international security, to defend the values on which the Alliance is based, to NATO’s operations, and to prepare interested nations for membership.

In both regional frameworks and on a bilateral level, NATO develops relations based on common values, reciprocity, mutual benefit and mutual respect.

In the Euro-Atlantic area, the 30 Allies engage in relations with 20 partner countries through the Euro-Atlantic Partnership Council and the Partnership for Peace – a major programme of bilateral cooperation with individual Euro-Atlantic partners. Among these partners, NATO has developed specific structures for its relationships with Russia1, Ukraine and Georgia.

NATO is developing relations with the seven countries on the southern Mediterranean rim through the Mediterranean Dialogue, as well as with four countries from the Gulf region through the Istanbul Cooperation Initiative.

NATO also cooperates with a range of countries which are not part of these regional partnership frameworks. Referred to as “partners across the globe”, they include Afghanistan, Australia, Colombia, Iraq, Japan, the Republic of Korea, Mongolia, New Zealand and Pakistan.

NATO has also developed flexible means of cooperation with partners, across different regions. NATO can work with so-called “30+n” groups of partners, where partners are chosen based on a common interest or theme. At the 2014 Wales Summit, NATO introduced the possibility of “enhanced opportunities” for certain partners to build a deeper, more tailor-made bilateral relationship with NATO. At the same time, Allied leaders launched the “Interoperability Platform”, a permanent format for cooperation with partners on the interoperability needed for future crisis management and operations.

In April 2014, NATO foreign ministers decided to suspend all practical civilian and military cooperation with Russia but to maintain political contacts at the level of ambassadors and above.

Key objectives of NATO’s partnerships

Under NATO’s partnership policies, the strategic objectives of NATO's partner relations are to:

Enhance Euro-Atlantic and international security, peace and stability;

Promote regional security and cooperation;

Facilitate mutually beneficial cooperation on issues of common interest, including international efforts to meet emerging security challenges;

Prepare interested eligible nations for NATO membership;

Promote democratic values and institutional reforms, especially in the defence and security sector;

Enhance support for NATO-led operations and missions;

Enhance awareness of security developments including through early warning, with a view to preventing crises;

Build confidence and achieve better mutual understanding, including about NATO's role and activities, in particular through enhanced public diplomacy.

That said, each partner determines – with NATO – the pace, scope, intensity and focus of their partnership with NATO, as well as individual objectives. This is often captured in a document setting goals for the relationship, which is to be regularly reviewed. However, many of NATO’s partnership activities involve more than one partner at a time.

Partnership in practice: how NATO works with partners

In practice, NATO’s partnership objectives are taken forward through a broad variety of means. Broadly speaking, NATO opens up parts of its processes, procedures and structures to the participation of partners, allowing partners to make concrete contributions through these. In some cases, special programmes have been created to assist and engage partners on their specific needs. Key areas for cooperation are set out below:

Consultation is key to the work of NATO as an alliance and is central to partnerships. Political consultations can help understand security developments, including regional issues, and shape common approaches to preventing crises or tackling a security challenge. NATO’s many committees and bodies often meet in formations with partners to shape cooperation in specific areas. NATO Allies meet with partners (individually or in groups) on a broad variety of subjects and at a variety of levels every day.

Interoperability is the ability to operate together using harmonized standards, doctrines, procedures and equipment. It is essential to the work of an alliance of multiple countries with national defence forces, and is equally important for working together with partners that wish to contribute in supporting the Alliance in achieving its tactical, operational and strategic objectives. Much of day-to-day cooperation in NATO – including with partners – is focused on achieving this interoperability. In 2014, recognising the importance of maintaining interoperability with partners for future crisis management, NATO launched the Partnership Interoperability Initiative, which inter alia launched mechanisms for enhanced cooperation with nations that wished to maintain deeper interoperability with NATO.

Partners contribute to NATO-led operations and missions, whether through supporting peace by training security forces in the Western Balkans or monitoring maritime activity in the Mediterranean Sea or off the Horn of Africa. As contributors to those missions, partners are invited to shape policy and decisions that affect those missions, alongside Allies. A number of tools have been created to assist partners in developing their ability to participate in NATO-led operations, and be interoperable with Allies’ forces.

For many years, NATO has worked with partners on defence reform, institution and capacity-building. As part of its work to project stability, NATO Allies have agreed that long-term and lasting stability is linked to improved governance of defence and security sector and institutions. Viable, effective and resilient defence institutions are essential to the long-term success of efforts to strengthen partner capacity. In 2004, NATO Allies and partners adopted the Partnership Action Plan on Defence Institution Building, setting basic benchmarks for defence institutions. In a NATO context, such work can go from strategic objective setting and joint reviews, to expert assistance and advice, as well as targeted education and training. Defence advice and reform is provided through bilateral partnership cooperation programmes, as well as through expert advisory programmes targeting specific aspects of Defence Institution Building, like the Defence Education Enhancement Programme or Building Integrity. In 2014, at the Wales Summit, NATO adopted the Defence and Related Security Capacity Building Initiative (see more below). The Initiative builds on NATO’s extensive track record and expertise in supporting, advising, assisting, training and mentoring countries requiring capacity-building support of the Alliance, and allows for the development of targeted, tailor-made packages of defence capacity-building support for countries, upon request and with Allied consent.

NATO also engages with partners in a broad variety of other areas where it has developed expertise and programmes. These include:

Counter-terrorism;

Counter-proliferation of weapons of mass destruction and their means of delivery;

Emerging security challenges, such as those related to cyber defence, energy security and maritime security, including counter-piracy;

Civil emergency planning.

### NATO---Includes Partners---1AR

#### NATO partnerships are a core part of NATO---that enables broad mechanism diversity

NATO ’21 [North Atlantic Treaty Organization; Aug 25; “Partnerships: projecting stability through cooperation,” https://www.nato.int/cps/en/natohq/topics\_84336.htm?]

The Allies seek to contribute to the efforts of the international community in projecting stability and strengthening security outside NATO territory. One of the means to do so is through cooperation and partnerships. Over more than 25 years, the Alliance has developed a network of partnerships with non-member countries from the Euro-Atlantic area, the Mediterranean and the Gulf region, and other partners across the globe. NATO pursues dialogue and practical cooperation with these nations on a wide range of political and security-related issues. NATO’s partnerships are beneficial to all involved and contribute to improved security for the broader international community.

Partners are part of many of NATO’s core activities, from shaping policy to building defence capacity, developing interoperability and managing crises.

NATO’s programmes also help partner nations to develop their own defence and security institutions and forces.

In partnering with NATO, partners can:

share insights on areas of common interest or concern through political consultations and intelligence-sharing;

gain access to advice and support as they reform and strengthen defence institutions and capacities;

participate in a rich menu of education, training and consultation events (over 1,200 events a year are open to partners through a Partnership Cooperation Menu);

prepare together for future operations and missions by participating in exercises and training;

contribute to current NATO-led operations and missions;

share lessons learned from past operations and develop policy for the future;

work together with Allies on research and capability development.

Through partnership, NATO and partners also pursue a broad vision of security:

integrating gender perspectives into security and defence;

fighting against corruption in the defence sector;

enhancing efforts to control or destroy arms, ammunition and unexploded ordnance;

advancing joint scientific projects.

Partnership has evolved over the years, to encompass more nations, more flexible instruments, and new forms of cooperation and consultation.

#### NATO relies on partners----any other interp wrecks the ability to shape doctrine effectively

Matlary ’14 [Janne Haaland; 2014; Professor of International Politics at the University of Oslo and at the Norwegian Defence University College, Norway; “Partners versus Members? NATO as an Arena for Coalitions,” in NATO’s Post-Cold War Politics, Palgrave Macmillan, London]

In this chapter, I discuss the importance of burden-sharing partnerships with NATO as a development that is, as I argue, symptomatic of the evolution of the Alliance into becoming an arena or platform for coalitions of the 'willing and able'. After the end of the Cold War, we live in an era where armed attacks against one or several Alliance members, obliging others to respond immediately (although not necessarily by military means), have become rare and unlikely. As a result, the organization has increasingly turned into a 'two-tiered' or 'multi-tiered' alliance. Current operations are mostly Article 4 and hence, unlike Article 5 cases, voluntary. This implies that partners, as well as members, may contribute. Moreover, few members seem to be willing and able to make a contribution,1 something that inter alia the Libya operation has shown - only eight allies were actually willing to contribute combat capabilities. In other operations, like ISAF, all members contribute, but only a few with risk-willing capabilities. All 'show the flag', but few are willing and able to contribute to sharp operations that require top skill and risk-willingness.

In NATO's currently valid Strategic Concept, the necessity for a part-nership policy is visibly highlighted: 'The promotion of Euro-Atlantic security is best assured through a wide network of partner relations with countries and organizations around the globe. These partnerships make a concrete and valued contribution to the success of NATO's fundamental tasks' (NATO 2010). The section continues to underline how flexible NATO will be in the time ahead: 'We will enhance our partnerships through flexible formats that bring NATO and partners together - across and beyond existing frameworks' (NATO 2010). NATO is also prepared to give partners in operations a 'structural role in shaping strategy and decisions on NATO-led missions to which they contribute' (NATO 2010, my emphasis).

These are interesting new thoughts about coalition warfare. NATO clearly requires military contributions from its partners, but the same is true the other way round: in return for their contributions to operations, partner governments obtain political influence (Edstrem et al. 2011). The latter is what is 'offered' for the first time in a Strategic Concept in the quotation above. From the perspective of the US, such a partnership policy has been a reality for quite some time. The extensive policy of partnerships is a new way of ensuring political and military strength (Kay 2011). In many ways, NATO seems to be introducing the same kind of partnership policy - the willing and able can contribute to operations, whereas members of the Alliance can opt out, as they are entitled to. A vivid illustration of this on the political level was Germany's abstention on the UNSC resolution on Libya (res. 73/11) along with, inter alia, Russia and China. Although the Libya operation only became a NATO operation after five days, it is nonetheless illustrative of the current degree of a lack of common strategic vision in NATO that a major member did not agree with other close allies in this case. In short, in NATO there is very great variety in politico-strategic thinking today, to the extent that there is hardly anything in common beyond Article 5, and operations reflect this fact.

NATO has come to rely on partners. In ISAF, partners like Australia played key roles in the war-fighting in the South of Afghanistan. The partners that bring substantial military capabilities and economic resources to the table clearly benefit the Alliance. Partners themselves achieve NATO interoperability and close ties at the operational and tacti-cal level, and manage to transcend their neutral stances at home, in their domestic debates, as in the cases of Sweden and Finland, two prominent NATO partners. Neutrality as a policy is almost an 'untouchable' in these countries. But the ability of partnering with NATO has enabled them to redefine neutrality to allow for participation in sharp operations abroad. Thus, there are benefits for NATO as well as for partners.

### NATO---List of Partners---2AC/1AR

#### US cooperation with NATO includes affiliated partnerships: EAPC countries, MD (Mediterranean Dialogue), ICI, partners across the globe, the EU, and UN

NATO ’20 [North Atlantic Treaty Organization; March 27; “Partners,” https://www.nato.int/cps/en/natohq/51288.htm]

PARTNERS

NATO cooperates with a range of international organisations and countries in different structures. Below is a list of these partners with links to web pages on their relations with NATO as well as links to their information servers.

Euro-Atlantic Partnership Council (EAPC)

The EAPC consists of all NATO member countries and the following Partnership for Peace countries:

A picture containing chart

Description automatically generated

NATO's Mediterranean Dialogue

The following seven countries of the Mediterranean region are currently involved:

Table

Description automatically generated

Istanbul Cooperation Initiative (ICI)

To date, the following four countries of the Gulf Cooperation Council have joined:

A picture containing table

Description automatically generated

Partners across the globe

In addition to its formal partnerships, NATO cooperates with a range of countries which are not part of these structures. Often referred to as "Partners across the globe", these countries develop cooperation with NATO in areas of mutual interest, including emerging security challenges, and some contribute actively to NATO operations either militarily or in some other way.

A picture containing table

Description automatically generated

International organisations

In addition to its partnerships with countries, NATO cooperates with a range of international organisations.

United Nations (UN) - http://www.un.org

European Union (EU) - http://europa.eu

Organization for Security and Co-operation in Europe - <http://www.osce.org>

## In

### In---Throughout---1NC

#### “In” means throughout.

Words and Phrases ’4 [Words and Phrases Dictionary; 1904; written by Members of the Editorial Staff of the National Reporter System, citing Joseph Church Helm, Justice on the Supreme Court of Colorado in the case *Reynolds v. Larkin*; Volume 4, “Freeze/Kept,” p. 3445]

As throughout.

In the act of 1861 providing that Justices of the peace shall have jurisdiction 'In" their respective counties to hear and determine all complaints, etc., the word "In" should be construed to mean "throughout" such counties. Reynolds v. Larkin, 14 Pac. 114, 117, 10 Colo. 126.

### In---AT: Throughout---2AC

#### “In” means within the limits of

Webster’s ‘6 [Merriam Webster Online Dictionary, 2006, <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=in>]

Main Entry: 1in

Pronunciation: 'in, &n, &n

Function: preposition

Etymology: Middle English, from Old English; akin to Old High German in in, Latin in, Greek en

1 a -- used as a function word to indicate inclusion, location, or position within limits <in the lake> <wounded in the leg> <in the summer>

#### “In” means within, not “throughout”

Cullen ’52 [Court of Appeals of Kentucky, Commissioner, Court of Appeals of Kentucky, November 13, 1952, Riehl et al. V. Kentucky unemployment compensation commission; the judgment is affirmed. Rehearing denied; COMBS, J., and SIMS, C. J., dissenting, <http://ky.findacase.com/research/wfrmDocViewer.aspx/xq/fac.19521113_0040095.KY.htm/qx>]

We do not find any ambiguity in KRS 341.070(1). It is our opinion that the key word in the statute is the word 'in,' preceding the words 'each of three calendar quarters', and if the word is accorded its ordinary and common meaning, the statute does not require simultaneous employment. According to Webster's New International Dictionary, the word 'in,' used with relation to a period of time, means 'during the course of.' The same meaning, expressed in another way, would be 'within the limits or duration of.' Employing this meaning, the statute says that an employer is subject to the Act if, during the course of, or within the limits or duration of each of three calendar quarters, he had in covered employment four or more workers, to each of whom the required amount of wages was paid. This clearly means that the employment need not be simultaneous. Obviously, the word 'in' does not mean 'throughout' or 'for the entire period of,' because then there would be no point in adding the requirement of the payment of a minimum of $50 in wages. In these times, no worker employed for a full calendar quarter would be paid less than $50 in wages. The appellant seeks to read into the statute the words 'at the same time,' following the words 'had in covered employment'. There is no justification for this, unless the word 'in' means 'during any one period of time in.' We are not aware of any authority for ascribing such a meaning to the word 'in'.

### In---Not Completely WIthin

#### In doesn’t require something to be completely within

Rader, 97 – US Circuit Judge for the Federal Circuit (Foster v. Hallco Mfg. Co., 1997 U.S. App. LEXIS 18989 (United States Court of Appeals for the Federal Circuit July 14, 1997, Decided ).

Next, the district court construed the claim language "in," "within," and "between." Each of these claim construction issues is similar to the interpretation of "between" discussed above in relation to claims 5 and 33-36 The district court construed these words more narrowly than required by the claim language and context. The word "in" does not require that something be completely and continuously inside of something else. The word "within" does not require that something be completely and continuously within something else. Further, as discussed above in more detail, the word "between" does not require that something be completely and continuously between two things.

### In---Enclosed Within

#### In means enclosed within

Smith ’60 [Gen. Am. Indem; Oct 25; Judge for the Supreme Court of Texas; Co. v. Pepper, 161 Tex. 263, 339 S.W.2d 660, 1960 Tex. LEXIS 612, 4 Tex. Sup. J. 79]

The word "in" means inside of, within the bounds or limits of. "In" is defines to mean: primarily, in denotes situation or position with respect to a surrounding, encompassment, or enclosure, indicating being within, as a bounded place, a limited time, an encompassing material. The word "in" is said in its most usual significance and popular use to mean enclosed or surrounded by limits, as in a room. A person may be said to be traveling in a carriage, while alighting therefrom, until he completely disconnects himself and lands.

## One or More of the Following Areas

### ‘Or’ = One or More---2AC

#### “Or” means any of three are fine, or more!

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “Conjunctive/Disjunctive Canon,” Ch. 12]

The conjunctions and and or are two of the elemental words in the English language. Under the conjunctive/disjunctive canon, and combines items while *or* creates alternatives. Competent users of the language rarely hesitate over their meaning. But a close look at the authoritative language of legal instruments—as well as the litigation that has arisen over them—shows that these little words can cause subtle interpretive problems. Although these conjunctions can appear in countless constructions, we have identified six types of sentences in which they most frequently appear in legal instruments.

#1: The Basic Requirement

|  |  |
| --- | --- |
| Conjunctive List | Disjunctive List |
| You must do A, B, and C. | You must do A, B, or C. |

With the conjunctive list, all three things are required—while with the disjunctive list, at least one of the three is required, but any one (or more) of the three satisfies the requirement. Hence in the well-known constitutional phrase cruel and unusual punishments,1 the and signals that cruelty or unusualness alone does not run afoul of the clause: The punishment must meet both standards to fall within the constitutional prohibition.2 The same point holds true for the phrase necessary and proper3 in Article I of the Constitution.

## Artificial Intelligence

### AI---Excludes Semi-Autonomous Weapons---1NC

#### The area of AI excludes semi-autonomous weapons. Prefer DODD 3000.09, which is the only pertinent legal guidance published by any military on the planet. Any other interp opens the floodgates to arms sales affs for any weapon with an autonomous sensor.

Allen ’22 [Gregory; June 6; director of the Artificial Intelligence (AI) Governance Project and a senior fellow in the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C; CSIS; “DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread,” https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread]

While describing a military system as AI-enabled or machine learning-enabled provides useful information, it often remains unclear just what functionality is being provided by AI and how central AI is to the system overall. Suppose, hypothetically, that the F-35 Joint Strike Fighter Program Office decided that it should use machine learning to improve the performance on one of the aircraft’s many different types of sensors. Does that mean that the entire F-35 program, with its more than $8.5 billion in annual spending, is building AI-enabled weapon systems? The DODD 3000.09 update is a good opportunity to formally define “AI-enabled” in DOD policy and to specify how using machine learning does or does not affect the autonomous weapon senior review process.

Confusingly, common usage of these terms differs significantly in other countries. For example, Russian weapons manufacturers routinely refer to their automated and robotic military systems as using AI even if the system does not use machine learning, and they rarely make it clear when it does. Varied definitions complicate international diplomacy on these subjects.

Define how retraining machine learning models will be handled in the senior review process.

A 2019 report from the Defense Innovation Board was memorably named “Software Is Never Done.” Updates, bug fixes, cybersecurity patches, and new features are a critical aspect of managing all modern software systems. However, software updates for machine learning systems are different in nature from traditional software, and perhaps even more important. The “learning” in a machine learning system comes from applying a learning algorithm to a training data set in order to produce a machine learning model, which is the software that performs the desired function. To update the machine learning model, the developers provide a new (usually larger) training data set that more accurately reflects the changing operational environment. If the operational environment changes, failing to rapidly retrain a machine learning model can lead to reduced performance.

Does each software update and machine learning model retraining require an autonomous weapon system to go through the senior review approval process all over again? If so, an already formidable process barrier risks unintentionally becoming an insurmountable one. A more reasonable solution would be for the senior review process to assess and decide upon the acceptability of the process for producing new training data; to test and evaluate procedures for determining whether new software updates are sufficiently robust and reliable; and to explicitly state which potential new features would trigger an additional round of the senior review approval process. This is similar to how the global automotive industry regulates software updates and safety compliance.

Clarify the specific features that formally define an autonomous weapon system.

Despite eight years of negotiations at the United Nations, there is still no internationally agreed upon definition of autonomous weapons or lethal autonomous weapons. DODD 3000.09 does, however, formally define autonomous weapon systems and semi-autonomous weapon systems from the perspective of U.S. policy:

Autonomous weapon system: A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.

Semi-autonomous weapon system: A weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator. This includes:

Semi-autonomous weapon systems that employ autonomy for engagement-related functions including, but not limited to, acquiring, tracking, and identifying potential targets; cueing potential targets to human operators; prioritizing selected targets; timing of when to fire; or providing terminal guidance to home in on selected targets, provided that human control is retained over the decision to select individual targets and specific target groups for engagement.

‘Fire and forget’ or lock-on-after-launch homing munitions that rely on [Tactics, Techniques, and Procedures] to maximize the probability that the only targets within the seeker’s acquisition basket when the seeker activates are those individual targets or specific target groups that have been selected by a human operator.

Notably, machine learning is not mentioned anywhere in these definitions, and that is because machine learning is not always necessary. Traditional software is sufficient to deliver a high degree of autonomy for some military applications. For example, the Israeli Aerospace Industries (IAI) Harpy is a decades-old unmanned drone that IAI openly acknowledges is an autonomous weapon. When in autonomous mode, the Harpy loiters over a given region for up to nine hours, waiting to detect electromagnetic emissions consistent with an onboard library of enemy radar, homes in on the emissions source (usually enemy air defense radar), and attacks. No human in the loop is required.

The critical feature of this definition is that the policy threshold for autonomy relates specifically and exclusively to the ability to autonomously “select and engage targets.” DOD officials talk often about their goals for increasing autonomy in weapon systems, but sometimes they mean increasing weapon autonomy in areas like guidance and navigation. For example, Mike E. White, assistant director for the DOD’s hypersonics office, stated in 2020 that he wanted future DOD hypersonic weapons to use autonomy and AI to “optimize flight characteristics.” Increasing hypersonic weapon autonomy for guidance and navigation is irrelevant from a DODD 3000.09 perspective and relatively innocuous from an international relations perspective, but the DOD should seek to minimize potential misunderstandings—especially about hypersonic weapons that could carry nuclear warheads and have significant implications for global strategic stability. This is an area where the DOD must communicate clearly and precisely.

Clarify the types of weapons that are and are not required to go through the autonomous weapon senior review process.

As mentioned above, DODD 3000.09 does not ban autonomous weapons systems but rather subjects them to additional technical and process scrutiny in the form of a senior review. However, not all weapons systems with autonomous functionality are required to go through the review. The below diagram provides a simplified depiction of what systems must go through the review and which ones are exempted. DOD should publish a similar diagram in a policy handbook to accompany the DODD 3000.09 update.

Diagram

Description automatically generated

### AI---Excludes Semi-Autonomous Weapons---2NC

#### DOD Directive 3000.9 distinguishes between semi-autonomous weapons and fully autonomous ones---none of those exist yet

Cruz ’20 [Jose de Arimateia da Cruz and Stephanie Mae Pedron; 2020; Professor of International Relations and Comparative Politics at Georgia Southern University and Research Professor at the U.S. Army War College; teaching assistant in the Department of Political Science & International Studies at Georgia Southern University; International Journal of Security Studies, “The Future of Wars: Artificial Intelligence (AI) and Lethal Autonomous Weapon Systems (LAWS),” 2:1]

II. Defining AI, Autonomy, and Autonomous Weapons

Debate concerning the expansion of AI has grown more complex in recent years. The language used to depict robots is often ambiguous due to the interdisciplinary nature of the subject. Before delving into the potential advantages and risks of LAWS, it is first necessary to establish a working definition of AI and the related subject of autonomy, which is part of what differentiates LAWS from other autonomous weapon systems (AWS). On February 11, 2019, President Donald J. Trump issued Executive Order (EO) 13859 on Maintaining American Leadership in Artificial Intelligence. EO 13859 states that, "artificial intelligence (AI) promises to drive growth of the United States economy, enhance our [U.S] economic and national security, and improve our quality of life" (Executive Order 13859). On § 9 of EO 13859, artificial intelligence means "the full extent of Federal investments in AI, to include: R & D of core AI techniques and technologies; AI prototype systems; application and adaptation of AI techniques; architectural and systems support of AI; and cyberinfrastructure, data sets, and standards for AI" (EO 13859).

Owing to distinct approaches of research in AI, no universal definition of it exists. However, H.R. 5515 (115th Congress) or the FY 2019 U.S. National Defense Authorization Act (NDAA) does provide a framework for the purpose of the bill. NDAA § 238, defines artificial intelligence as:

(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

(3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.

As outlined above, AI encompasses a range of technologies with assorted capabilities, many of which have the potential to advance military operations in several areas. AI applications for defense are diverse. They have proven useful for reconnaissance and surveillance missions, and have marked potential to speed-up cyberspace operations (Sayler, 2019b). For example, the 2016 Cyber Grand Challenge hosted by the U.S. Defense Advanced Research Project Agency (DARPA) exhibited the budding aptitude of future Al-enabled cyber tools by challenging participants to develop an AI algorithm that could detect and patch software vulnerabilities in seconds instead of months (Fraze, 2016; Sayler, 2019b). Al-enhanced cyber tools have marked potential to detect derived viruses, suspicious nodes in networks, and identify system oddities (Asiru, Dlamini, Blackledge, 2017; Kubovic, Kosinar, & Janosik, 2018). AI technology is also being incorporated into military vessels to communicate with other vehicles, navigate routes, determine distance between vehicles and surrounding objects, and improve safety and vehicle performance. (Canis, 2018). Similarly, offensive applications of AI also vary. They may boost the destructive competencies of legitimate military forces or third party attackers. A hacker group's intrusion capability, for example, may be augmented by AI applications that allow its members to generate new evasive malware variants, combine attack techniques, disseminate propaganda, and implement automatic self-destruct mechanisms in case of detection (Kubovic, Kosinar, & Janosik, 2018). In other words, according to James S. Johnson, a postdoctoral research fellow at the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies, "AI is best understood, therefore, as a potentially powerful force multiplier of these developments" (Johnson, 2020).

Assistant Professor Rebecca Crootof (2015) in her article, "The Killer Robots Are Here: Legal and Policy Implications," asserts that "autonomy carries vastly different meanings in different fields" and due to these mixed understandings, experts can often speak past each other. For the purpose of this paper, we will use the definition of autonomy provided by the U.S. Army Robotic and Autonomous System Strategy (2017), which states that, "[autonomy is] the condition or quality of being self-governing to achieve an assigned mission based on the system's own situational awareness (integrated sensing, perceiving, analyzing) planning and decision-making." The U.S. Army Robotic and Autonomous System Strategy (2017) further emphasizes that independence is "a point on a spectrum that can be tailored to the specific mission, level of acceptable risk, and degree of human-machine teaming." According to this view, autonomy can thus be seen as a continuum and not a dichotomy. Weapon systems occupy different points according to how broadly they can identify and engage a specified target as well as their degree of self-governance over their pre-programmed or machine-learned actions. Technology on the lower end of the autonomy spectrum (i.e. semi-autonomous weapons) are currently employed by the U.S. military. The Phalanx Close-In Weapons System (CIWS), for example, which has been used by the U.S. Navy since the 1980s. CIWS provides battleships with a mechanized defense system. It can automatically "detect, evaluate, engage, and perform kill

assessments against anti-ship missiles (ASM) and high-speed aircraft threats" (U.S. Navy: Fact File, 2019).

Similar to AI, there is no internationally acceptable definition of AWS. Moreover, these weapons cannot be easily categorized because they incorporate a diverse range of technologies (Patrick, 2019). U.S. DoD Directive 3000.9, however, identifies two types of weapon systems according to their level of autonomy—autonomous and semi-autonomous. LAWS fall under the first category, which refers to a system that, once started, can engage targets without further human intervention. Unlike other countries, the U.S. definition of autonomous weapons specifies the inclusion of human-supervised AWS; this is a system designed to provide people with the ability to terminate operation of the weapon system following activation. Emphasis on possible human intercession is necessary to assuage concerns related to the use of LAWS in a combat environment.

### AI---Full Autonomy---1NC

#### AI refers exclusively to completely autonomous technologies---that excludes data mining and logistics. Any other interp opens the floodgates to any military action that uses data (so all of them)

Ware ’19 [Jacob; September 24; holds a master’s in security studies from Georgetown University and an MA (Hons) in international relations and modern history from the University of St Andrews; War on the Rocks, “Terrorist Groups, Artificial Intelligence, and Killer Drones,” https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/]

In 2016, the Islamic State of Iraq and the Levant (ISIL) carried out its first successful drone attack in combat, killing two Peshmerga warriors in northern Iraq. The attack continued the group’s record of employing increasingly sophisticated technologies against its enemies, a trend mimicked by other nonstate armed groups around the world. The following year, the group announced the formation of the “Unmanned Aircraft of the Mujahedeen,” a division dedicated to the development and use of drones, and a more formal step toward the long-term weaponization of drone technology.

Terrorist groups are increasingly using 21st-century technologies, including drones and elementary artificial intelligence (AI), in attacks. As it continues to be weaponized, AI could prove a formidable threat, allowing adversaries — including nonstate actors — to automate killing on a massive scale. The combination of drone expertise and more sophisticated AI could allow terrorist groups to acquire or develop lethal autonomous weapons, or “killer robots,” which would dramatically increase their capacity to create incidents of mass destruction in Western cities. As it expands its artificial intelligence capabilities, the U.S. government should also strengthen its anti-AI capacity, paying particular attention to nonstate actors and the enduring threats they pose. For the purposes of this article, I define artificial intelligence as technology capable of “mimicking human brain patterns,” including by learning and making decisions.

AI Could Turn Drones into Killer Robots

The aforementioned ISIL attack was not the first case of nonstate actors employing drones in combat. In January 2018, an unidentified Syrian rebel group deployed a swarm of 13 homemade drones carrying small submunitions to attack Russian bases at Khmeimim and Tartus, while an August 2018 assassination attempt against Venezuela’s Nicolas Maduro used exploding drones. Iran and its militia proxies have deployed drone-carried explosives several times, most notably in the September 2019 attack on Saudi oil facilities near the country’s eastern coast.

Pundits fear that the drone’s debut as a terrorist tool against the West is not far off, and that “the long-term implications for civilian populations are sobering,” as James Phillips and Nathaniel DeBevoise note in a Heritage Foundation commentary. In September 2017, FBI Director Christopher Wray told the Senate that drones constituted an “imminent” terrorist threat to American cities, while the Department of Homeland Security warned of terrorist groups applying “battlefield experiences to pursue new technologies and tactics, such as unmanned aerial systems.” Meanwhile, ISIL’s success in deploying drones has been met with great excitement in jihadist circles. The group’s al-Naba newsletter celebrated a 2017 attack by declaring “a new source of horror for the apostates!”

The use of drones in combat indicates an intent and capability to innovate and use increasingly savvy technologies for terrorist purposes, a process sure to continue with more advanced forms of AI. Modern drones possess fairly elementary forms of artificial intelligence, but the technology is advancing: Self-piloted drones are in development, and the European Union is funding projects to develop autonomous swarms to patrol its borders.

AI will enable terrorist groups to threaten physical security in new ways, making the current terrorism challenge even more difficult to address. According to a February 2018 report, terrorists could benefit from commercially available AI systems in several ways. The report predicts that autonomous vehicles will be used to deliver explosives; low-skill terrorists will be endowed with widely available high-tech products; attacks will cause far more damage; terrorists will create swarms of weapons to “execute rapid, coordinated attacks”; and, finally, attackers will be farther removed from their targets in both time and location. As AI technology continues to develop and begins to proliferate, “AI [will] expand the set of actors who are capable of carrying out the attack, the rate at which these actors can carry it out, and the set of plausible targets.”

For many military experts and commentators, lethal autonomous weapon systems, or “killer robots,” are the most feared application of artificial intelligence in military technology. In the words of the American Conservative magazine, the difference between killer robots and current AI-drone technology is that, with killer robots, “the software running the drone will decide who lives and who dies.” Thus, killer robots, combining drone technology with more advanced AI, will possess the means and power to autonomously and independently engage humans. The lethal autonomous weapon has been called the “third revolution in warfare,” following gunpowder and nuclear weapons, and is expected to reinvent conflict, not least terrorist tactics.

Although completely autonomous weapons have not yet reached the world’s battlefields, current weapons are on the cusp. South Korea, for instance, has developed and deployed the Samsung SGR-A1 sentry gun to its border with North Korea. The gun supposedly can track movement and fire without human intervention. Robots train alongside marines in the California desert. Israel’s flying Harpy munition can loiter for hours before detecting and engaging targets, while the United States and Russia are developing tanks capable of operating autonomously. And the drones involved in the aforementioned rebel attack on Russian bases in Syria were equipped with altitude and leveling sensors, as well as preprogrammed GPS to guide them to a predetermined target.

Of particular concern is the possibility of swarming attacks, composed of thousands or millions of tiny killer robots, each capable of engaging its own target. The potentially devastating terrorist application of swarming autonomous drones is best summarized by Max Tegmark, who has said that “if a million such killer drones can be dispatched from the back of a single truck, then one has a horrifying weapon of mass destruction of a whole new kind: one that can selectively kill only a prescribed category of people, leaving everybody and everything else unscathed.” Precisely that hypothetical scenario was illustrated in a recent viral YouTube video, “Slaughterbots,” which depicted the release of thousands of small munitions into British university lecture halls. The drones then pursued and attacked individuals who had shared certain political social media posts. The video also depicts an attack targeting sitting U.S. policymakers on Capitol Hill. The video has been viewed over three million times, and was met with increasing concern about potential terrorist applications of inevitable autonomous weapons technology. So far, nonstate actors have only deployed “swarmed” drones sparingly, but it points to a worrying innovation: Swarming, weaponized killer robots aimed at civilian crowds would be nearly impossible to defend against, and, if effective, cause massive casualties.

### AI---Includes Narrow/Strong AI---2AC

#### AI refers to systems that perform tasks that normally require human intelligence---that covers the gamut from narrow AI to theoretical strong AI

Jensen ’16 [Benjamin and Ryan Kendall; September 2; Major in the US Army Reserve currently serving as a Fellow in the Office of the Chief of Staff of the Army, Strategic Studies Group; Lieutenant Colonel in the US Army currently serving in the Chief of Staff of the Army, Strategic Studies Group;

War on the Rocks, “Waze For War: How The Army Can Integrate Artificial Intelligence,” [https://warontherocks.com/2016/09/waze-for-war-how-the-army-can-integrate-artificial-intelligence]](https://warontherocks.com/2016/09/waze-for-war-how-the-army-can-integrate-artificial-intelligence%5d)

Artificial intelligence is commonly defined as the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. It can range from weak forms, such as narrow artificial intelligence, that processes big data to answer basic questions and generate predictions (e.g., think of Waze helping you drive home or ad placements online) to strong forms such as “Artificial General Intelligence” and “Artificial Super Intelligence” that exceed human intelligence, creativity, and adaptability. Military applications range from finding optimal human-machine symbiosis, the centaur Deputy Secretary of Defense Robert Work speaks about, to using increased computer processing power to replace people on the battlefield with autonomous attack swarms.

Short of the promise of driverless cars and robot servants, narrow forms of artificial intelligence like machine learning are starting to change sectors ranging from healthcare to logistics. With respect to public health, Flowminder, a Swedish NGO, uses narrow artificial intelligence to predict the spread of diseases. In logistics, machine learning is helping companies make supply chain adjustments, optimize delivery routes, and design warehouse systems. Vehicle developers, such as Volvo, apply artificial intelligence to improve predictive maintenance. Volvo collects data with smart sensors on their vehicles and applies machine learning techniques to conduct diagnostics that reduce down time for services and better inform the resupply.

Artificial Intelligence for the Military

While many commercial applications of artificial intelligence are based on identifying patterns and trends using big data, most military applications focus on autonomous systems. Existing artificial intelligence programs in the Department of Defense include Navy unmanned undersea and aerial vehicle programs such as the Low-Cost Unmanned Aerial Vehicle Swarming Technology (LOCUST), and Air Force/DARPA ventures such as the Gremlin anti-surface-to-air missile drone program. The Gremlin program involves launching a large number of unmanned systems from a transport plane that swarm to attack hard targets such as mobile SAM platforms and C4ISR nodes. Within the Army, labs are using artificial intelligence to experiment with autonomous vehicles. Concepts range from larger logistics convoys composed of one manned vehicle and a large number of autonomous vehicles to combat formations mixing manned and unmanned platforms.

While the private sector focuses on narrow artificial intelligence applications that aid decision making and optimize business models, the military’s focus on autonomy arises from a technological bottleneck. A more advanced version of artificial intelligence than exists today is likely a necessary development before the military can field autonomous systems able to adapt to complex, changing environments. This evolution is especially important for land forces. Ground platforms have more variables to address than air or naval systems. Jets and submarines do not have to dodge potholes or jaywalkers. An autonomous system operating in a future megacity would have to do both under fire. The result is that autonomous combat vehicles will likely emerge in the air and maritime domain faster than the ground domain. Yet, that should not stop continued investment in and experimentation with artificial intelligence by the Army.

### AI---Broad Interp---2AC

#### ‘AI’ is a broad umbrella term referring to any technique aimed at approximating human cognition using machines----encompasses ML, neural networks, data mining, expert systems, robotics, and more.

Chiles ’19 [John and Clara Reyes; 2019; Partner at Burr & Forman LLP; Assistant Professor of Law and Director of R&D at Michigan State Law School and Faculty Associate at Berkman Klein Center for Internet and Society at Harvard University; “Robot Loans: Artificial Intelligence and Its Place in Consumer Finance?,” 73 Consumer Fin. L.Q. Rep. 205, WestLaw]

John: Carla is an Assistant Professor of Law and Director of R&D at Michigan State Law School. She's a Faculty Associate at Berkman Klein Center for Internet and Society at Harvard Law School. Or is it at the university?

Carla: University.

\*210 John: University, not the law school, which is a think tank collaboration of a number of top intellectuals in this field of fintech. Her focus is on the intersection of blockchain and law, but she knows AI, because she's authoring a casebook on AI and the law. And she's very familiar with all the writings on this issue, so she's an asset to our discussion here.

I want to do something that. ... It may seem elementary to some of you, but having sat through a number of discussions of the use of AI and machine learning and large datasets and analysis for credit-related issues, I was puzzled exactly how this works, to be honest with you. How does the AI model work? How does the machine learning model work? And what is done with big datasets, particularly non-traditional data that's being used more and more by fintech companies? As a kickoff to this, I wanted to ask Carla to give us an overview of how these particular programs and tools, that are being developed in fairly substantial quantities and numbers, how these actually work and how the machine learning and the large dataset analysis is deployed. Just how it works, so we can understand.

Carla: So, in other words, you're asking the professor to do what professors do, which is lay the foundation definitionally. I can do this. Generally speaking, there's really no straightforward consensus on the definition of artificial intelligence. As a result, discussion of AI and its sub-fields really are susceptible to a lot of hype and confusion. For instance, people use the term “machine learning” and “artificial intelligence” interchangeably, but they're really not the same thing, and so the goal here is just to break some of that down a little bit. At a pretty high level still, but just to lay the foundation definitionally.

A best consensus definition of artificial intelligence is that it's a broad term, an umbrella term, used to refer to a large set of information science. It's best understood as a set of techniques aimed at approximating some aspect of human cognition using machines. And the main takeaway is that, although we use the term “artificial intelligence” as though it's monolithic, it's really not. It covers a range of sub fields, which include, and I should say “but is not limited to” as lawyers say, neural networks, vision, data mining, expert systems, robotics, natural language processing, natural language understanding, planning, and evolutionary computation.

We actually have a class on evolutionary analysis and the law at MSU Law School, so all of these are relevant to the legal field and legal issues, but the one primarily people think about and mean when they use the term “artificial intelligence” is machine learning. Machine learning refers generally to the capacity of a system to improve its performance at some task, some specific task, over time. Often, the task involves recognizing patterns in datasets. Although machine learning outputs can include everything from translating languages to grasping objects or helping to drive a car.

\*211 Specifically, machine learning relies on algorithms to analyze huge datasets. It basically performs predictive analytics far faster than any human can on a dataset that's larger than any human could reasonably get through efficiently. Notably, however and something I think that gets lost sometimes in legal discussions, is that, generally speaking, oftentimes, not always but often, the machine learning system is both ... and this should be always, is both designed and created by humans, and then you put inputs into it and it output results. Those outputs are then interpreted and applied by humans, right?

### AI---AT: “AI Approximates Humans”/Full Autonomy---2AC

#### Their interp anthropomorphizes AI---no integration of AI into military affairs is ever fully autonomous---imprecise and means no affs meet

Carchidi ’22 [Vincent; May 16; Master of Political Science from Villanova University specializing in the intersection of technology and international affairs, with an interdisciplinary background in cognitive science; War on the Rocks, “Is Artificial Intelligence Made in Humanity’s Image? Lessons for an AI Military Education,” https://warontherocks.com/2022/05/is-artificial-intelligence-made-in-humanitys-image-lessons-for-an-ai-military-education]

Artificial intelligence is not like us. For all of AI’s diverse applications, human intelligence is not at risk of losing its most distinctive characteristics to its artificial creations.

Yet, when AI applications are brought to bear on matters of national security, they are often subjected to an anthropomorphizing tendency that inappropriately associates human intellectual abilities with AI-enabled machines. A rigorous AI military education should recognize that this anthropomorphizing is irrational and problematic, reflecting a poor understanding of both human and artificial intelligence. The most effective way to mitigate this anthropomorphic bias is through engagement with the study of human cognition — cognitive science.

This article explores the benefits of using cognitive science as part of an AI education in Western military organizations. Tasked with educating and training personnel on AI, military organizations should convey not only that anthropomorphic bias exists, but also that it can be overcome to allow better understanding and development of AI-enabled systems. This improved understanding would aid both the perceived trustworthiness of AI systems by human operators and the research and development of artificially intelligent military technology.

For military personnel, having a basic understanding of human intelligence allows them to properly frame and interpret the results of AI demonstrations, grasp the current natures of AI systems and their possible trajectories, and interact with AI systems in ways that are grounded in a deep appreciation for human and artificial capabilities.

Artificial Intelligence in Military Affairs

AI’s importance for military affairs is the subject of increasing focus by national security experts. Harbingers of “A New Revolution in Military Affairs” are out in force, detailing the myriad ways in which AI systems will change the conduct of wars and how militaries are structured. From “microservices” such as unmanned vehicles conducting reconnaissance patrols to swarms of lethal autonomous drones and even spying machines, AI is presented as a comprehensive, game-changing technology.

As the importance of AI for national security becomes increasingly apparent, so too does the need for rigorous education and training for the military personnel who will interact with this technology. Recent years have seen an uptick in commentary on this subject, including in War on the Rocks. Mick Ryan’s “Intellectual Preparation for War,” Joe Chapa’s “Trust and Tech,” and Connor McLemore and Charles Clark’s “The Devil You Know,” to name a few, each emphasize the importance of education and trust in AI in military organizations.

Because war and other military activities are fundamentally human endeavors, requiring the execution of any number of tasks on and off the battlefield, the uses of AI in military affairs will be expected to fill these roles at least as well as humans could. So long as AI applications are designed to fill characteristically human military roles — ranging from arguably simpler tasks like target recognition to more sophisticated tasks like determining the intentions of actors — the dominant standard used to evaluate their successes or failures will be the ways in which humans execute these tasks.

But this sets up a challenge for military education: how exactly should AIs be designed, evaluated, and perceived during operation if they are meant to replace, or even accompany, humans? Addressing this challenge means identifying anthropomorphic bias in AI.

Anthropomorphizing AI

Identifying the tendency to anthropomorphize AI in military affairs is not a novel observation. U.S. Navy Commander Edgar Jatho and Naval Postgraduate School researcher Joshua A. Kroll argue that AI is often “too fragile to fight.” Using the example of an automated target recognition system, they write that to describe such a system as engaging in “recognition” effectively “anthropomorphizes algorithmic systems that simply interpret and repeat known patterns.”

But the act of human recognition involves distinct cognitive steps occurring in coordination with one another, including visual processing and memory. A person can even choose to reason about the contents of an image in a way that has no direct relationship to the image itself yet makes sense for the purpose of target recognition. The result is a reliable judgment of what is seen even in novel scenarios.

An AI target recognition system, in contrast, depends heavily on its existing data or programming which may be inadequate for recognizing targets in novel scenarios. This system does not work to process images and recognize targets within them like humans. Anthropomorphizing this system means oversimplifying the complex act of recognition and overestimating the capabilities of AI target recognition systems.

By framing and defining AI as a counterpart to human intelligence — as a technology designed to do what humans have typically done themselves — concrete examples of AI are “measured by [their] ability to replicate human mental skills,” as De Spiegeleire, Maas, and Sweijs put it.

Commercial examples abound. AI applications like IBM’s Watson, Apple’s SIRI, and Microsoft’s Cortana each excel in natural language processing and voice responsiveness, capabilities which we measure against human language processing and communication.

Even in military modernization discourse, the Go-playing AI “AlphaGo” caught the attention of high-level People’s Liberation Army officials when it defeated professional Go player Lee Sedol in 2016. AlphaGo’s victories were viewed by some Chinese officials as “a turning point that demonstrated the potential of AI to engage in complex analyses and strategizing comparable to that required to wage war,” as Elsa Kania notes in a report on AI and Chinese military power.

But, like the attributes projected on to the AI target recognition system, some Chinese officials imposed an oversimplified version of wartime strategies and tactics (and the human cognition they arise from) on to AlphaGo’s performance. One strategist in fact noted that “Go and warfare are quite similar.”

Just as concerningly, the fact that AlphaGo was anthropomorphized by commentators in both China and America means that the tendency to oversimplify human cognition and overestimate AI is cross-cultural.

The ease with which human abilities are projected on to AI systems like AlphaGo is described succinctly by AI researcher Eliezer Yudkowsky: “Anthropomorphic bias can be classed as insidious: it takes place with no deliberate intent, without conscious realization, and in the face of apparent knowledge.” Without realizing it, individuals in and out of military affairs ascribe human-like significance to demonstrations of AI systems. Western militaries should take note.

For military personnel who are in training for the operation or development of AI-enabled military technology, recognizing this anthropomorphic bias and overcoming it is critical. This is best done through an engagement with cognitive science.

The Relevance of Cognitive Science

The anthropomorphizing of AI in military affairs does not mean that AI is always given high marks. It is now cliché for some commentators to contrast human “creativity” with the “fundamental brittleness” of machine learning approaches to AI, with an often frank recognition of the “narrowness of machine intelligence.” This cautious commentary on AI may lead one to think that the overestimation of AI in military affairs is not a pervasive problem. But so long as the dominant standard by which we measure AI is human abilities, merely acknowledging that humans are creative is not enough to mitigate unhealthy anthropomorphizing of AI.

Even commentary on AI-enabled military technology that acknowledges AI’s shortcomings fails to identify the need for an AI education to be grounded in cognitive science.

For example, Emma Salisbury writes in War on the Rocks that existing AI systems rely heavily on “brute force” processing power, yet fail to interpret data “and determine whether they are actually meaningful.” Such AI systems are prone to serious errors, particularly when they are moved outside their narrowly defined domain of operation.

Such shortcomings reveal, as Joe Chapa writes on AI education in the military, that an “important element in a person’s ability to trust technology is learning to recognize a fault or a failure.” So, human operators ought to be able to identify when AIs are working as intended, and when they are not, in the interest of trust.

Some high-profile voices in AI research echo these lines of thought and suggest that the cognitive science of human beings should be consulted to carve out a path for improvement in AI. Gary Marcus is one such voice, pointing out that just as humans can think, learn, and create because of their innate biological components, so too do AIs like AlphaGo excel in narrow domains because of their innate components, richly specific to tasks like playing Go.

Moving from “narrow” to “general” AI — the distinction between an AI capable of only target recognition and an AI capable of reasoning about targets within scenarios — requires a deep look into human cognition.

The results of AI demonstrations — like the performance of an AI-enabled target recognition system — are data. Just like the results of human demonstrations, these data must be interpreted. The core problem with anthropomorphizing AI is that even cautious commentary on AI-enabled military technology hides the need for a theory of intelligence. To interpret AI demonstrations, theories that borrow heavily from the best example of intelligence available — human intelligence — are needed.

The relevance of cognitive science for an AI military education goes well beyond revealing contrasts between AI systems and human cognition. Understanding the fundamental structure of the human mind provides a baseline account from which artificially intelligent military technology may be designed and evaluated. It possesses implications for the “narrow” and “general” distinction in AI, the limited utility of human-machine confrontations, and the developmental trajectories of existing AI systems.

The key for military personnel is being able to frame and interpret AI demonstrations in ways that can be trusted for both operation and research and development. Cognitive science provides the framework for doing just that.

Lessons for an AI Military Education

It is important that an AI military education not be pre-planned in such detail as to stifle innovative thought. Some lessons for such an education, however, are readily apparent using cognitive science.

First, we need to reconsider “narrow” and “general” AI. The distinction between narrow and general AI is a distraction — far from dispelling the unhealthy anthropomorphizing of AI within military affairs, it merely tempers expectations without engendering a deeper understanding of the technology.

The anthropomorphizing of AI stems from a poor understanding of the human mind. This poor understanding is often the implicit framework through which the person interprets AI. Part of this poor understanding is taking a reasonable line of thought — that the human mind should be studied by dividing it up into separate capabilities, like language processing — and transferring it to the study and use of AI.

The problem, however, is that these separate capabilities of the human mind do not represent the fullest understanding of human intelligence. Human cognition is more than these capabilities acting in isolation.

Much of AI development thus proceeds under the banner of engineering, as an endeavor not to re-create the human mind in artificial ways but to perform specialized tasks, like recognizing targets. A military strategist may point out that AI systems do not need to be human-like in the “general” sense, but rather that Western militaries need specialized systems which can be narrow yet reliable during operation.

This is a serious mistake for the long-term development of AI-enabled military technology. Not only is the “narrow” and “general” distinction a poor way of interpreting existing AI systems, but it clouds their trajectories as well. The “fragility” of existing AIs, especially deep-learning systems, may persist so long as a fuller understanding of human cognition is absent from their development. For this reason (among others), Gary Marcus points out that “deep learning is hitting a wall.”

An AI military education would not avoid this distinction but incorporate a cognitive science perspective on it that allows personnel in training to re-think inaccurate assumptions about AI.

Human-Machine Confrontations Are Poor Indicators of Intelligence

Second, pitting AIs against exceptional humans in domains like Chess and Go are considered indicators of AI’s progress in commercial domains. The U.S. Defense Advanced Research Projects Agency participated in this trend by pitting Heron Systems’ F-16 AI against a skilled Air Force F-16 pilot in simulated dogfighting trials. The goals were to demonstrate AI’s ability to learn fighter maneuvers while earning the respect of a human pilot.

These confrontations do reveal something: some AIs really do excel in certain, narrow domains. But anthropomorphizing’s insidious influence lurks just beneath the surface: there are sharp limits to the utility of human-machine confrontations if the goals are to gauge the progress of AIs or gain insight into the nature of wartime tactics and strategies.

## Biotechnology

### Biotech---Excludes SynthBio---1NC

#### Biotech is distinct from synthbio---it’s not technologically advanced enough to encompass gene editing and bioengineering---precludes the vast majority of capabilities described in the 1AC

Diep ’17 [Patrick; 2017; Synthetic Biologist, PhD in Chemical Engineering at the University of Toronto; “What is synthetic biology,” Quora]

Clearing the Fog | A Definition

A discipline is a branch of knowledge.[2]If it is a sub-branch, then it is a sub-discipline. The term synbio is comprised of “synthetic” and “biology.” Biology is already a discipline with many sub-disciplines (e.g. microbiology, immunology, molecular biology, etc.), but “synthetic” is a descriptive word that alters what we are referring to much like “computational” biology and “systems” biology. Computational biology is the use of computational systems to assist with exploration of and discoveries in biology.[3] Systems biology, branching off from computational biology, models biological systems largely to discover emergent properties and how they arise.[4][5]

“Synthetic” has interesting definitions, the most important being “made by chemical synthesis, especially to imitate a natural product.”[6]Does this kind of work already exist in the discipline of biology?

Not really. There are two generic sub-disciplines that come close to this, in my opinion (though they’re such large fields I’m not sure if “sub-discipline” would still capture their individual significance). They are biotechnology and bioengineering.

Biotechnology uses living systems and their components to produce things that we want.[7]If you were to look through this textbook on molecular biotechnology that I studied throughout two courses, the biotechnology examples that are provided are, at most, mutagenesis of existing genes or splicing of genes together. Promoters might be cloned around to accomplish specific goals, but no where is there an example of making a promoter from nearly scratch.[8] Genes might be put together to form new metabolic networks to produce some product, but they aren’t characterizing and modularizing these genes like electric circuit components.[9]Perhaps the textbook is too old? Even this recent molecular biotechnology textbook published last year barely mentions synthetic biology. It uses the term 19 times covering only 7/622pgs, not counting citations.

Bioengineering (or biomedical engineering) use to be more strictly defined by efforts on prosthetics and clinical/medical devices, but the advent of DNA synthesis and attempts to characterize/modularize genetic parts (i.e. promoters, tags, terminators, etc.) allowed bioengineering to expand into cellular and molecular biology.[10][11][12] By “expand into” I mean “apply engineering principles” to these life systems, which has lead to a spur in other technologies: bioprocess engineering, stem cell engineering, biomimetics, etc.

In relation to biotechnology, synbio is what I argue to be the evolved version. What previous biotechnology could not achieve, synbio strives to address those challenges. For example I mentioned promoter design earlier. Before synbio, “designing” promoters was more like “let’s mutate this and see which mutants do what we want.” There have been many attempts now to de novo design promoters, most recently here[13].

In relation to bioengineering, synbio overlaps with it. There’s a blurred line whether synbio is a separate sub-discipline that can be used in some bioengineering challenges, or if synbio is a product of bioengineering, meaning that synbio is a sub-sub-discipline. My opinion is the former because synbio does serve bioengineering, but synbio also serves environmental[14], computational[15], and aesthetic/artistic(!) challenges too[16]. Wikipedia seems to describe bioengineering more generically by capturing all these themes, but university websites describe their bioengineering programs as life science-/health-based which leaves me the impression that bioengineering is strongly-motivated by human health research[17][18][19][20]. Honestly I wonder why? (#grantcommitteepriorities)

Contrasting synbio, biotechnology and bioengineering is important because those two are the closest sub-disciplines within the biology umbrella to synbio. The differences are what define synbio. Therefore, I conclude this to be the simplest definition:

Synthetic biology is the characterization and modularization of life’s genetic parts to serve as tools to address challenges contingent on the manipulation of life at the molecular level.

### Biotech---AT: Excludes SynthBio---2AC

#### ‘Biotech’ is broad---and it contains synthetic bio as a subsidiary component

Dieulis ’18 [Diane; Nov 27; Senior Research Fellow at the Center for the Study of Weapons of Mass Destruction and leads studies on biosecurity, biodefense and the synthetic biology industry, a biologist by training and served for over two decades in various capacities at the Department of Health and Human Services and the Office of Science and Technology Policy at the White House; War on the Rocks, “Biotechnology for the Battlefield: In Need of a Strategy,” https://warontherocks.com/2018/11/biotechnology-for-the-battlefield-in-need-of-a-strategy]

If today’s technology headlines are any indication, the science fiction of comic books is becoming science reality. Impenetrable skin and resilience to gamma rays are no longer just for superheroes. For instance, scientists have recently discovered ways to create spider silk, an innovative biotechnology that can lead to lighter, more flexible, and stronger body armor. And microscopic animals nicknamed “water bears” are showing promise to protect soldiers from the health effects of radiation exposure by boosting capacity for DNA repair or even preventing damage to DNA in the first place.

Biotechnology — a broad term used to describe technological innovation based on biology — has become an increasingly agile platform for developing new types of soldier enhancements. As such, the field offers novel opportunities for improving warfighter survivability on the battlefield. Despite recent developments, however, the Department of Defense has yet to strategically guide the development of these new technologies at the national level. Recently, War on the Rocks published an article outlining concerns about the lack of coordinated policy for developing synthetic biology – a branch of biotechnology – while preventing its misuse by adversaries. The article rightly pointed to the need to think strategically about the risk of proliferating synthetic biology capabilities, but this is only one part of the picture. Current national strategies encourage policymakers to view advances in biology through a narrow lens of risks to national security and the development of countermeasures to protect against those risks, which, while crucial, neglects the promise for using the same science to develop life-saving or other advanced tools for warfighters. The Pentagon’s current efforts to take advantage of synthetic biology as a platform for defense lack internal cohesion and external direction, and biological innovation faces further challenges given the absence of agile business models to fully harness emerging biotechnologies for the battlefield. Greater coordination between those in the Defense Department whose work relates to biotechnology and improved relationships with the private sector are important first steps toward using this burgeoning area of science not just to mitigate security risks, but also to benefit soldiers on the battlefield.

#### Prefer NATO definitions---biotech in a military context is defined broadly

Melson ‘4 [Ashley; 2004; Associate, The Barkley Law Firm, PC. B.S. P.T., University of Oklahoma Health Sciences Center, 1997 and J.D., Valedictorian, University of Tulsa College of Law; “Bioterrorism, Biodefense, and Biotechnology in the Military: A Comparative Analysis of Legal and Ethical Issues in the Research, Development, and Use of Biotechnological Products on American and British Soldiers,” 14 Alb. L.J. Sci. & Tech. 497, lexis]

Biology, 1 one of the three primary natural sciences, like its counterpart sciences of chemistry and physics, uses the experimental method 3 Unlike its counterparts, however, the study of biology inherently involves living things, including human beings. 4 Because of this distinction, which implicates both human rights and the Hippocratic Oath, 5 the experimental method becomes legally and ethically unacceptable as a means of studying biology, at least when human subjects are involved. 6 Further, knowledge gleaned in this science does not truly come to fruition until applied and used in the real world through technological innovations, thus the term "biotechnology." 7

Although not officially defined until 1919 by Hungarian engineer, Karl Ereky, 8 the first example of biotechnological innovations noted in literature dates back well before Ereky's time to the selective breeding of livestock and growing of crops during the Agricultural Revolution. 9 Today, a sort of "biotechnological age" is being realized, 10 as the United States (U.S.) Government, alone, invested over $ 18 billion in biotechnology research and development (R&D) for fiscal year 2000. 11 This figure is dwarfed by the R&D budgets of large pharmaceutical companies and other commercial investors. 12

Beyond the financial investment in biotechnology is the investment from both individuals and society as a whole. Because the testing and use of biotechnological products inherently involves living organisms from microbes to human beings, 13 complex legal and ethical issues arise, the solutions to which have yet to be answered, and, at times, even addressed. Basic standards for research using human subjects have been enunciated in international instruments beginning with the Nuremberg Code, 14 but, as history has shown, the research context has often dictated whether such standards would apply, and to what extent, in actual practice. 15 Furthermore, research involving the use of human "materials," namely stem cells 17 raises perhaps even more controversial issues than human subject research. Once biotechnology products are developed, a new series of debates arises as to whether their use is appropriate, and, if so, by whom and for what purpose, 18 as well as what may be done with information obtained through the research or the use of biotechnology. 19

Ultimately, this question is presented: Do the benefits of biotechnology outweigh risks associated with these unresolved issues? The answer may depend on what stands to be lost if testing and use of biotechnology products is not pursued. In the public health context, these products provide potential solutions to pressing concerns in the national, as well as global, arena. Developments in genetically engineered foods and drugs, for example, pose alternatives to addressing issues of world hunger and disease. In the medical context, biotechnology products have revolutionized health care by providing new options for injury and illness prevention, as well as treatment, in the form of pharmaceuticals, procedures, and devices.

Also affected on a global scale and, perhaps, ever so evident with the recent threats of bioterrorism, are the opportunities biotechnology presents in the military context, 20 which is defined as "the exploitation and manipulation of biological systems to benefit overall military capability." 21 [21]Dr. Steve Nicklin, Medical Issues: The Future Impact of Biotechnology on Human Factors, in NATO Research & Technology Organization, RTO Meeting Proceedings 77: Human Factors in the 21st Century, RTO-MP-077 AC/323(HFM-062)TP/38 (2002), http://www.rta.nato.int/Abstracts.asp?Restrict Panel=HFM (last visited Mar. 20, 2004).[/21] According to a recent report by the Information Assurance Technology Analysis Center (IATAC), "history has shown that an infusion of technology can provide a significant military advantage to the side that first realizes its potential and exploits it." 22 However, the historical examples described, namely invention of the tank, development of U.S. naval aviation capabilities, and technologies emerging from the Information Revolution, fail to invoke the legal and ethical complexities presented by biotechnological research, development, and use in the military. Such concerns become particularly relevant in light of the history of abuse of civilian and service member subjects in research conducted or sponsored by the militaries of both the U.S. 23 and its European Ally, the United Kingdom (U.K.). 24

## Cybersecurity

### Cybersecurity---CIA Triad---1NC

#### Cybersecurity policy must expand protections for the confidentiality, integrity, AND availability of data on computer systems and networks---plans that don’t address all three explicitly don’t meet.

Cybersecurity law promotes the confidentiality, , integrity, and availability of public and private information, systems, and networks

Kosseff ’18 [Jeff; March; Assistant Professor of Cybersecurity Law, United States Naval Academy. J.D., Georgetown University Law Center; M.P.P., B.A., University of Michigan; Iowa Law Review, “Defining Cybersecurity Law,” 103 Iowa L. Rev. 985, lexis]

In late 2015, after years of attempts, Congress passed legislation to enable companies to voluntarily share information about cybersecurity threats - such as attempted hacks - with the federal government and other companies. The bill, entitled the Cybersecurity Act of 2015, was tucked into a massive omnibus appropriations bill as Division N. 1 The Cybersecurity Act occupies 136 of the 2,009 pages in the omnibus bill, and it in detail establishes rules for operators of private networks to defend their networks, monitor possible threats, and collaborate with the federal government. 2 The new law also bolsters the Department of Homeland Security's ("DHS") cybersecurity efforts. The focus of the legislation, not surprisingly, is cybersecurity; indeed, "cybersecurity" appears in the bill nearly 200 times. 3

There is just one problem: The Cybersecurity Act does not define "cybersecurity." The statute allows companies to take certain actions for a "cybersecurity purpose," which it defines as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." 4 The statute defines "security vulnerability" as "any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control." 5 The statute defines "cybersecurity threat" as

an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. 6

The statute also defines "security control," 7 "malicious cyber command and control," 8 and "cyber threat indicator." 9 Although these definitions help to illuminate the purpose of the legislation, the Cybersecurity Act does not directly explain what lawmakers meant by "cybersecurity."

The statute fails to provide a concrete definition that sets forth the scope and goals of cybersecurity law. Although the new statute can function without the definition - and as described in Part III of this Article: , is a significant improvement over existing law - its omission of this key definition is illustrative of a larger problem: When policymakers talk about cybersecurity, they are not always talking about the same concept.

A day rarely passes without another report of a major cybersecurity incident. Hackers routinely breach the systems of retailers, stealing consumer credit card data, social security numbers, and other valuable personal information. 10 Attackers launch distributed denial-of-service attacks, knocking some of the most popular websites offline for hours or days. 11 Home security webcams become remote spying devices. 12 Even the U.S. electoral system is compromised by hacks of the email accounts of political officials and attacks on state elections systems. 13 In the increasingly frequent news coverage of these attacks, commentators, and lawmakers demand immediate and swift legal solutions to prevent further damage. 14 The constant media coverage begs the question: How well do our existing laws address cybersecurity threats?

The short answer: Not well at all. The slightly longer answer: The patchwork of U.S. statutes and regulations that constitute cybersecurity law is an uncoordinated mishmash of requirements that mostly were conceived long before modern cyber-threats. Modern U.S. cybersecurity law stems from century-old privacy norms, torts, and criminal laws that bear little relation to the protection of the confidentiality, integrity, or availability of systems, networks, and data.

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.

One might argue that it is unnecessary to define a legal field. By proposing a definition of "cybersecurity law," I seek to offer the definition as a broad taxonomy for policymakers and courts as they develop statutes, regulations, and court rulings that could shape cybersecurity for generations to come. By defining "cybersecurity law," I suggest the types of subjects that the law seeks to secure, the methods by which cybersecurity law protects those subjects, and the reasons behind cybersecurity law. Moreover, I intend this definition to do more than merely add to a legal taxonomy; a clear definition of "cybersecurity law" will provide policymakers with goals and guideposts as they debate new laws to protect information, systems, and networks.

III. Defining "Cybersecurity Law"

The Sony incident - and similar cybersecurity challenges that companies and governments have faced - provide us with a roadmap for defining this new area of law. A clear definition of "cybersecurity law" is necessary for lawmakers, regulators, courts, and commentators to offer solutions to these ongoing threats. This Part offers some elements of the definition based on the experiences with incidents such as the attack on Sony Pictures. This Part concludes with a suggested comprehensive definition of "cybersecurity law."

To form the definition, we must answer five fundamental questions that examine the underlying values that should shape our cybersecurity laws: (1) What are we securing?; (2) Where and whom are we securing?; (3) How are we securing?; (4) When are we securing?; and (5) Why are we securing?

After addressing these five framing questions, this Article: proposes a definition for "cybersecurity law" that takes into account the important considerations in the field of cybersecurity. This definition allows us to assess the current laws that are frequently associated with cybersecurity and explore the areas where they are lacking.

A. What Are We Securing?

At the outset of any attempt to define "cybersecurity law," it is necessary to understand the intended subject matter. In other words, what should the law seek to secure? Based on the ongoing drumbeat of significant and damaging cybersecurity incidents 44 and the increased vulnerability due to the connection of everyday devices to the Internet, 45 I propose that "cybersecurity law" broadly seek to promote the confidentiality, integrity, and availability of information, systems, and networks.

Cybersecurity often is conflated, particularly in legal circles, with data security. 46 Although data security is an important part of cybersecurity, it is only one part. Cybersecurity focuses not only on the protection of data, but also on the systems and networks of the public and private sector. In other words, cybersecurity involves more than merely the protection of data.

Consider, for example, the 2016 Distributed Denial of Service ("DDOS") attack on Dyn, a relatively obscure but exceptionally important company that provides a large portion of the domain name system that directs traffic on the Internet. 47 A DDOS attack floods a targeted server with traffic from multiple sources, causing a slowdown in traffic or a complete shutdown. 48 Due to the DDOS attack on Dyn, Netflix, Twitter, and other popular online services were unavailable for the majority of a day. 49 Although the attack resulted in some data being unavailable, it would not be characterized as a traditional data security compromise. Instead, it was an attack that compromised an entire network. 50 Laws focused exclusively on data - rather than networks and systems - will do little to prevent and remediate harms such as the Dyn attack.

To be sure, data security is a vital component of cybersecurity. For instance, the attack on Sony compromised a significant amount of the company's valuable data, including confidential emails and unreleased movies. That aspect of the attack attracted a great deal of publicity. 51 However, Sony also suffered great business harm due to the unavailability of its systems and networks. 52 The attack on Sony, in other words, was not merely an attack on the company's data security. It was a comprehensive attack on Sony's cybersecurity. The attack compromised more than just the confidentiality of Sony's information, though it certainly had that effect as well. The attack compromised the fundamental ability of Sony to carry out its routine business operations.

A focus on the security of systems and networks - and not just information - is necessary as physical devices are increasingly connected to the Internet. For instance, policymakers and regulators are understandably concerned about a cyberattack on a connected automobile that causes a highway crash, or a remote exploit of a factory's control systems that causes explosions, physical injury, and property damage. 53 By focusing exclusively on attacks on information, cybersecurity law would not address such threats to cyber-physical systems. Cybersecurity law should be flexible enough to address not only the incidents that already have occurred, but also potential future vectors of attack.

Therefore, when we develop the contours for cybersecurity law, we must develop a broader and more appropriate approach. The National Initiative for Cybersecurity Careers and Studies reflects such an approach, as its definition of "cybersecurity" is "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." 54 This definition captures the need to protect not only data, but also the systems on which data are stored and the networks on which data are transmitted. A definition of "cybersecurity law" that includes this important aspect will focus on the threats posed by cyberattacks.

We have established that cybersecurity law should focus not only on the security of information, but on systems and networks as well. However, the law does not provide much clarity as to what "security" means in the context of cybersecurity. Even though we know that we are securing information, networks, and systems, what do we mean by "securing"? Relatedly, how do we accomplish this task?

Cybersecurity professionals commonly think about security as covering three general categories of goals: (1) confidentiality; (2) integrity; and (3) availability, known in the industry as the "CIA Triad." 55 Confidentiality refers to the "the prevention of unauthorized disclosure of information." 56 Confidentiality often is associated with data breaches because attackers seek to obtain information without proper authorization. Integrity refers to "the guarantee that the message that is sent is the same as the message received and that the message is not altered in transit." 57 The defacement of a company's website, for example, is an example of a threat to data integrity. A threat to integrity also could refer to the modification of a business's financial records, as such a modification would cause internal chaos for the business's operations. 58 Availability refers to "the guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of [the] location of the user." 59 A DDOS attack that knocks a popular website offline, for example, is an attack on that site's availability.

The Sony Pictures attack threatened all three prongs of the CIA triad. The hackers compromised the confidentiality of employees' personal information as well as the company's highly sensitive business information. By altering the interface of the Sony Pictures internal computer systems, the attackers compromised the integrity of Sony's systems. The attack also harmed the availability of Sony's information and systems, as employees were unable to access the network.

Likewise, the reports of Russian interference in the 2016 U.S. elections demonstrate attempts to attack the entire CIA triad. The hack of Clinton campaign chairman John Podesta's emails was a classic compromise of confidentiality. 60 But Russia at least attempted to do more than access private emails. According to media reports, Russian hackers accessed voter databases and other elections systems in 39 states. 61 These attacks may have been attempts to compromise the integrity of U.S. voting data. Had the hackers knocked the voting systems offline on election day, the attacks would have compromised the availability of information systems and networks that are fundamental to U.S. democracy.

As Part IV of this Article: explains, U.S. cybersecurity-related laws heavily focus on only one prong of the CIA Triad: confidentiality. This focus is because many of the statutes and regulations that intersect with cybersecurity are outgrowths of privacy law, which has a much more established field of jurisprudence and theory that has developed over more than a century. 62 The conflation of privacy and cybersecurity is understandable, 63 as many highly publicized cybersecurity incidents have involved breaches of sensitive information. While cybersecurity law should be concerned about preventing privacy violations, that should not be the unilateral focus of our approach to cybersecurity law. To be sure, we want to make sure that cybersecurity law attempts to prevent breaches of confidentiality that invade individual privacy and exposes corporate intellectual property and other sensitive information. However, cybersecurity law should not focus on confidentiality to the exclusion of integrity and availability. A comprehensive approach to cybersecurity law will consider all three prongs of the CIA Triad.

A focus on integrity and availability is particularly important in the Internet of Things era, as everyday devices, ranging from medical devices to kitchen appliances to automobiles, are connected to the Internet. 64 Imagine the chaos if hackers manage to disable thousands of pacemakers, or cause vehicles to accelerate to 100 miles per hours as they drive through Times Square. Such attacks have little to do with confidentiality of information, and instead involve the integrity and availability of systems and networks.

B. Where and Whom Are We Securing?

So far, we have determined that cybersecurity law should promote the confidentiality, integrity, and availability of information, systems, and networks. We also must examine which information, systems, and networks should be protected under cybersecurity law. Should U.S. laws focus on bolstering the security of military and civilian government systems? Or should the laws apply equally rigorous requirements for private-sector cybersecurity? This confusion leads to both overlapping legal requirements and blind spots, caused partly by the application of criminal and international law principles to cyberspace. 65 The security of public infrastructure often will face quite different legal requirements than the security of private infrastructure. However, the policymakers should consider the security of both types of systems and networks comprehensively, and understand how the security (or lack thereof) of one affects the other.

The fundamental design of the Internet would make it impossible to effectively address cybersecurity exclusively through the information and infrastructure of the public sector. Government systems intertwine with private networks and rely on the infrastructure of telecommunications companies, cloud storage providers, and others in order to operate. In 2006, the Government Accountability Office recognized that one of the "key challenges" of securing Internet infrastructure was the diffuse control among the private and public sectors. 66 As described in Part IV of this Article: , cybersecurity-related laws largely have not adapted in the decade since that report.

Often, it is difficult to isolate a target of an attack as private or public sector, just as it often is difficult to attribute an attack to a state or nonstate actor. 67 DDOS attacks, ransomware, and other common attack vectors can quickly disperse around the globe, and many do not discriminate between governments, companies, and individuals. 68 Accordingly, any effective cybersecurity law regime will seek to secure both the public sector and private sector. As seen after the Sony Pictures attack, even if the initial target is a private company that lacks strong links to the government, the fallout of an attack on that company can have significant ramifications for the federal government and international relations. Therefore, it would be short-sighted for cybersecurity law to focus exclusively on the public infrastructure and government information.

Accordingly, when policymakers develop cybersecurity laws, they should consider the security of both public and private infrastructure and information. As discussed in more detail in Part IV of this Article: , some U.S. cybersecurity laws focus exclusively on certain sectors and do not consider how they operate in conjunction with laws that address cybersecurity of other sectors. To the greatest extent possible, cybersecurity law should operate harmoniously across sectors. It is inevitable that highly sensitive information and systems - such as in the healthcare sector - may face more rigorous laws than in other areas, but those laws should not function in a black box.

C. How Are We Securing?

We have determined that we want to secure the confidentiality, integrity, and availability of public and private information, systems, and networks. A difficult question - particularly in the context of lawmaking - is how to achieve those goals. This debate often appears to be a binary choice: coercive laws that deter inadequate cybersecurity versus cooperative laws that provide incentives for companies and government agencies to invest in cybersecurity. 69 I propose that cybersecurity law focus on both coercive and cooperative laws, provided that the regulations and incentives for both systems are aligned to achieve similar goals.

The debate over coercive or cooperative laws is not new to the U.S. legal system. For instance, environmental-law scholars for decades have debated the most appropriate way to encourage companies to adapt their business processes to minimize harm to the environment. 70 Advocates of the coercive approach to environmental regulation argue that companies seek to maximize profits, and therefore their "decisions regarding compliance are based on self-interest; businesses comply when the costs of noncompliance outweigh the benefits of noncompliance." 71

A regulatory model based on coercion and deterrence assumes robust government oversight through "extensive government monitoring and inspections coupled with penalties for observed violations." 72 The penalties for noncompliance, therefore, must be sufficiently severe to encourage companies to invest in compliance and, in many cases, forego potential revenue. 73

Critics of the coercive approach in environmental regulation have developed an alternative model, based on cooperation and incentives. Under this model, the government's function is not "to accumulate evidence of violations for subsequent enforcement actions, but rather to provide advice to regulated entities as a means of facilitating compliance." 74 With this approach, companies are not only profit-maximizers, but also "institutions influenced by a mix of civic and social motives." 75 For example, an environmental inspector would suggest improvements rather than impose severe penalties.

The debate over regulation is not unique to environmental law. Policymakers and academics have long debated how to best regulate financial services, 76 consumer safety, 77 and other areas. 78 In most of these areas, the end result is not a binary choice. Legal regimes that apply to specific industries or sectors contain both coercive and cooperative elements. 79

Cybersecurity law should contain a mix of penalty-based regulatory deterrence along with cooperation and incentives. A unilateral focus on coercion through regulation would be misguided, as there are many opportunities for cooperative cybersecurity law. As described above, cyberspace is a combination of public and private infrastructure. A threat to a company's cybersecurity can harm the government, and vice versa. Unlike other regulatory areas, regulators cannot achieve an ideal level of cybersecurity exclusively through the actions (voluntary or otherwise) of the private sector. Although a company's adoption of cybersecurity measures could help to reduce the likelihood of a successful cybersecurity incident, the ultimate chances of a successful attack depend on many other factors, including law enforcement's ability to deter hackers, the security of the company's service providers, and whether the government and companies can quickly communicate with each other about cybersecurity threats and defensive measures. Accordingly, for cybersecurity law to succeed, it must foster effective collaboration between the public and private sectors. As I describe below, we have made some strides toward that goal, primarily with the Cybersecurity Act of 2015. That statute takes the first significant steps to encourage the private sector and federal government to work together to identify and defend against cybersecurity threats. However, the vast majority of the laws broadly considered to be related to cybersecurity are punitive, and they do little to actually encourage investments in cybersecurity.

The U.S. legal system should continue to penalize behavior that degrades our nation's cybersecurity. The regulations, however, should have the ultimate effect of encouraging companies to invest in cybersecurity. Consider the Sony Pictures data breach. Three years earlier, in 2011, Sony's Play Station network experienced one of the largest data breaches in world history when tens of millions of customers' accounts (including credit card data) were compromised by hackers. 80 The company faced costly class action litigation and regulatory inquiries, and it reported that through the end of 2012, the breach cost the company $ 171 million. 81 Despite those regulatory and litigation costs - which are far higher than those associated with an average cybersecurity incident 82 - Sony did not sufficiently change its organizational structure or invest in cybersecurity measures to prevent the Sony Pictures attack three years later. 83 Of course, Sony's failure to properly secure its networks does not mean that all companies would react similarly to the threat of significant fines and litigation costs. However, it demonstrates that for some companies, regulatory and litigation penalties alone will not deter bad behavior.

The questionable efficacy of coercive cybersecurity regulation is traceable, in part, to the relatively low costs of penalties for large companies. Benjamin Dean of Columbia University's School of International and Public Affairs analyzed the breaches at Sony Pictures, Target, and Home Depot, concluding that the breaches cost less than one percent of the companies' annual revenues. 84 This suggests that fines, court awards, and other expenses would need to be significantly higher to encourage corporate executives to invest in cybersecurity, even at the expense of other business units that might actually generate more revenues, such as marketing. Moreover, Dean notes, even if companies suffer significant expenses due to data breaches and other cybersecurity incidents, they often can be at least partially reimbursed by insurance, or they can write off those expenses. 85 This moral hazard, he reasoned, means that it "does not make economic sense for companies like Home Depot to make large investments in information security." 86 The cybersecurity vulnerabilities of individual companies - as seen in recent attacks on Equifax, Dyn, Target, and Ashley Madison - pose a significant risk to individuals and, in some cases, national interests. However, our legal system has not yet created adequate incentives for individual companies to take the necessary - and sometimes costly - steps to reduce the likelihood of cybersecurity attacks.

To create an incentive for greater cybersecurity investments, the government could raise the costs of data breaches to such a high level that even large companies would go out of business if they suffered a large data breach or other attack. The government could accomplish this punitive goal by imposing astoundingly high fines on companies that suffered from cybersecurity incidents, or by allowing plaintiffs to recover large damages in class action lawsuits. However, this strategy would be short-sighted for a few reasons. First, even companies that invest heavily in cybersecurity cannot anticipate every future vector of attack. A hyper-regulatory environment for cybersecurity likely would threaten to penalize even the companies that attempted to make adequate investments in safeguards. Second, and more practically, it is politically unlikely that Congress or state legislatures would impose fines so high that would threaten to put companies out of business.

That is not to say that cybersecurity should be a regulation-free zone. Coercion can play an important and necessary role in cybersecurity law. However, coercive measures should encourage the most effective safeguards, and these measures should be fairly imposed. Most importantly, coercive cybersecurity measures should be used in conjunction with cooperative laws.

Cooperation is particularly important for cybersecurity law, as compared to other business laws, because companies' goals often - but not always - are aligned with those of the government. It would be absurd for a rational Chief Executive Officer to be entirely indifferent to a cyberattack that cripples the company's operations for weeks. For instance, it is safe to say that both the U.S. government and Sony Pictures ultimately want to prevent another such attack. It is in the national interests and Sony's corporate interests to avoid another high-profile embarrassment at the hands of another country. In contrast, corporate and government interests are not necessarily aligned for environmental law. The federal government's goal may be to reduce pollution and negative impacts on the environment, while an automaker's goal may be to efficiently produce cars and maximize value to shareholders. Accordingly, there is far more room for cooperation with cybersecurity than with other areas. When we discuss cybersecurity law, we should consider both cooperation and coercion, and determine the appropriate blend that maximizes effective cybersecurity protections for both the public and private sector.

The coercive and cooperative cybersecurity laws must be harmonious. For instance, if the government determines that medical devices are particularly vulnerable to attacks, it could take a multipronged approach. First, the government could provide companies with the technical guidance to adopt adequate safeguards for the devices, as the National Institute of Standards and Technology ("NIST") often does by developing many cybersecurity controls. 87 Second, the government could create tax incentives for device-makers to invest in the technology and staff necessary to implement the controls. Third, the Food and Drug Administration ("FDA") could refuse to approve new devices that have not incorporated these controls into new products. Fourth, the FDA could impose heavy fines on companies that do not maintain these safeguards and fix vulnerabilities in existing devices. The government need not choose only one of these options. Rather, all four approaches could achieve a common goal.

In short, a well-conceived legal framework will include incentives and penalties, and ensure that those policies achieve a common goal of improving cybersecurity. A legal system that consists entirely of coercion or entirely of cooperation likely will have limited success. The challenge for policymakers is to determine how to use a combination of penalties and incentives to most effectively encourage companies to adopt safeguards.

D. When Are We Securing?

By asking "when are we securing?," we must assess whether cybersecurity laws should focus on events that already have occurred, or if they should attempt to build resilience and defenses to prevent the attacks from occurring in the future.

To the greatest extent possible, cybersecurity law should be forward-looking. Cybersecurity law should prevent cybersecurity incidents from ever occurring, and if incidents do occur, cybersecurity law should help companies and government recover as quickly as possible and prevent future harmful events.

This element of the definition sounds obvious, but many of our laws are backward-looking. They require companies and regulators to litigate the minute details of incidents that already have occurred. In some cases, such retrospection may be valuable, as it can help companies and governments avoid repeating past mistakes. However, the ultimate focus always should be on preventing additional attacks and losses from occurring in the future.

The necessity of a forward-looking component of cybersecurity law is most apparent in any discussion of cyber-resilience, an increasing focus of cybersecurity professionals. 88 In 2013, President Obama issued Presidential Policy Directive 21, which encouraged the cybersecurity of critical infrastructure, such as the electric grid. 89 The Directive defines "resilience" as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions," and it states that "resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." 90 The DHS has stated that resilience measures include business continuity plans, back-up power generators, and durable building materials. 91 This growing - and entirely justified - focus on resilience requires cybersecurity law to be forward-looking and consider not only how to prevent cybersecurity incidents from occurring (either through coercion or cooperation), but also how to recover from cybersecurity incidents once they have occurred.

This is not to say that cybersecurity laws should not address cybersecurity incidents that already have occurred. Companies that have been particularly negligent or reckless with their cybersecurity safeguards should expect to face consequences, such as regulatory investigations, fines, and lawsuits. Large fines and judgments could set an example for other companies and motivate them to invest in stronger cybersecurity safeguards. But the ultimate goal of penalties for past cybersecurity incidents should be deterrence of future events.

E. Why Are We Securing?

To fully define the scope of cybersecurity law, we must fully articulate our ultimate goals. The government should not impose regulations or make substantial investments until there is a more thorough understanding of why it is doing so.

The Sony Pictures attack caused great harm and embarrassment to individuals by allowing egregious privacy violations. The cyberattack also damaged Sony's business interests by exposing its confidential business information and significantly reducing the value of its movies. Finally, the incident threatened U.S. national security and further strained the U.S. government's relationship with North Korea. In short, the Sony Pictures attack (and others like it) highlight three distinct types of harm that cybersecurity law should seek to provide: (1) harm to individuals; (2) harm to business interests; and (3) harm to national security.

The first reason to enact cybersecurity laws is to prevent and mitigate harm to individuals. This harm often involves privacy violations, 92 such as the disclosure of the email messages of Sony executives and the personal information of Sony employees. Such disclosures are highly embarrassing and can have dramatic effects on individuals' lives. Courts and legislators often focus on the financial harm to individuals - such as the consequences of identity theft - caused by data breaches. Indeed, in some consumer lawsuits against companies that have experienced data breaches, courts have refused to find that the plaintiffs have Article: III standing unless the plaintiffs demonstrate that they have actually suffered identity theft as a result of the breach. 93 However, cybersecurity law - both statutes and court rulings - should attempt to prevent not only identity theft and other financial harm; cybersecurity law should address all potential harm to individuals caused by cybersecurity incidents. Daniel J. Solove and Danielle Keats Citron recently articulated this wide spectrum of harms by making a compelling case for courts to recognize the intangible harms of data breaches, such as increased anxiety among consumers:

The harm from an increased risk of identity theft is akin to the risk of contracting a chronic disease. The risk of a data breach is ongoing. Data breach notification letters explicitly inform people that there is a risk of identity theft. Credit monitoring services are offered for one or two years, signaling to plaintiffs an increased risk of theft for that time period. When a person has a reasonable belief that her credit identity is in jeopardy, she is rightly afraid that her creditworthiness is out of her hands. 94

The concern about anxiety-related harms to individuals could be seen after the 2015 data breach of Ashley Madison, a site that allowed users to seek extramarital affairs. 95 Despite the lack of concrete financial harm, the public disclosure of the names of Ashley Madison customers had far-reaching effects, including job resignations and suicides. 96

The second reason to enact cybersecurity laws is to prevent economic harm to companies. On average, a data breach costs a company approximately $ 4 million, and the cost per stolen record is approximately $ 158, according to a recent report by the Ponemon Institute for IBM. 97 According to the report, a U.S. company has a 26% chance of experiencing a breach within 24 months of at least 10,000 records. 98 On aggregate, cybersecurity incidents take a significant economic toll. A recent study estimated that the aggregate cost of data breaches will exceed $ 2 trillion in 2019. 99 Cybersecurity law should attempt to reduce these negative impacts both on individual companies and the economy as a whole.

Finally, cybersecurity law must incorporate the national security interests of the United States. In the Sony incident, these concerns came to the forefront when the United States attributed the attack to North Korea and imposed sanctions, at the time an unprecedented move after a cyberattack. Similarly, Russia's interference in the 2016 U.S. election, via cyberattacks, threatened to fundamentally undercut the confidence and legitimacy of the U.S. democratic system. Even if the attacks target entirely private infrastructure - such as the email system of a political party - the consequences for the public and national security can be far-reaching.

Moreover, attacks on critical infrastructure - even if it is owned and operated by the private sector - can severely harm national security. President Obama recognized this danger in Presidential Policy Directive 21, writing of the need "to strengthen and maintain secure, functioning, and resilient critical infrastructure - including assets, networks, and systems - that are vital to public confidence and the Nation's safety, prosperity, and well-being." 100 To date, the United States has not suffered a devastating cyberattack on critical infrastructure that has caused significant physical damage, but serious critical infrastructure attacks have occurred in other countries. For instance, in 2007, Estonia, a small nation that is highly dependent on the Internet, suffered a massive economic slowdown after its cyber-infrastructure was hit with massive denial-of-service attacks. 101 In 2015, Ukraine suffered a cyberattack that caused blackouts for more than 80,000 people for several hours. 102 U.S. cyber officials have reported a rapid increase in the number of attacks on critical infrastructure, such as the industrial control systems of utilities. 103 Such attacks not only threaten economic and business interests; they can cause injuries, death, and national unrest. Accordingly, national security must be among the top considerations of cybersecurity law.

F. A Proposed Definition of "Cybersecurity Law"

Factoring in all of these considerations, we can develop a broad and flexible definition that provides the general parameters and scope of cybersecurity law. By providing this definition, this Article: does not intend to suggest that cybersecurity law should be limited to a particular set of policy prerogatives. Rather, this Article: identifies areas that should be considered when we develop and refine laws that address cybersecurity:

Cybersecurity law 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.

### Cybersecurity---CIA Triad---AT: Kosseff is Normative/Unpredictable---2NC

#### The article’s not normative---it’s purely attempting to define a previously undefined term---it’s from a well-cited law review called “defining cybersecurity law” and is as predictable as any other interp, which means you should prefer it if it’s better for debate

Kosseff ’18 [Jeff; March; Assistant Professor of Cybersecurity Law, United States Naval Academy. J.D., Georgetown University Law Center; M.P.P., B.A., University of Michigan; Iowa Law Review, “Defining Cybersecurity Law,” 103 Iowa L. Rev. 985, lexis]

This Article: has attempted to formulate a definition of "cybersecurity law" that broadly encompasses our modern conception of cybersecurity, and addresses the most significant cyber-threats that the United States currently confronts. Of course, this definition is only one formulation, based on our nation's current cybersecurity threats. This Article: does not advocate for specific policy changes to improve cybersecurity. Rather, it identifies the key areas of cybersecurity law that are not addressed adequately by current U.S. laws. As policymakers and courts continue to address cybersecurity law, it is increasingly important that they use a common taxonomy and have an understanding of all areas that should be covered by their statutes, regulations, and court rulings.

Providing a taxonomy and a proposed set of goals is only the first step toward focusing the U.S. legal system on the actual cyber-threats that the public and private sector face. This common definition and aspiration will allow for coherence and a broad framework as scholars, policymakers, and legislators evaluate our existing laws and consider new policies. Part V of this Article: provides a starting point for discussion as to how U.S. laws could better achieve the ultimate goals of cybersecurity. Future scholarship can use this definition and these goals to propose solutions to evolving cybersecurity threats.

### Cybersecurity---Excludes Cybercrime---1NC

#### Cybersecurity protects government and private systems from vulnerabilities---excludes cybercrime, which covers fraud and harassment

Graham ’17 [Roderick S. Graham; Oct 18; Assistant Professor of Sociology, Old Dominion University; “The difference between cybersecurity and cybercrime, and why it matters,” https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654]

This story is a cautionary example of a crime that happens online. But most advice for avoiding online dangers – like having long passwords, using two-factor authentication and encrypting data – wouldn’t have helped Amy.

The crime that befell her has nothing to do with cybersecurity. It’s cybercrime, a human-centered crime committed in a digital environment. There are more of these each year: In the U.S. in 2016, 298,728 complainants reported losing more than $1.3 billion in various types of cybercrimes, including romance scams but also involving fraudulent online sales, extortion, violent harassment and impersonation scams, among others. As a social scientist who studies online behavior and as the program coordinator for one of the few cybercrime undergraduate programs in the United States, I find it unfortunate that problems like Amy’s get relatively little national attention, especially compared to cybersecurity.

Understanding the differences

Cybersecurity is not merely a set of guidelines and actions intended to prevent cybercrime. The two types of problems differ substantially in terms of what happens and who the victims are, as well as the academic areas that study them.

Cybersecurity is ultimately about protecting government and corporate networks, seeking to make it difficult for hackers to find and exploit vulnerabilities. Cybercrime, on the other hand, tends to focus more on protecting individuals and families as they navigate online life.

### Cybersecurity---Excludes Nuclear Weapons---1NC

#### Cybersecurity refers exclusively to protecting against risks that arise from being connected to the internet---any other interp is unpredictable and explodes limits, undermining preparedness for all debates

Von Solms ’18 [Basie and Rossouw; March 12; Academy for Computer Science and Software Engineering, University of Johannesburg, Johannesburg, South Africa; School of ICT, Nelson Mandela University, Port Elizabeth, South Africa; Information and Computer Security, “Cybersecurity and information security – what goes where?,” ISSN: 2056-4961]

The definitions and explanations of cybersecurity and cybersecurity governance argued above allow us to present cybersecurity to executive management from the following point of view:

Cybersecurity aims to protect against the risks which arise because one’s organization is connected to the internet in some way or another. The more one is dependent on the internet, i.e. the more services one’s company provides via and using the internet, the bigger the cyber threat and the more comprehensive one’s cybersecurity efforts and commitments should be.

Relating cybersecurity and cybersecurity governance directly to their enterprise’s exposure to cyber space, and explaining that this exposure, widens the potential attack from cyber criminals, should simplify matters. It would furnish executive management and BoDs with a clearer understanding of why cybersecurity governance has become such an important aspect lately, requiring their direct and dedicated attention.

information security and the governance thereof, used to be, and still is, very important in every modern-day enterprise, but cybersecurity and cybersecurity governance have grown to become critical issues today, calling for the direct attention and oversight of BoDs and executive management.

Information security, through the activity referred to as information security governance, was and still is an important responsibility of the BoDs, and it forms part of their general governance mandate. In the light of the recent proliferation of business activities and processes utilizing cyber space (the internet), the extent of the cyber-related risks has increased to such an extent that the BoDs and executive management must pay more attention to the potential (negative) effects thereof. It would certainly be negligent not to do so. For this reason, understanding what cybersecurity entails has become very important to BoDs, to properly govern cybersecurity in this time and age. This is certainly non-negotiable to any modern BoD.

BoDs must demand to be informed and made aware of the enterprise’s involvement in and exposure to cyber space. Once the BoD realizes the extent of the enterprise’s exposure to cyber space, they should ensure that they understand the associated risks of this exposure. Once the BoD has understood (evaluated) the situation, it must demand (direct) that a plan of action to address these risks is put in place. Subsequently, the board must ensure that it regularly gets updated on (monitor) the risk status. These aspects should feature as a permanent BoD agenda item, and they would assist BoDs in properly governing cybersecurity.

#### US nuclear weapons are not connected to the internet---can’t solve any of the aff

Lin ’21 [Herbert; Summer; senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University; Texas National Security Review, <http://dx.doi.org/10.26153/tsw/13986>]

The Energy Department also depends on computer-controlled fabrication machinery that shapes various components of nuclear weapons, such as the high-explosive components used to compress fissile material to critical mass. But because the shapes must be precisely machined to very tight tolerances, the equipment used to fabricate charges is necessarily controlled by computers. Although these computers would not be connected directly to the internet, it must be possible to program them, and they must access data from appropriate databases to fabricate the components in question. Compromising these programs or data could cause the components to be fabricated in ways that are slightly off from the specification. Such imperfections would likely be caught in subsequent inspections, but their deliberate introduction into the fabrication process would be a definite minus for quality control.

### Cybersecurity---‘Property Rights’ Link---1NC/2NC

#### Cybersecurity requires recognizing and enforcing property rights

Craigen ’14 [Dan, Nadia Diakun-Thibault, and Randy Purse; October; Director of Carleton University's Global Cybersecurity Resource; Technology Innovation Management Review, “Defining Cybersecurity,” <https://timreview.ca/article/835>]

A New Definition of Cybersecurity

We propose the following definition, which integrates key concepts drawn from the literature and engagement with the multidisciplinary group:

Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.

We deconstruct this definition as follows:

...the organization and collection of resources, processes, and structures…: This aspect captures the multiple, interwoven dimensions and inherent complexity of cybersecurity, which ostensibly involve interactions between humans, between systems, and between humans and systems. By avoiding discussion of which resources, processes, or structures, the definition becomes non-prescriptive and recognizes the dynamic nature of cybersecurity.

…used to protect cyberspace and cyberspace-enabled systems…: This aspect includes protection, in the broadest sense, from all threats, including intentional, accidental, and natural hazards. This aspect also incorporates the traditional view of cyberspace but includes those systems that are not traditionally viewed as part of cyberspace, such as computer control systems and cyber-physical systems. By extension, the protection applies to assets and information of concern within cyberspace and connected systems.

…from occurrences…: This aspect recognizes that "protections" are intended to address the full range of intentional events, accidental events, and natural hazards. It also suggests that some of the occurrences are unpredictable.

…that misalign de jure from de facto property rights…: This aspect incorporates the two separate notions of ownership and control that dominate discussion of cybersecurity and digital assets introduced in the property rights framework of Ostrom and Hess (2007), which include access, extraction, contribution, removal, management, exclusion, and alienation. Any event or activity that misaligns actual (de facto) property rights from perceived (de jure) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident.

Substantiating Our Definition

As discussed earlier, our definition should engender greater interdisciplinary and collaborative efforts on cybersecurity. Our goal is to “bring together” not to “push apart” or “isolate”. Our success (or failure) can be partly validated if we can demonstrate that:

We can map other definitions of cybersecurity into our definition.

Our definition is unifying and inclusive in that it supports interdisciplinarity.

To assist in the analysis and mapping of the definitions to our new definition, we identified conceptual categories from definitions drawn from the literature as well as our own definition (Table 2). Unless otherwise cited, the category definitions are drawn largely from the Oxford (2014) online dictionary. The exact wordings of the definitions are meant to be as encompassing as possible.

This analysis helps to demonstrate that our new definition is inclusive of key components from a sample of extant and participant definitions. Furthermore, three of the dominant themes – technological solutions; strategies, processes, and methods; and human engagement – are all refinements of the “the organization and collection of resources, processes, and structures used to protect...” component of our definition. The dominant theme of “events” is a refinement of “occurrences.” We also view “referent objects (of security)” as a refinement of “cyberspace and cyberspace-enabled systems.” Retrospectively, we therefore show how our definition is consistent with the dominant themes of cybersecurity and reflects the previously identified distinguishing aspects. Therefore, this mapping illustrates how our definition supports interdisciplinarity.

Conclusion

We have provided a new, more inclusive, and unifying definition of cybersecurity that we believe will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and, thereby, will influence the approaches of researchers, funding agencies, and organizations to cybersecurity challenges. For example, the new definition and associated perspectives could lead to changes in public policy and inform legislative actions.

#### Prefer Craigen’s definition of cybersecurity---robust interdisciplinary engagement and intent to define

Craigen ’14 [Dan, Nadia Diakun-Thibault, and Randy Purse; October; Director of Carleton University's Global Cybersecurity Resource; Technology Innovation Management Review, “Defining Cybersecurity,” <https://timreview.ca/article/835>]

Abstract

Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. In conjunction with an in-depth literature review, we led multiple discussions on cybersecurity with a diverse group of practitioners, academics, and graduate students to examine multiple perspectives of what should be included in a definition of cybersecurity. In this article, we propose a resulting new definition: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to cybersecurity challenges.

Introduction

The term "cybersecurity" has been the subject of academic and popular literature that has largely viewed the topic from a particular perspective. Based on the literature review described in this article, we found that the term is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative. There is a paucity of literature on what the term actually means and how it is situated within various contexts. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. For example, there is a spectrum of technical solutions that support cybersecurity. However, these solutions alone do not solve the problem; there are numerous examples and considerable scholarly work that demonstrate the challenges related to organizational, economic, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts (e.g., Goodall et al., 2009; Buckland et al., 2010; Deibert, 2012). Fredrick Chang (2012), former Director of Research at the National Security Agency in the United States discusses the interdisciplinary nature of cybersecurity:

“A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed.”

In attempting to arrive at a more broadly acceptable definition aligned with the true interdisciplinary nature of cybersecurity, we reviewed relevant literature to identify the range of definitions, to discern dominant themes, and to distinguish aspects of cybersecurity. This research was augmented by multiple engagements with a multidisciplinary group of cybersecurity practitioners, academics, and graduate students. Together, these two activities resulted in a new, more inclusive, and unifying definition of cybersecurity that will hopefully enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby influence the approaches of academia, industry, and government and non-government organizations to cybersecurity challenges. This article reflects the process used to develop a more holistic definition that better situates cybersecurity as an interdisciplinary activity, consciously stepping back from the predominant technical view by integrating multiple perspectives.

Literature Review

Our literature review spanned a wide scope of sources, including a broad range of academic disciplines including: computer science, engineering, political studies, psychology, security studies, management, education, and sociology. The most common disciplines covered in our literature review are engineering, technology, computer science, and security and defence. But, to a much lesser extent, there was also evidence of the topic of cybersecurity in journals related to policy development, law, healthcare, public administration, accounting, management, sociology, psychology, and education.

Cavelty (2010) notes there are multiple interlocking discourses around the field of cybersecurity. Deconstructing the term cybersecurity helps to situate the discussion within both domains of "cyber" and "security" and reveals some of the legacy issues. “Cyber” is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality (Oxford, 2014). It evolved from the term "cybernetics", which referred to the “field of control and communication theory, whether in machine or in the animal” (Wiener, 1948). The term "cyberspace" was popularized by William Gibson’s 1984 novel, Neuromancer, in which he describes his vision of a three-dimensional space of pure information, moving between computer and computer clusters where people are generators and users of the information (Kizza, 2011). What we now know as cyberspace was intended and designed as an information environment (Singer & Friedman, 2013), and there is an expanded appreciation of cyberspace today. For example, Public Safety Canada (2010) defines cyberspace as “the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where… people are linked together to exchange ideas, services and friendship.” Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors (Deibert & Rohozinski, 2010), who represent the range of human intentions.

As for the term "security", in the literature we reviewed, there appeared to be no broadly accepted concept, and the term has been notoriously hard to define in the general sense (Friedman & West, 2010; Cavelty, 2008). According to Buzan, Wæver, and Wilde (1998), discourses in security necessarily include and seek to understand who securitizes, on what issues (threats), for whom (the referent object), why, with what results, and under what conditions (the structure). Although there are more concrete forms of security (e.g., the physical properties, human properties, information system properties, or mathematical definitions for various kinds of security), the term takes on meaning based on one’s perspective and what one values. It remains a contested term, but a central tenet of security is being free from danger or threat (Oxford, 2014). Further, although we have indicated that security is a contested topic, Baldwin (1997) states that one cannot use this designation as “an excuse for not formulating one’s own conception of security as clearly and precisely as possible”.

As a result of our literature review, we selected nine definitions of cybersecurity that we felt provided the material perspectives of cybersecurity:

“Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders.” (Kemmerer, 2003)

“Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.” (Lewis, 2006)

“Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on.” (Amoroso, 2006)

“Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.” (ITU, 2009)

“The ability to protect or defend the use of cyberspace from cyber-attacks.” (CNSS, 2010)

“The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.” (Public Safety Canada, 2014)

“The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure.” (Canongia & Mandarino, 2014)

“The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.” (Oxford University Press, 2014)

“The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.” (DHS, 2014)

Although some of these definitions include references to non-technical activities and human interactions, they demonstrate the predominance of the technical perspective within the literature. As stated by Cavelty (2010), the discourse and research in cybersecurity “necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat”. Accordingly, within their particular context, the definitions above are helpful but do not necessarily provide a holistic view that supports interdisciplinarity. Referring back to Buzan, Wæver, and Wilde’s (1998) discussion of securitization studies, any definition should be able to capture an understanding of the actor, subject, the referent object, the intentions and purposes, the outcomes, and structure. In our review of the literature, we did not find a definition that is inclusive, impactful, and unifying. Cybersecurity is a complex challenge requiring interdisciplinary reasoning; hence, any resulting definition must attract currently disparate cybersecurity stakeholders, while being unbiased, meaningful, and fundamentally useful.

Towards a New Definition

Faced with many definitions of cybersecurity from the literature, we opted for a pragmatic qualitative research approach to support the definitional process, which melds objective qualitative research with subjective qualitative research (Cooper, 2013). In effect, the result is a notional definition that is grounded in objectivity (e.g., an intrusion-detection system) versus supposition (e.g., the intentions of a hacker). This definitional process included: a review of the literature, the identification of dominant themes and distinguishing aspects, and the development of a working definition. This definition was in turn introduced to the multidisciplinary group discussions for further exploration, expansion, and refinement to arrive at the posited definition.

Dominant themes

In our literature review, we identified five dominant themes of cybersecurity: i) technological solutions; ii) events; iii) strategies, processes, and methods; iv) human engagement; and v) referent objects (of security). Not only do these themes support the interdisciplinary nature of cybersecurity, but, in our view, help to provide critical context to the definitional process.

Distinguishing aspects

In conjunction with the emergence of the themes, we formulated distinguishing aspects of cybersecurity, initially through discussion amongst the authors to be refined later through the multidisciplinary group discussions. In the end, we identified that cybersecurity is distinguished by:

its interdisciplinary socio-technical character

being a scale-free network, in which the capabilities of network actors are potentially broadly similar

high degrees of change, connectedness, and speed of interaction

Through the process, there was consensus within the multidisciplinary group to adopt the view that the Internet is a scale-free network (e.g., Barabási & Albert, 1999), meaning it is a network whose degree distribution follows a power law, at least asymptotically. Even though this characterization of the Internet is a subject of debate (e.g., Wallinger et al., 2009), we argue that there are cyber-attack scenarios, and especially the evolution of malware markets, where the capabilities for launching attacks has been largely commoditized, hence flattening the space of network actors.

Throughout the initial part of the process that resulted in a working paper, we intentionally attempted to redress the technical bias of extant definitions in the cybersecurity literature by ensuring that scholars and practitioners contributed to the discussion and were provided an opportunity to review and comment on our initial definition, themes, and distinguishing aspects. To expand the discussion and create additional scholarly dialogue, we posited an original "seed" definition for discussion and further refinement during two three-hour engagements with a multidisciplinary group of cybersecurity practitioners, academics, industry experts from the VENUS Cybersecurity Institute, and graduate students in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada.

Emergent definitions of cybersecurity

Our engagement with the multidisciplinary group primarily consisted of providing selected readings from the literature, an initial presentation and discussion of our own work to date, followed by a syndicate activity related to distinguishing aspects and defining cybersecurity. Three syndicates were formed from the group and they were asked to develop their own definitions. These definitions, along with the authors’ brief critiques, are presented in Table 1. The first two definitions were developed by the authors, whereas the next three definitions arose from group participants.

### Cybersecurity---Broad+Predictble CI---2AC

#### Cybersecurity is the protection and defense of both analogue and digital electronic devices and their communication channels---it can entail both defensive and offensive operations

RWCS ’20 [Real World Cyber Security; April 14; cyber analyst with deep expertise and extensive experience in embedded systems product development and product development security, including hardware security, secure boot, software and firmware security, network and protocol security, operating systems hardening, user interaction and user experience security, industrial design security, data protection and data privacy, cryptographic security, secure software development practices, security test and evaluation, government product security certifications and validation, intellectual property protection, import/export compliance, product liability, supply chain integrity, security in mergers and acquisitions, and corporate security governance; RWCS, “Defining Cybersecurity,” <https://medium.com/swlh/defining-cybersecurity-44cf1b1d6ae0>]

If You Can’t Properly Define Cybersecurity, How Can You Know What It Is?

It’s clear that the cybersecurity industry hasn’t been able to agree upon what cybersecurity is and isn’t. Even NIST, who is responsible for the definition of technical terms used by the U.S. Federal Government, has four different definitions of cybersecurity! At a minimum, there are dozens of different definitions of cybersecurity currently in use. Nearly all are incomplete in scope, some are horridly wrong, and nearly all fail to differentiate between cybersecurity and its information security cousin.

Background

If you look up the definition of “cybersecurity,” most of the answers you get are laughable. Most appear to be written by some “expert” with no actual concept of what cybersecurity is. Nearly all of those definitions sound as though they were written by an academic pontificating what he thinks cybersecurity theoretically should be, without himself ever having done any actual hands-on cybersecurity engineering.

Until July 2019, the sole “official” definition of cybersecurity (as defined by NIST) was: “The ability to protect or defend the use of cyberspace from cyber attacks.” Hyper-informative, wasn’t it? It’s about like telling a man who’s never seen a donut that, “A donut is a pastry shaped like a donut torus.” [See note 1.]

Then, just when you think it can’t get worse, it does. Now NIST can’t even agree within itself what cybersecurity is! It now four different definitions of cybersecurity! None of them tell you anything particularly useful about cybersecurity. Those definitions of cybersecurity are: [2]

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

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

The process of protecting information by preventing, detecting, and responding to attacks.

The prevention of damage to, unauthorized use of, exploitation of, and — if needed — the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

If you search online for a definition of cybersecurity, most definitions are just as bad — if not worse — than the definitions NIST provides. Here are some examples:

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. [3]

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. [4]

May also be referred to as information technology security. [5]

The preventative techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access. [6]

The practice of protecting systems, networks, and programs from digital attacks. [7]

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems. [14]

Notice the pattern? The definitions all talk about defending computers, networks, and data. That isn’t what cybersecurity is. That’s what information security is! Plus, the scope is strictly digital in many cases. Clearly, whoever wrote those definitions have no experience with industrial controls security, where even analogue devices can be at risk of attack. [8]

We have two problems here. First, we have failed to define what cybersecurity adequately or accurately is. Worse, we are trying to somehow shoehorn cybersecurity into being either the same as information security or some subset of information security. It isn’t, and I’ll go into detail why in a minute.

So, if we can’t even agree upon what cybersecurity is, how can we possibly expect to create reasonably secure systems and products that depend upon an in-depth understanding of cybersecurity?

Clearly, we can’t.

And, the problem is compounded by the mindset that the same tools and techniques used for information security are applicable to cybersecurity. Yes, most information security tools and techniques can be applied to cybersecurity, but cybersecurity requires tools and techniques which go far beyond those of information security.

How can we expect to secure our systems when we are using the wrong tools? Or, at best, an incomplete set of tools?

Again, clearly, we can’t.

In my professional opinion, the root of the problem we’re facing is that too many “cybersecurity experts” began their careers as “information security experts” and never have had actual hands-on cybersecurity experience beyond applying partial aspects of cybersecurity to information systems. Thus, we are left with information-centric definitions of cybersecurity, where the “experts” have tried to mold cybersecurity into the shape of information security.

Well, it’s time to break that mold!

Let’s get started with a few definitions.

Definitions

First, let’s define security:

Security is the protection of assets from threats.

That’s fairly clear, but let’s dissect it to ensure the subtleties are covered:

Assets are anything tangible or intangible that has value. In the context of security, usage of the word “asset” usually refers to a “protected asset.”

Protected Assets are any asset protected by a security service. Examples of protected assets could include: data or information (electronic or physical), network and computing infrastructure, software, products and associated intellectual property, people (employees, customers, vendors), real estate and personal property, and utilities and other critical infrastructure. That is, anything of value is a potential protected asset.

Security Services are any threat reduction capability provided by security. There are five generally recognized security services: Confidentiality, Integrity, Availability, Authenticity, and Access-Control. (See the blog post, What Are The Fundamental Services Provided By Security? Hint: CIA Is Not The Answer for additional details.)

Threats are anything with the potential to cause harm. For example, the potential for an attack to occur. Threats can be either intentional (e.g., sabotage) or accidental (e.g., aircraft bird strike), and they can be both man-made events (e.g., human errors, cyber attacks, power failures, and network outages) or natural events (e.g., fires, floods, earthquakes, hurricanes, and tornados). Also, see security threats, below.

Attacks are any action taken against an asset with the intention of causing harm.

Security Threats are anything that may cause harm to a protected asset and/or associated entities. For example, whereas a security threat that discloses personally identifiable information would most likely inflict minimal harm to the asset that held the disclosed information, the disclosure itself could do considerable harm to both the organization’s brand and to the individuals whose information was disclosed. There are seven generally recognized categories of security threats: Denial of Access, Forgery, Spoofing, Repudiation, Unauthorized Access, Unauthorized Disclosure, and Unauthorized Modification (see blog post referenced in Security Services for more details.).

Entities, in the context of security, are anything that attempts to use a protected asset. An entity can be a person, software, robot, or anything else that attempts to use a protected asset.

Okay, I lied: That definition has a lot of subtly buried within it. Hopefully, now the definition of security has a deeper meaning for you.

So, that’s the definition of the mission of security across all of the organization’s security domains. In most organizations, there should be three top-level security domains:

Corporate Security

Information Security

Cyber Security

Now, let’s define each of those security domains.

Corporate Security

Corporate Security is those aspects of an organization’s security not directly related to technology.

That is, in general, corporate security is those aspects of security that pre-date technology or technological security solutions, or are unrelated to technology. Falling under the corporate security domain would be aspects of security related to employee services, safety, environmental services, or facilities; or which are intellectual property, legal, or regulatory in nature. (This is not an all-inclusive list.)

In other words, much of what you would think of as an organization’s security before the advent of digital technologies falls into the corporate security domain.

Today, corporate security often makes extensive use of technology. But, corporate security’s technology is often not under the auspices of information security or cybersecurity. Without close collaboration between security groups, serious gaps in security defenses will occur.

Worse, there often isn’t a corporate security group in the organization. Instead, you often find aspects of corporate security disbursed between multiple (and, often non-communicating) groups, such as human resources, facilities, safety, plant protection, legal, risk management, and environmental.

I plan to discuss corporate security in more detail in an upcoming blog post, Corporate Security: The Forgotten Security Domain.

Information Security

Information Security is the protection of information in any form and at all times.

That’s pretty much the classic paragraph-long definition of information security, summarized into one sentence.

Now, let’s dissect it to get a deeper understanding of what that means.

Security is the protection of assets from threats.

Protection is the rendering safe from harm. Protection is passive security. That is, security that does not offer a response to an attack. It is equivalent to putting a lock on a door to secure your house.

In any form means it includes both physical (e.g., printed documents) and electronic (e.g., files and databases) information.

At all times means the information must be protected, whether it is at rest (i.e., in storage), in use, or in motion (e.g., electronic information sent over a network, or a printed document transported by a courier).

Thus, we define information security as the protection of information. Note that we didn’t place any constraints upon the scope of protection. That is, if we have to protect computers and networks to protect information, then that would be within the scope of information security. But, keep in mind that the objective is the protection of information. Nothing more. Nothing less.

Cyber Security

We’ve already shown that there isn’t a commonly agreed-to definition for cybersecurity. Now, I’m going to propose a definition for cybersecurity which covers all aspects of cybersecurity — something which is lacking from other definitions — while providing a clear distinction from information security. [10]

Cybersecurity is the protection and defense of both analogue and digital electronic devices, their communications channels, and their processing-and-control logic and algorithms.

Now, let’s dissect that definition to get a deeper understanding of what it means and its ramifications.

Security is the protection of assets from threats.

Protection is the rendering safe from harm. Protection is passive security. That is, security that does not offer a response to an attack. It is equivalent to putting a lock on a door to secure your house.

Defense is an action taken to resist an attack. Defense is active security. This means that you have dynamic security with ever-changing defenses — which can include offensive actions to stop an attack. It is the equivalent of confronting an intruder in your house with a loaded weapon.

Digital Devices are any electronic device that uses discrete data and processes for all its operations. This clearly includes computers, cell phones and tablets, routers, switches, WiFi access points, and firewalls, but it also includes all other digitally networked devices, such as all IoT devices, VoIP telephones, digital security cameras, smart badge readers, etc.

Analogue Devices are any electronic device that uses continuous data and processes for all its operations. This would include landline telephones, fax machines, most nuclear reactor control systems, older radar systems, older industrial controls, some satellite and other space systems controls, and literally thousands of other devices. In industrial controls situations, analogue devices often serve as failsafe backups to digital controls.

Communications Channels are the means by which a device is connected to other devices. For analogue device communications, this could be a simple wire or wire-pair, coax cable, analogue radio, or similar technologies. For digital device communications, it would include any type of wired or wireless network. For digital to analogue device communications, it could include any of the previously mentioned means of analogue device communications used to communicate to an analogue interface in the digital device.

Processing Logic and Algorithms are the means by which a device accomplishes its designated purpose. For analogue devices, this is all done in hardware. For digital devices, this includes both hardware and software (microcode, firmware, operating systems, applications, etc.).

Control Logic and Algorithms are the means by which a device regulates its processing. For analogue devices, this is all done in hardware. For digital devices, this includes both hardware and software (microcode, firmware, operating systems, applications, etc.).

Now, let’s put the phrases together and detail the bigger picture.

Is the protection and defense is cybersecurity’s first significant difference from information security. Cybersecurity not only offers protection like information security, but it also offers defense. In other words, cybersecurity can take the offensive actions necessary to defend systems.

Of both analogue and digital electronic devices is the next significant difference from information security, as information security’s tools seldom address analogue devices. It is also different in that information security offers protection of non-electronic information (e.g., printed), whereas cybersecurity only deals with electronic devices and their data. [11]

This definition means that protection and defense are also offered to the electronic devices (components) combined to construct a more complex electronic device. For example, protection and defense would be offered to CPUs, GPU, FPGAs, ASICs, NICs, DACs, memory, controllers, and all the other various analogue and digital components that comprise a modern end-purpose electronic device, such as a smartphone or a computer. In other words, cybersecurity protects and defends any security-sensitive electronic device, be it analogue or digital, and be it an end-purpose device or a component of such a device.

Their communications channels is again a difference between cybersecurity and information security. Cybersecurity provides both protection and defense of the electronic communications channels themselves, both analogue and digital. Whereas, information security only provides for the protection of the information conveyed over those communications channels.

Additionally, information security also provides for the protection of information communicated by non-electronic means (e.g., printed documents), which is outside the scope of cybersecurity.

And their processing-and-control logic and algorithms is the final difference between cybersecurity and information security. Cybersecurity offers protections to both hardware and software, and can take actions to defend both from attack. By contrast, information security only provides passive protection to information.

So, that is the definition of cybersecurity and an explanation of its scope.

To recap, cybersecurity provides security for all electronic technology, except for the information processed by such technology (information is protected by information security).

Or, another way to view the difference between information security and cybersecurity is that information security secures the information itself, and cybersecurity secures everything that creates, uses, processes, stores, or communicates that information.

Where Information Security Fails Us

In my blog introduction, I state that “trying to treat cybersecurity problems as though they are information security problems” is one of the fundamental mistakes we are making in security today. The lack of an understanding of the differences between information security and cybersecurity is the root cause of this problem.

As we have seen in the preceding definitions, information security is “data-centric,” and cybersecurity is “device-centric.” Trying to apply information security principals to “device security” creates two problems: First, you can’t adequately secure “hardware” using the same controls used to secure data; And second, there is nothing in information security that provides for an active defense.

Let’s look at some of the issues that the premises supporting information security fail to address. To do this, we’ll examine an example from product security.

The overwhelming insecurity of IoT products has filled the news recently. Why? Many would say that it’s a simple matter of companies trying to produce products on the cheap. However, I would argue that the issue is more likely the product’s designers’ failure to recognize the potential for security problems in their products.

I believe that fundamentally, such product failures are compounded by an incomplete view of security: a view driven by an information security focus. A focus that, for embedded systems products (such as IoT devices), is incomplete, at best. Why incomplete? Because most security issues with IoT devices are not information related. Rather the problems are with the devices themselves.

Let’s begin by listing some of the security questions that product designers should be asking, but are obviously not asking. And, with most product security practitioners coming from an information security background, those product security architects probably do not even know they should be asking these questions.

After all, why should they know better? Nothing they had learned in the scope of information security would indicate that these are issues with which to be concerned. The types of product security questions (that is, cybersecurity questions) which all product security architects should be asking include:

How do you prevent reverse engineering of the product?

How do you prevent tampering with the product?

How do you prevent the production of unlicensed clones of the product?

How do you prevent access to the hardware interfaces used for development debugging of the product?

How do you prevent access to the hardware interfaces used for manufacturing testing of the product?

How do you perform failsafe firmware updates of the product (such that a failed update does not brick the product)?

How do you prevent unauthorized modification of the product’s firmware?

How do you prevent your firmware from running on third-party devices?

How do you ensure the integrity of your supply chain?

How do you prevent unauthorized modification of the device itself?

How do you prevent misuse of the device from damaging the device itself (e.g., using a USB port on a device for other than its intended purpose, and drawing too much power)?

How do you prevent misuse of the device from creating a safety incident (e.g., using an aerosol can to create a vapor fog to trigger a motion detector to unlock a door)?

How can this device be abused by an attacker to cause harm?

How can we verify that our UI is always unambiguous to its intended audience?

How can we verify that our UX is always intuitive to its intended audience?

How can we verify that our UI creates neither security or safety issues?

How can we verify that our ID creates neither security or safety issues?

And this is just a very small sample of the questions that every product development organization should be asking, but which is clearly failing to occur.

Now, I can already hear the objections: “These are hardware engineering issues, not information security issues, and that’s why they’re not covered by information security.” Well, that’s half wrong and half right. Wrong, in that they are not hardware engineering issues; rather, they are hardware security issues. Right, in that they are not information security issues; rather, they are cybersecurity issues. [12]

These, and tens of thousands of other similar issues, are being left unaddressed during product development because information security doesn’t address these types of issues. Nor should it, as those issues are cybersecurity issues and not information security issues.

Nothing in an information security professional’s background or training would prepare them to even know that they should be asking the types of questions I posited. And, that’s what should be expected, because these are not information security issues and I would not expect an information security professional even to have half-a-clue that such problems exist. It’s for precisely this reason that cybersecurity exists and is different from information security.

The problem is really simple: Information security exists to protect information. Nothing in the fundamentals of information security was ever intended to secure anything other than information. Thus, we need to stop trying to use an information security mindset to secure “stuff” that isn’t information. We must recognize that cybersecurity’s scope is beyond that of information security, and thus apply cybersecurity principals to cybersecurity problems.

Defense

We also need to remember that cybersecurity allows for active measures to defend devices. There’s a reason that the military and intelligence agencies refer to their security operations as cybersecurity, and that’s because they take active countermeasures to attacks. You don’t do that when your objective is to secure information. In fact, that entire concept is an anathema to the information security principals and mindset.

Cybersecurity defense is a big rabbit hole I don’t plan to explore further in this posting, other than to remind you that cybersecurity’s objective is the protection and defense of assets.

Summary

There is an old saying, “When the only tool you have is a hammer, everything looks like a nail.” With no real cybersecurity experience, too many information security experts are trying to hammer cybersecurity into becoming an information security nail. We need to reset the thinking of those information security professionals and teach them that cybersecurity is more like a bolt than a nail, and that you use a wrench, not a hammer, when installing or removing a bolt.

Now, a quick review…

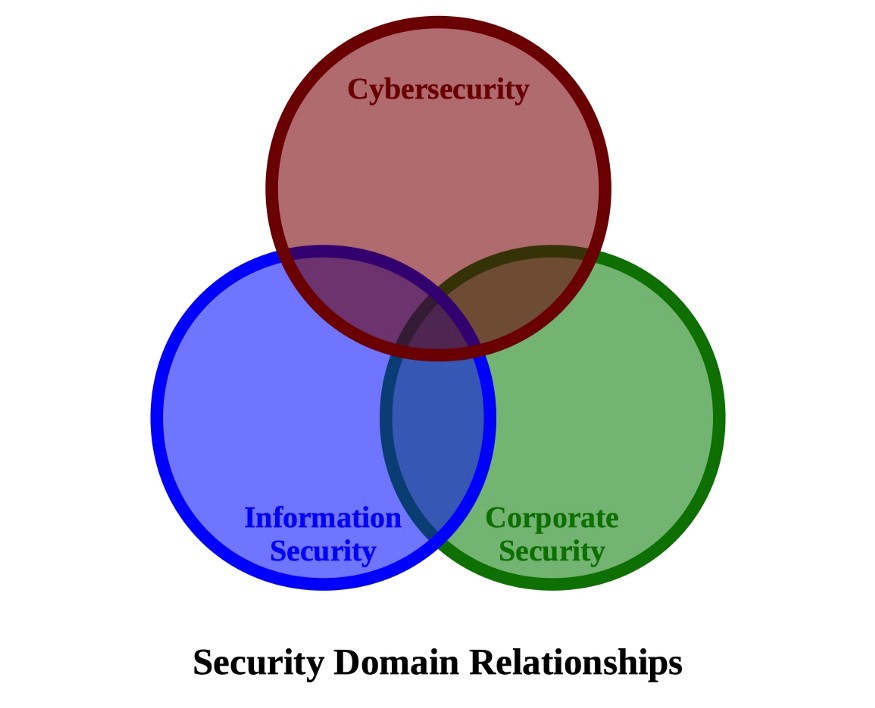
In most organizations, there are three security domains with which it must be concerned:

Corporate Security, which protects (and sometimes defends) people; and real, corporate, and intellectual property.

Information Security, which protects information (data).

Cybersecurity, which protects and defends: hardware, communications, and software.

The diagram below illustrates those relationships among the organization’s security domains.



We established the following definitions in support of those security domains:

Security is the protection of assets from threats.

Corporate Security is those aspects of an organization’s security not directly related to technology.

Information Security is the protection of information in any form and at all times.

Cybersecurity is the protection and defense of both analogue and digital electronic devices, their communications channels, and their processing-and-control logic and algorithms.

Trying to treat cybersecurity problems as though they are information security problems is one of the fundamental mistakes we are making in security today. We have to remember that information security is “data-centric,” and cybersecurity is “device-centric.” Trying to apply information security principals to “device security” creates two problems:

You cannot adequately secure “hardware” using the same controls used to secure data, and

There is nothing in information security that provides for active defense.

If you search the Internet, you will find that many so-called “information security experts” claim that cybersecurity is a subset of information security. But, compared to information security, cybersecurity has a substantially broader scope, addresses a more complex set of security threats, and offers active defenses not provided by information security.

If anything, we should view information security as a subset of cybersecurity. However, that’s not accurate either, as what those two domains are attempting to secure is different — data vs. hardware, software, and communications. Some overlap between the two is unavoidable, but at the most fundamental levels, they are attempting to solve different problems. [13]

Thus, we need clear, concise, unambiguous definitions of both cybersecurity and information security.

Hopefully, you will find the definitions provided here meet those criteria.

So, don’t let alleged information security experts try to tell you what is and is not cybersecurity! Those so-called “information security experts” are precisely that, and nothing more, because they clearly do not understand cybersecurity!

Please leave cybersecurity to actual cybersecurity practitioners.

Thank you!

### Cybersecurity---Includes Preemption/OCO’s---2AC

#### Cybersecurity, especially for NATO, entails preventive and preemptive action.

Panagiotis ’19 [Marios; 2019; Efthymiopoulos Journal of Innovation and Entrepreneurship, “A cyber-security framework for development, defense and innovation at NATO,” 8:12 Springer Open]

Characteristics of cyber-Security

Cyber-security is a strategy of both preventive and/or pre-emptive action. It allows for technological growth and advancement; it also allows for innovation and entrepreneur- ship. It introduces us to a new virtual reality that we created and are standing at: the worldwide web, its methods and opportunities, is by now an integrated part of our lives. All elements that we are working with or at professionally or privately at some given time rely or depend on technological advancements that make our life easier and at the same time more complicated while we are in need for constant and enhanced cyber-security protection of our data and also virtual way of life.

Strategically, constant security resilience is of essence. Security as policy is a protection method. Among others, it reflects government policies. In the virtual world, through cyber-security, democracy, development, sustainability, and growth, innovation and entrepreneurship can take place.

Cyber-security is both a strategy and operational framework, a field of operational capacity, an element of cross-disciplinary and trans-disciplinary approach that is fit to all levels of socio-political, economic, engineering, IT, legal, and security-led levels of theoretical approach and practicability uses and issues.

A cyber-security strategy is holistically and politically business oriented; it is entrepre-neurial and innovative. Cyber-security in the field of defense is a continued struggle for technological methods of defense development, growth, innovation, democracy, and continuity toward the convergence of a society that is very much depended on technology.

Resilience in cyber-security is reflected in multiple fields. As long as there is a cooperative or global cyber-security strategy. The necessity for a joined cooperative strategic and operational capacity needs to be displayed and pointed out. Safeguarding and enhancing methods and tools of protection against malicious attacks that may involve one or more countries, institutions, businesses, or agencies.

An alliance cyber-security becomes a policy framework for technological continuity, a multinational aspect of cooperative approach that enhances elements of pluralism of Democracy; it will help boost interconnectedness and will boost security efforts to meet all security threats symmetrical and asymmetrical.

National securities and defense strategies rely solely on national cyber-security protection policies and application methods; how cooperation can and will be achieved; information agility and technological advance mechanisms; considering the multidimensional level of threats and challenges. Yet risk analyses and threat analyses are to this extend considered only as national. The article proposes for a joined cooperative approach on Grand Cyber-Security Strategy. A strategy that at an age of interconnect- edness and operational creativity will provide an efficient political and military framework to work on, a legal framework that will in turn allow for operational deliverables through a cyber-security command such like the new cyber-security center in Mons Belgium, a decision-taken by Heads of States and Governments, at the recent Brussels NATO Summit of July 2018.

Setting the stage

Cyber-security is yet to be globally, legally, operationally, and strategically defined. The scale of a security perspective is more attractive at this time considering the geostra- tegic challenges and threats. The possibility of innovation and entrepreneurship in the field is also a tangible reality, due to the necessary research and development methods. More so, the possibility of an open market economy sharing of knowledge and technological skills makes security and cyber-security or defense for that matter more attractive. What lacks in the world wide legal and political framework of operations, exchange of information and protectiveness from new sources or methods that can be deemed as elements of infiltration.

The article's aim is to examine and recommend a global strategic framework for op-erational capacity and management resilience between allied and cooperative partners in the field of cyber-security. The current article is a follow up of prior scientific publications made in 2014 first and later in 2018, on NATO's cyber-security strategy, presented through a framework of Cyber-Development, Cyber-Democracy, and Cyber-Defense (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018). The aim is to converge diversified information on cyber-security, in a single strategic framework; reflect to the actual practical needs in understanding operations and tactical ability to deliver in multi-complex and dimensional world through management and operational efficiency capabilities. The article requests interoperability of aims and objectives under a global framework of cyber-security; through a strategic framework on cyber-security, global law can be proposed, defined, and adopted by the international community. The strategic framework will define structures that are needed to be put in place on a global scale, when reflecting issues of cyber-security and inclusive for NATO. It will define threats and challenges, as cyber-attacks are real. Cyber-security is not an asymmetrical or hybrid threat, but an existential one. Its destructive capacity can be multi-leveled and can also lead to human casualties. The future of e-safety lays at both a global estimation framework of what constitutes cyber-security and how we react to it; it lays in between cooperation of allies and members of wider alliances, against specified or approximate threats. Yet, its framework of aims and objectives, management, command and control, and operations will be defined and decided by allied parties only such as is the case of NATO.

## Predictability

### Plain Meaning---2AC

#### Prefer plain meaning.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “Ordinary-Meaning Canon,” Ch. 6]

Words are to be understood in their ordinary, everyday meanings—unless the context indicates that they bear a technical sense.

“The enlightened patriots who framed our constitution, and the people who adopted it, must be understood to have employed words in their natural sense, and to have intended what they have said.”

Chief Justice John Marshall,

Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1, 71 (1824).

The ordinary-meaning rule is the most fundamental semantic rule of interpretation.1 It governs constitutions, statutes, rules, and private instruments. Interpreters should not be required to divine arcane nuances or to discover hidden meanings. Justice Joseph Story’s words are as true today as they were when written in the middle of the 19th century, and they are true not just of constitutions but of all other legal instruments:

[E]very word employed in the constitution is to be expounded in its plain, obvious, and common sense, unless the context furnishes some ground to control, qualify, or enlarge it. Constitutions are not designed for metaphysical or logical subtleties, for niceties of expression, for critical propriety, for elaborate shades of meaning, or for the exercise of philosophical acuteness or judicial research. They are instruments of a practical nature, founded on the common business of human life, adapted to common wants, designed for common use, and fitted for common understandings.2

### General Terms---2AC

#### General terms like “security cooperation” should be understood broadly.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “General-Terms Canon,” Ch. 9]

General terms are to be given their general meaning (generalia verba sunt generaliter intelligenda).

Without some indication to the contrary, general words (like all words, general or not) are to be accorded their full and fair scope. They are not to be arbitrarily limited. This is the general-terms canon, which is based on the reality that it is possible and useful to formulate categories (e.g., “dangerous weapons”) without knowing all the items that may fit—or may later, once invented, come to fit—within those categories.

### Intent To Exclude Unnecessary---2NC

#### A definition need not specify something is excluded to actually exclude something.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “General-Terms Canon,” Ch. 10]

The expression of one thing implies the exclusion of others (expressio unius est exclusio alterius).

Expressio unius, also known as inclusio unius, is a Latin name for the communicative device known as negative implication. In English, it is known as the negative-implication canon. We encounter the device—and recognize it—frequently in our daily lives. When a car dealer promises a low financing rate to “purchasers with good credit,” it is entirely clear that the rate is *not* available to purchasers with spotty credit.

### Intent to Exclude Necessary---2AC

#### Disagreed with the above.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “General-Terms Canon,” Ch. 10]

Virtually all the authorities who discuss the negative-implication canon emphasize that it must be applied with great caution, since its application depends so much on context.1 Indeed, one commentator suggests that it is not a proper canon at all but merely a description of the result gleaned from context.2 That goes too far. Context establishes the conditions for applying the canon, but where those conditions exist, the principle that specification of the one implies exclusion of the other validly describes how people express themselves and understand verbal expression.

The doctrine properly applies only when the unius (or technically, unum, the thing specified) can reasonably be thought to be an expression of all that shares in the grant or prohibition involved. Common sense often suggests when this is or is not so. The sign outside a restaurant “No dogs allowed” cannot be thought to mean that no other creatures are excluded—as if pet monkeys, potbellied pigs, and baby elephants might be quite welcome. Dogs are specifically addressed because they are the animals that customers are most likely to bring in; nothing is implied about other animals. On the other hand, the sign outside a veterinary clinic saying “Open for treatment of dogs, cats, horses, and all other farm and domestic animals” does suggest (by its detail) that the circus lion with a health problem is out of luck. (Notice how ejusdem generis [§ 32] also comes into play with this example.) The more specific the enumeration, the greater the force of the canon:

### “Include” Does Not Exclude---2AC

#### When a “definition” is based on the word “include,” it does not exclude any aff.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “Presumption of Nonexclusive Include,” Ch. 15]

The verb to include introduces examples, not an exhaustive list.

In normal English usage, if a group “consists of” or “comprises” 300 lawyers, it contains precisely that number. If it “includes” 300 lawyers, there may well be thousands of other members from all walks of life as well. That is, the word include does not ordinarily introduce an exhaustive list, while comprise—with an exception that we will discuss shortly—ordinarily does. That is the rule both in good English usage1 and in textualist decision-making.2 Some jurisdictions have even codified a rule about include.3

### No Redundancy---2NC

#### Reject interpretations that make words redundant.

Scalia ’12 [Antonin Scalia and Bryan Garner; 2012; Justice on the Supreme Court of the United States; American lawyer, lexicographer, and teacher; Reading Law: The Interpretation of Legal Texts, “Surplusage Canon,” Ch. 26]

If possible, every word and every provision is to be given effect (verba cum effectu sunt accipienda1). None should be ignored. None should needlessly be given an interpretation that causes it to duplicate another provision or to have no consequence.

“These words cannot be meaningless, else they would not have been used.”

United States v. Butler,

297 U.S. 1, 65 (1936) (per Roberts, J.).

The surplusage canon holds that it is no more the court’s function to revise by subtraction than by addition. A provision that seems to the court unjust or unfortunate (creating the so-called casus male inclusus) must nonetheless be given effect. As Chief Justice John Marshall explained: “It would be dangerous in the extreme, to infer from extrinsic circumstances, that a case for which the words of an instrument expressly provide, shall be exempted from its operation.”2 Or in the words of Thomas M. Cooley: “[T]he courts must . . . lean in favor of a construction which will render every word operative, rather than one which may make some idle and nugatory.”3 This is true not just of legal texts but of all sensible writing: “Whenever a reading arbitrarily ignores linguistic components or inadequately accounts for them, the reading may be presumed improbable.”4

### Words and Phrases Defense---2NC

#### Words and Phrases is qualified.

Words and Phrases ’4 [Words and Phrases Dictionary; 1904; written by Members of the Editorial Staff of the National Reporter System; Volume 1, “A/Casting Vote,” p. iii]

This compilation represents the first systematic attempt to present in complete and available form the vast quantity of judicial interpretation and construction of the meaning of words and phrases found in the reported decisions of the American appellate courts. It has been over ten years in preparation, and has involved enormous editorial labor and research. The effort has been made to secure all the words judicially defined and all the definitions of each word. In collecting the material recourse has been had in all cases to the opinions of the courts as the original sources, and the work is the result of a page-to-page examination of the reported American cases. A careful search for definitions for words and phrases has also been made in all the latest codes and revisions of statutes, state and federal.