# Topicality – BEJJK Lab – 7Wk

**Special thanks to the students that worked on this file: Anish, Drew, Janise, Leah, Lucy, Stephen and Win!**

## Notes

# Resolved

## 1NC---Resolved

#### Resolved requires a specific course of action

AHD 6

(American Heritage Dictionary, http://dictionary.reference.com/browse/resolved)

INTRANSITIVE VERB:1. To reach a decision or make a determination: resolve on a course of action. 2. To become separated or reduced to constituents. 3. Music To undergo resolution.

#### Violation – the Aff read 7 plans by including “one or more of the following”

---any one, any two, or all three

Dahmani 87 – Martinus Nijhoff publishers

(Mohamed, “The Fisheries Regime of the Exclusive Economic Zone,” p. 70-71)

Secondly, the use of the expression 'sub-region or region' is also ambiguous. If the word 'or' means a choice for land-locked and geographically disadvan-taged states then obviously a region might be a better area than a sub-region. Whereas for a coastal state in whose EEZ fishing is to take place it would be advantageous to limit fishing rights to the EEZ's of states of the sub-region rather than the region as a whole. There are two possible interpretations. The first is chat where there is a sub-region land-locked and geographically disad-vantaged states' participation applies only to such sub-region. In other words, it will apply to a region only when there is no generally recognised sub-region, as in Latin America where the Caribbean is generally regarded as a sub-region of the Latin American region. A second, more favourable interpretation to land-locked and geographically disadvantaged states is that participation applies to both sub-region and region.¶ Similarly, problems of interpretation may also arise in connection with the definition of geographically disadvantaged states. Article 70(2) docs not proceed on the basis of any definition of such states.

#### Vote neg:

#### ---Aff conditionality – “one or more of the following” enables aff choice, always favors the aff because they get to choose in the last speech.

#### ---Ground – stable plan text is only way to garner DA or counterplan competition – has a tangible effect because discourages introducing DAs about either

#### ---Jurisdiction – if you don’t know definitely what the plan does, you can’t vote for it

Burstyn 11 – JD, not the Copeland winner

(Joseph Burstyn, JD “Void for Vagueness Doctrine,” 2011, http://law.jrank.org/pages/11152/Void-Vagueness-Doctrine.html)

If a person of ordinary intelligence cannot determine what persons are regulated, what conduct is prohibited, or what punishment may be imposed under a particular law, then the law will be deemed unconstitutionally vague. The U.S. Supreme Court has said that no one may be required at peril of life, liberty, or property to speculate as to the meaning of a penal law. Everyone is entitled to know what the government commands or forbids. The void for vagueness doctrine advances four underlying policies. First, the doctrine encourages the government to clearly distinguish conduct that is lawful from that which is unlawful. Under the Due Process Clauses, individuals must be given adequate notice of their legal obligations so they can govern their behavior accordingly. When individuals are left uncertain by the wording of an imprecise statute, the law becomes a standardless trap for the unwary.

## 2NC---Overview

#### The aff read 7 plans, not 1- this isn’t 1982

-ai

-cyber

-biotech

-ai + cyber

-ai + biotech

-biotech + cyber

-ai + biotech + cyber

#### Three impacts:

#### FIRST – 2ar sandbagging – they will choose the strategic version of the plan based on negative strategy. For example, if we said the plan was insufficient to solve the advantage, they would say they are ai, cyber, AND biotech, but if we read a cyber da, they’d say they were just ai

#### SECOND – the plan text is key, and it’s meaning should be up for debate. Letting the aff exclusively decide the meaning of the plan tanks counterplan competition and motivates aff laziness because who needs to cut answers when they can just say no link

#### THIRD – presumption – even a hint of uncertainty about the conduct done by the plan means the plan should be void

## 2NC---Interp: Resolved

#### Resolved means determined and firm in intent

Random House 6

(Unabridged Dictionary, http://dictionary.reference.com/browse/resolve)

re·solved Audio Help /rɪˈzɒlvd/ Pronunciation Key - Show Spelled Pronunciation[ri-zolvd] –adjective firm in purpose or intent; determined.

## 2NC---Impact

#### Jurisdiction: vagueness means that you vote negative even if the violation is minor

Shannon 2 – Professor of Law

(Bradley Scott, Associate Professor of Law, ARTICLE: ACTION IS AN ACTION IS AN ACTION IS AN ACTION, Washington Law Review, January, 2002, 77 Wash. L. Rev. 65, pg. ln)

The first answer to this question is, why should we not care? If proper terminology (of whatever type) is readily available and comprehendible, why should one not want to use it? Does one really need a reason for not misusing any word, technical or otherwise? In other words, though many misuses of Rules terminology might not seem to cause serious problems, surely that is not an argument in favor of a disregard of proper Rules terminology, particularly where the cost of using proper terminology is negligible. n79 The second answer to the question why we should care about the use of proper Rules terminology goes to the cost of using improper terminology even in seemingly trivial contexts. Understanding legal concepts is difficult enough without the confusion created when an inappropriate term is used to represent those concepts. And this is true regardless of how minor the misuse. In some sense, every misuse of legal language impedes the understanding - and, consequently, the progress - of the law. There are at least two additional reasons, somewhat unique to the law, why one should always strive to use proper Rules terminology. The first reason relates to the nature of the Rules as law (or, as some prefer, a source of law). Many bodies of professional terminology might be considered in some way authoritative, in that reliance thereon not only is widespread, it is almost viewed as compulsory. n80 But the Rules [\*86] essentially are of the same character as a federal statute. n81 And despite the fact that there is often no direct penalty for the misuse or disregard of Rules terminology, n82 the Rules, by their nature, nonetheless command respect and, in some sense, obeisance. n83 Another reason for using proper legal terminology goes to persuasion. As most good attorneys know, using proper procedural terminology is almost as important as using the Rules themselves properly, as the use of proper terminology enhances the perceived credibility and competence of the proponent, and helps convey the image of the proponent as the giver of the truth. n84 Though this is probably true of every profession, the [\*87] stature of argument, and thus of persuasion, in legal discourse magnifies its importance in the law. n85

#### Strong negative presumption – even if they intended for the plan to be read a certain way, the judge should not apply sloppily worded laws, anything else is unconstitutional and prohibitive to clear DA and counterplan links

Burstyn 11 – JD, not the Copeland winner

J(oseph Burstyn, JD “Void for Vagueness Doctrine,” 2011, http://law.jrank.org/pages/11152/Void-Vagueness-Doctrine.html)

Third, the void for vagueness doctrine discourages judges from attempting to apply sloppily worded laws. Like the rest of society, judges often labor without success when interpreting poorly worded legislation. In particular cases, courts may attempt to narrowly construe a vague statute so that it applies only to a finite set of circumstances. For example, some courts will permit prosecution under a vague law if the government can demonstrate that the defendant acted with a SPECIFIC INTENT to commit an offense, which means that the defendant must have acted wilfully, knowingly, or deliberately. By reading a specific intent requirement into a vaguely worded law, courts attempt to insulate innocent behavior from criminal sanction. However, such judicial constructions are not always possible. Ultimately, a confusing law that cannot be cured by a narrow judicial interpretation will not be submitted to a jury for consideration but will be struck down as an unconstitutional violation of the Due Process Clauses.

#### Vote neg on presumption – the plan will be intentionally misinterpreted by forces of inertia

Crabble 88 – Honorable Justice, Professor of Law @ West Indies

(The Honorable Mr. Justice V.C.R.A.C. Crabbe, Visiting Professor of Law & Director, Legislative Drafting Programme, Faculty of Law, University of the West Indies, Barbados, Statute Law Review 2, Summer)

And advocates would always argue as to where a comma or a semi-colon should be placed. This is done because a particular interpretation favours a particular presentation of a particular line of argument. It cannot be otherwise. Out of the anvil of argument justice, as far as humanly possible, is done. And the legislative draftsman, nonetheless will have to use punctuation marks in drafting the law. The less room he leaves for argument the better. And we cannot ignore the observation of Stephen J., that although Acts of Parliament “may be easy to understand, people continually try to misunderstand.” The legislative draftsman must, therefore not only “attain to a degree of precision which a person reading in good faith can understand, but it is necessary to attain if possible to a degree of precision which a person reading in bad faith cannot misunderstand. It is all the better if he cannot pretend to misunderstand it.”34

# Increase

## 1NC---Increase = Pre-Existing

#### Increase means to expand a pre-existing program

Oxford Learner’s Dictionaries (“Increase” <https://www.oxfordlearnersdictionaries.com/us/definition/academic/increase1>; Accessed 7/11/22) //LVL

to become or make something greater in size, amount or degree

#### Violation – the aff creates () – that’s not a pre-existing program

#### Voter for

#### Limits – they justify affs creating entirely new programs and NATO initiatives which skews the negative research burden

#### Ground – avoids core neg generics that are based on increased security cooperation of existing NATO programs

## 2NC---Pre-Existing

#### US Code describes security programs as activities that contribute to existing coalitions

Legal Information Institute (“10 U.S. Code § 333 - Foreign security forces: authority to build capacity” Cornell Law School Legal Information Institute <https://www.law.cornell.edu/uscode/text/10/333>; Accessed 7/10/22) //LVL

(a)Authority.—The Secretary of Defense is authorized to conduct or support a program or programs to provide training and equipment to the national security forces of one or more foreign countries for the purpose of building the capacity of such forces to conduct one or more of the following:

(1)Counterterrorism operations.

(2)Counter-weapons of mass destruction operations.

(3)Counter-illicit drug trafficking operations.

(4)Counter-transnational organized crime operations.

(5)Maritime and border security operations.

(6)Military intelligence operations.

(7)Air domain awareness operations.

(8)Operations or activities that contribute to an existing international coalition operation that is determined by the Secretary to be in the national interest of the United States.

(9)Cyberspace security and defensive cyberspace operations.

### XT Increase=expansion

#### Increase is to grow in quantity

Merriam Webster Dictionary, 22 (Last updated: 7/4/22; “Increase”; Merriam Webster Dictionary <https://www.merriam-webster.com/dictionary/increase>; Accessed 7/11/22) //LVL

INCREASE, ENLARGE, AUGMENT, MULTIPLY mean to make or become greater. INCREASE used intransitively implies progressive growth in size, amount, or intensity.

## 2AC---Pre-Existing

#### W/M – we expand security cooperation

#### CI: Increase means to increase the objective of security cooperation, not an already existing program – Madrid Summit proves

James Coker, 22 (7/4/22; reporter for Infosecurity Magazine, MA in Journalism; “NATO to Develop Rapid Cyber Response Capabilities”; Infosecurity Magazine <https://www.infosecurity-magazine.com/news/nato-rapid-cyber-response/>) //LVL

NATO has announced plans to develop virtual rapid response capabilities “to respond to significant malicious cyber activities.” The plans were unveiled in a declaration published following the NATO Summit in Madrid, Spain, last week. The latest summit took on extra significance in light of the Russian invasion of Ukraine earlier this year, amid fears of the conflict spilling beyond the current borders into NATO territory. Referring to the war, the declaration read: “We, the Heads of State and Government of the North Atlantic Alliance, have gathered in Madrid as war has returned to the European continent. We face a critical time for our security and international peace and stability.” Among other areas, the declaration outlined an agreement between member countries “on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability.” The military alliance acknowledged that “we are confronted by cyber, space and hybrid and other asymmetric threats, and by the malicious use of emerging and disruptive technologies.”

# Substantially Increase

## 1NC---50%

**Interpretation**: **Substantially increase means greater than 50%**

**Brown 94** (Mark R., Professor of Law – Stetson University College of Law, “The Demise of Constitutional Prospectivity: New Life for Owen?”, Iowa Law Review, January, 79 Iowa L. Rev. 273, Lexis)

n241 I am assuming here that "foreseeable" means "probable," as in "more probable than not." This appears to be a safe assumption given the proliferance of cases granting immunity to officials who offend the Constitution. If this definition is correct, deterrence only works and liability should only attach if one's conduct, viewed ex ante, is more likely illegal than legal: the risk of illegality must be more than fifty percent. In other words, one cannot face deterrence, and liability will not attach, if the risk of illegality is less than fifty percent. (When viewed in this fashion, one might perceive a risk of illegality but still not be deterrable because the risk is **not substantial, i.e., not greater than fifty percent**.). Lawful conduct, of course, need not be probably lawful. That is what risk is about. Situations might arise where the objective risk is that conduct is unlawful, but ex post it is lawful. Lest judicial reasoning be completely askew, a fairly strong correlation exists, however, between action that is ex ante probably lawful and that which is lawful ex post in the courts. If this is not true, then courts are reaching objectively improbable conclusions, and the whole idea of reliance is illusory.

#### Violation [the aff doesn’t increase security cooperation by more than 50% is a small subset of security cooperation].

#### Vote neg for limits and ground, they allow thousands of miniscule subsets that no-link all neg generics.

## 2NC---50%

**Less than 50% is insubstantial**

**Brown 94** (Mark R., Professor of Law – Stetson University College of Law, “The Demise of Constitutional Prospectivity: New Life for Owen?”, Iowa Law Review, January, 79 Iowa L. Rev. 273, Lexis)

n241 I am assuming here that "foreseeable" means "probable," as in "more probable than not." This appears to be a safe assumption given the proliferance of cases granting immunity to officials who offend the Constitution. If this definition is correct, deterrence only works and liability should only attach if one's conduct, viewed ex ante, is more likely illegal than legal: the risk of illegality must be more than fifty percent. In other words, one cannot face deterrence, and liability will not attach, if the risk of illegality is less than fifty percent. (When viewed in this fashion, one might perceive a risk of illegality but still not be deterrable because the risk is **not substantial, i.e., not greater than fifty percent**.). Lawful conduct, of course, need not be probably lawful. That is what risk is about. Situations might arise where the objective risk is that conduct is unlawful, but ex post it is lawful. Lest judicial reasoning be completely askew, a fairly strong correlation exists, however, between action that is ex ante probably lawful and that which is lawful ex post in the courts. If this is not true, then courts are reaching objectively improbable conclusions, and the whole idea of reliance is illusory.

**Legal experts agree**

**Davignon v. Clemmey 1** (Davignon v. Clemmey, 176 F. Supp. 2d 77, Lexis)

The court begins the lodestar calculation by looking at the contemporaneous billing records for each person who worked on the plaintiff's case. The absence of detailed contemporaneous time records, except in extraordinary circumstances, will call for a substantial reduction in any award or, in egregious cases, disallowance. **What is a "substantial reduction"? Fifty percent is a favorite among judges.**

## 1NC/2NC---General

### Subs = Needs a Baseline

#### “Substantial” must be measured relative to baseline numbers to the overall category

**Small Business Administration, 10** (“A Guide for Government Agencies How to Comply with the Regulatory Flexibility Act,” June, http://www.sba.gov/sites/default/files/rfaguide.pdf

Legislative history of “substantial number.” To affect a substantial number, a proposed regulation must certainly have an impact on at least one small entity. At the other end of the range, legislative history would not require agencies “to find that an overwhelming percentage [more than half] of small [entities] would be affected” before requiring an IRFA. 63 Legislative history also says that the term “substantial” is intended to mean a substantial number of entities within a particular economic or other activity. 64 The intent of the RFA, therefore, was not to require that agencies find that a large number of the entire universe of small entities would be affected by a rule. Quantification of “substantial” may be industry- or rule-specific. However, it is very important that agencies use the broadest category, “more than just a few,” when initially reviewing a regulation before making the decision to certify or do an initial regulatory flexibility analysis. The goal at this stage of the process is to ensure that the broadest possible impacts are fully considered. The interpretation of the term “substantial number” is not likely to be five small firms in an industry with more than 1,000 small firms. On the other hand, it is important to recognize that five small firms in an industry with only 20 small firms would be a substantial number. Depending on the rule, the substantiality of the number of small businesses affected should be determined on an industry-specific basis and/or on the number of small businesses overall. For example, the Internal Revenue Service, when changing the tax deposit rules, would examine the entire universe of small businesses to see how many would be affected. On the other hand, a change by the Food and Drug Administration in the regulation of meat irradiators might affect only 15 firms, but that would be the entire industry.

### Subs = 33-40% Increase f/baseline

**“Substantial” means 40% --- strict quantification avoids vagueness**

**Schwartz 4** (Arthur, Lawyer – Schwartz + Goldberg, 2002 U.S. Briefs 1609, Lexis)

In the opinion below, the Tenth Circuit suggested that a percentage figure would be **a way to avoid vagueness issues**. (Pet. App., at 13-14) Indeed, one of the Amici supporting the City in this case, the American Planning Association, produced a publication that actually makes a recommendation of a percentage figure that should be adopted by municipalities in establishing zoning  [\*37]  regulations for adult businesses. n8 The APA's well researched report recommended that the terms "**substantial" and "significant" be quantified at 40 percent** for floor space or inventory of a business in the definition of adult business. n9 (Resp. Br. App., at 15-16)

**“Substantial” means 33 percent**

**Maples 7** (Larry, “Pitfalls in Preserving Net Operating Losses”, The CPA Journal, 3-1, Lexis)

If a new loss corporation has substantial nonbusiness assets, the value of the old loss corporation must be reduced by the amount of the nonbusiness assets less liabilities attributable to those assets. "Substantial" is defined as one-third of total assets. This is a difficult provision to interpret. IRC section 382(1)(4) provides that a value reduction in the old loss corporation is required if, just after an ownership change, the new loss corporation has substantial nonbusiness assets. This language seems odd because the purpose of IRC section 382 is to prevent loss trafficking, so it would seem that the asset test ought to apply to the old loss corporation.

### Subs = Across the Board

#### “Substantially means across the board

Brian Anderson 5, Becky Collins, Barbara Van Haren & Nissan Bar-Lev, WCASS Research / Special Projects Committee\* Report on: A Conceptual Framework for Developing a 504 School District Policy, <http://www.specialed.us/issues-504policy/504.htm>

A substantial limitation is a significant restriction as to the condition, manner, or duration under which an individual can perform a particular major life activity as compared to the condition, manner, or duration under which the average person in the general population can perform that same major life activity.¶ The 504 regulation does not define substantial limitation, and the regulation gives discretion to schools to decide what substantial limitation is. The key here is to be consistent internally and to be consistent with pertinent court decisions.¶ The issue “Does it substantially limit the major life activity?” was clarified by the US Supreme Court decision on January 8th, 2002 , “Toyota v. Williams”. In this labor related case, the Supreme Court noted that to meet the “substantially limit” definition, the disability must occur across the board in multiple environments, not only in one environment or one setting. The implications for school related 504 eligibility decisions are clear: The disability in question must be manifested in all facets of the student’s life, not only in school.

## 1NC/2NC---Topic Specific

### Subs = Military

#### “Substantial” means affecting support for all military services and branches

NATO 22 [North Atlantic Treaty Organization; 2/2022; “The Substantial NATO-Georgia Package”; https://www.nato.int/nato\_static\_fl2014/assets/pdf/2022/2/pdf/Air-Maritime-Domains-georgia.pdf]

The Substantial NATO-Georgia Package (SNGP) aims to strengthen Georgia’s ability to defend itself and advance its preparations for NATO membership. The package is composed of 16 defence and related security capacity building initiatives. It involves support for all military services and branches, advice and liaison at all levels (strategic, operational, tactical), capacity-building and training activities, and multinational exercises. As of early 2022, all NATO members and two partner countries have provided support to the implementation of the package in the form of expertise and resources.

#### “Substantial” means affecting defense trade, military capabilities, and cooperation

Nylen et al. 22 [Alexendria Nylen; Civil-Military Program Coordinator at Brown University CHRHS; Archibald Henry; Policy Coordinator at InterAction; Fiona Campbell; Student Researcher at Brown University CHRHS; Lauren Woods; Director at Security Assistance Monitor; Sarah Haviland; former Protection of Civilians Intern at InterAction; 5/2022; The Case of Nigeria and the Nigerian Armed Forces (NAF); https://watson.brown.edu/chrhs/files/chrhs/imce/partnerships/Civ-Mil/Nigeria-May-2022-Factsheet.pdf]

The U.S. security partnership with Nigeria is substantial, with more than $232 million in security assistance, $593 million in foreign military sales, and $305 million in direct commercial sales over the last 20 years.3 This partnership is part of a larger U.S. military presence throughout Africa in response to rising attacks by militant groups that have made West Africa and other parts of the continent key focus areas of U.S. counterterrorism goals. Nigeria is part of the Multinational Joint Task Force (MNJTF)4, the Global Coalition to Defeat Daesh/ISIS, and the Trans-Sahara Counterterrorism Partnership (TSCTP). According to the U.S. government, joint security efforts with Nigeria are focused on counterterrorism efforts against the armed groups Jammatul Ahlis Sunnah lid Daawa wal Jihad (JAS)—commonly known as “Boko Haram”—and the Islamic State’s West Africa Province (ISWAP), increasing defense trade, promoting cooperation on maritime and border security, and strengthening military professionalization and governance of the security sector.

#### “Substantial” in the context of security cooperation means affecting political interaction, diplomatic support, capacity building, and military cooperation

Grønning 18 [Bjørn Elias Mikalsen; Researcher and Professor at the Norwegian Institute for Defence Studies (Norwegian Defence University College) and Norwegian University of Science and Technology (NTNU); 2018; The Pacific Review; “Japan's security cooperation with the Philippines and Vietnam”; https://www.tandfonline.com/doi/full/10.1080/09512748.2017.1397730]

Replacing the National Defense Program Guideline (NDPG) as the capstone document of its security policy, Japan issued its first National Security Strategy (NSS) in December 2013. ‘In order to overcome national security challenges and achieve national security objectives,’ the document notes, ‘Japan needs to expand and deepen cooperative relationships with other countries […]’ (National Security Council of Japan, 2013, p. 14). This statement codifies a recent trend in Tokyo’s foreign policy, namely a push to diversify its bilateral security ties, long the exclusive purview of the Japan–US alliance. Japan’s increasingly comprehensive and substantial security cooperation with the Philippines and Vietnam are two notable examples. These are the topic of this article, which seeks answers to questions such as these: What are the characteristics of Japan’s maturing security relationships with the Philippines and Vietnam? What factors have driven and enabled their recent emergence, and what promotes and constrains their further development? What, finally, do they suggest about Japan’s future direction as a security actor in the region and beyond?

The article argues that Japan’s security cooperation with the Philippines and Vietnam has their six basic characteristics in common: the ‘Strategic Partnership’ diplomatic superstructure, regularization of strategic dialogues, increasing frequency of high-level political interaction, diplomatic support in territorial disputes with China, aid-based maritime capacity building, and increasingly substantial military cooperation. The article moreover argues that Japan’s substantiation of these non-US security bilaterals is fundamentally driven by the contemporary power shift in East Asia and the strategic challenge with which China’s emerging maritime power and behavior presents Japan. It has been pursued under American auspices and further invited by Japanese nationalism and security legislative reforms. Notwithstanding these incentives to further substantiate the two security bilaterals, Japan faces considerable domestic and geo-strategic constraints and counterincentives. For this reason, the article concludes that we are to expect further substantiation, but limited military significance, from the Japan’s ‘Strategic Partnerships’ with the Philippines and Vietnam.

### Subs = Readiness and Sustainability

#### “Substantially increase” means to affect readiness and sustainability

Kramer & Pavel 6/13 [Franklin D. Kramer; Distinguished Fellow, Board Director, and Former Assistant Secretary of Defense for International Security Affairs at the Scowcroft Center for Strategy and Security; Barry Pavel; Senior Vice President and Director at the Scowcroft Center for Strategy and Security; 6/13/2022; “NATO priorities: Initial lessons from the Russia-Ukraine war”; Atlantic Council; https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-priorities-initial-lessons-from-the-russia-ukraine-war/]

As that analysis makes clear, just meeting NATO’s 2-percent defense-spending goal will not be sufficient to resolve the substantial readiness and sustainment deficiencies in any reasonable timeframe. To be sure, the 2-percent goal is important, but NATO needs to establish an additional readiness/sustainment initiative over a shorter period—perhaps three or four years—that would substantially increase the readiness of national forces.

The large increases in Germany’s investment budget provide a model for a budgetary approach that should be undertaken by other countries. Germany has promised to reach 2 percent annually, including by spending one hundred billion euros over a four-year period on investment.5 Other countries should follow the German approach and establish special investment-funding streams focused on readiness and sustainability that would be designed to resolve the shortfalls in a three-to-four-year period. Along with the funding increases, and as an additional part of a NATO readiness/sustainment effort, the Supreme Allied Commander for Europe (SACEUR) should be given the task (and authority) to review and report on the readiness of the forces that will be called upon in the event of a contingency. A focused effort on readiness and sustainability, generated through the defense-planning process and overseen by the SACEUR, will significantly enhance NATO’s deterrent and defense posture

### Subs = Flight funding (for Space Affs)

#### Substantial coop increase is measured by flight funding

NRC ’14 (National Research Council Of The National Academies, Committee on Human Spaceflight; Aeronautics and Space Engineering Board; Space Studies Board; Division on Engineering and Physical Sciences; Committee on National Statistics; Division of Behavioral and Social Sciences and Education; “PATHWAYS TO EXPLORATION: RATIONALES AND APPROACHES FOR A U.S. PROGRAM OF HUMAN SPACE EXPLORATION”, <https://www.nap.edu/read/18801/chapter/1>, 2014)

NASA can sustain a human space exploration program with meaningful milestones that simultaneously reasserts U.S. leadership in space and allows ample opportunity for substantial international collaboration when that program Has elements that are built in a logical sequence. Can fund a frequency of flights sufficiently high to ensure retention of critical technical capability, proficiency of operators, and effective use of infrastructure.

## 2AC/1AR Aff---Topic Specific

### Subs = Significant

#### A “substantial increase” means significant in amount, extent, or degree in the context of security

Law Insider ND [“Substantial increase definition”; https://www.lawinsider.com/dictionary/substantial-increase]

Substantial increase means “important or significant in a large amount, extent, or degree,” and not resulting in insignificant or small benefit to the public health and safety, common defense and security, or the environment, regardless of costs. However, this standard is not intended to be interpreted in a way that would result in disapproval of worthwhile safety or security improvements with justifiable costs

## 2AC/1AR Aff---General

### Subs = Elastic

#### Substantial can be elastic – the numerical percentage is a soft target only

**Words and Phrases, 2** (40A W&P-486)

Utah 1950. The words “all or substantially all” in unemployment compensation law provision concerning experience rating of employer acquiring “all or substantially all” the assets of another employer will be accorded their everyday usage, and some degree of elasticity will be accorded to the word “substantial”.

### Subs = In the main

#### “Substantially” is in the main---ensures stable lit base.

Words and Phrases 2 (Words and Phrases Permanent Edition, “Substantially,” Volume 40B, p. 324-330 October 2002, Thomson West)

Okla. 1911. “Substantially” means in substance: in the main; essentially; by including the material or essential part.

### Subs = Of considerable size/effect

#### Substantial means of considerable size and effect

**Corby, 20 -** Assistant Information Commissioner for the Office of the Information Commissioner in Queensland, Australia (“Decision and Reasons for Decision” R76 and Gold Coast Hospital and Health Service [2020] QICmr 29 (26 May 2020), <https://www.oic.qld.gov.au/__data/assets/pdf_file/0006/42765/decision-314770-external-review-26-05-2020.pdf> //DH

40 ‘Substantial’ is defined as meaning ‘considerable amount, quantity, size, etc.: a substantial sum of money’ (Macquarie

Dictionary, Fifth Edition) and ‘of telling effect: a substantial reform’ (Collins Dictionary, 3rd Australian Edition).

**"Substantial" means of real worth or considerable value --- this is the USUAL and CUSTOMARY meaning of the term**

**Words and Phrases 2** (Volume 40A, p. 458)

D.S.C. 1966. The word “substantial” within Civil Rights Act providing that a place is a public accommodation if a “substantial” portion of food which is served has moved in commerce must be construed in light of its **usual and customary meaning**, that is, something of real worth and importance; of considerable value; valuable, something worthwhile as distinguished from something without value or merely nominal

**“Substantial” means considerable or to a large degree --- this common meaning is preferable because the word is not a term of art**

**Arkush 2** (David, JD Candidate – Harvard University, “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”, Harvard Civil Rights-Civil Liberties Law Review, Winter,   
37 Harv. C.R.-C.L. L. Rev. 131)

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. [99](http://www.lexis.com/research/retrieve?_m=1421887dc00d6c0b78bddb20857a69fa&docnum=16&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAz&_md5=3f3ffe65eadff46b38ea49c40cb1037e&focBudTerms=definition%20of%20the%20term%21%20substantial%21%20or%20definition%20of%20the%20word%20substantial%21&focBudSel=all#n99) It is commonly accepted that words that are not legal terms of art should be accorded their ordinary, not their legal, meaning, [100](http://www.lexis.com/research/retrieve?_m=1421887dc00d6c0b78bddb20857a69fa&docnum=16&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAz&_md5=3f3ffe65eadff46b38ea49c40cb1037e&focBudTerms=definition%20of%20the%20term%21%20substantial%21%20or%20definition%20of%20the%20word%20substantial%21&focBudSel=all#n100) 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: "Substantially" 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": "relating to or proceeding from the essence of a thing; essential"; "of ample or considerable amount, quantity or dimensions"). [101](http://www.lexis.com/research/retrieve?_m=1421887dc00d6c0b78bddb20857a69fa&docnum=16&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAz&_md5=3f3ffe65eadff46b38ea49c40cb1037e&focBudTerms=definition%20of%20the%20term%21%20substantial%21%20or%20definition%20of%20the%20word%20substantial%21&focBudSel=all#n101)

**"Substantial" means considerable in amount or value**

**Words and Phrases 2** (Volume 40A) p. 453

N.D.Ala. 1957. The word “substantial” means considerable in amount, value, or the like, large, as a substantial gain

**“Substantial” means having worth or value**

**Ballentine's 95** (Legal Dictionary and Thesaurus, p. 644)

having worth or value

# Its

## 1NC---Its

#### ‘Its protection’ means the protection must be possessed *and overseen* by the federal government

William B. Bardwell 18, Counsel for the Appellants, Araujo v. Bryant, in the Supreme Court of Mississippi, 12/19/18, “REPLY BRIEF OF THE APPELLANTS,” <https://www.splcenter.org/sites/default/files/documents/2018.12.19_araujo_v_bryant_-_reply_brief_of_the_appellants_filed.pdf> /jpb

The word “its” is not a complicated word. “Its” is a possessive pronoun, demonstrating that something belongs to the noun being modified. See Its, MerriamWebster, https://www.merriam-webster.com/dictionary/its (last viewed Nov. 12, 2018) (“of or relating to it or itself especially as possessor, agent, or object of an agent”) (emphasis added). But the Charter Schools Act could not be clearer: charter schools do not belong to the district in which they are geographically located. Miss. Code Ann. § 37- 28-45(3) (“Although a charter school is geographically located within the boundaries of a particular school district and enrolls students who reside within the school district, the charter school may not be considered a school within that district . . . .”). When Section 206 empowers a school district to levy an ad valorem tax and then requires that revenue to be used “to maintain its schools,” it obviously means the schools overseen by (belonging to) the tax-levying entity. Any other interpretation of “its” has no support in case law, history, or dictionaries.

#### Violation---the affirmative [fiats international actors]

#### It’s a voter for limits and ground–extra-topical consultation erases links to perception-based offense AND competition for counterplans–allows consultation of any international institution–decks competition for CPs like DoS, QPQ, EU, UN since they can’t generate offense and no links every perception-based DA like DoD and BBB

## 1NC/2NC---General

### Its = Possessive

#### ‘Its’ means the security cooperation must be possessed *and overseen* by the federal government

William B. Bardwell 18, Counsel for the Appellants, Araujo v. Bryant, in the Supreme Court of Mississippi, 12/19/18, “REPLY BRIEF OF THE APPELLANTS,” <https://www.splcenter.org/sites/default/files/documents/2018.12.19_araujo_v_bryant_-_reply_brief_of_the_appellants_filed.pdf> /jpb

The word “its” is not a complicated word. “Its” is a possessive pronoun, demonstrating that something belongs to the noun being modified. See Its, MerriamWebster, https://www.merriam-webster.com/dictionary/its (last viewed Nov. 12, 2018) (“of or relating to it or itself especially as possessor, agent, or object of an agent”) (emphasis added). But the Charter Schools Act could not be clearer: charter schools do not belong to the district in which they are geographically located. Miss. Code Ann. § 37- 28-45(3) (“Although a charter school is geographically located within the boundaries of a particular school district and enrolls students who reside within the school district, the charter school may not be considered a school within that district . . . .”). When Section 206 empowers a school district to levy an ad valorem tax and then requires that revenue to be used “to maintain its schools,” it obviously means the schools overseen by (belonging to) the tax-levying entity. Any other interpretation of “its” has no support in case law, history, or dictionaries.

#### “Its” refers to the United States Federal Government and is possessive

Updegrave 91 (W.C., “Explanation of ZIP Code Address Purpose”, 8-19, <http://www.supremelaw.org/ref/zipcode/updegrav.htm>)

More specifically, looking at the map on page 11 of the National ZIP Code Directory, e.g. at a local post office, one will see that the first digit of a ZIP Code defines an area that includes more than one State. The first sentence of the explanatory paragraph begins: "A ZIP Code is a numerical code that identifies areas within the United States and its territories for purposes of ..." [cf. 26 CFR 1.1-1(c)]. Note the singular possessive pronoun "its", not "their", therefore carrying the implication that it relates to the "United States" as a corporation domiciled in the District of Columbia (in the singular sense), not in the sense of being the 50 States of the Union (in the plural sense). The map shows all the States of the Union, but it also shows D.C., Puerto Rico and the Virgin Islands, making the explanatory statement literally correct.

### Its = Exclusive

#### “Its” is exclusive---the security cooperation must come from the U.S.

Updegrave ’91 [W.C.; August 19; Supreme Law.org, “Explanation of ZIP Code Address Purpose,” <http://www.supremelaw.org/ref/zipcode/updegrav.htm>]

More specifically, looking at the map on page 11 of the National ZIP Code Directory, e.g. at a local post office, one will see that the first digit of a ZIP Code defines an area that includes more than one State. The first sentence of the explanatory paragraph begins: "A ZIP Code is a numerical code that identifies areas within the United States and its territories for purposes of ..." [cf. 26 CFR 1.1-1(c)]. Note the singular possessive pronoun "its", not "their", therefore carrying the implication that it relates to the "United States" as a corporation domiciled in the District of Columbia (in the singular sense), not in the sense of being the 50 States of the Union (in the plural sense). The map shows all the States of the Union, but it also shows D.C., Puerto Rico and the Virgin Islands, making the explanatory statement literally correct.

## 2AC/1AR---General

### Its = Associated with

#### Counterinterp: its means associated with.

**OED, ND** (“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

# Security Cooperation

## 1NC---Security Cooperation---Title 10

#### Security cooperation must be under Title 10 and security assistance must be under Title 22

Congressional Research Service ’16 [08/23/16; "DOD Security Cooperation: An Overview of Authorities and Issues," CRS, https://www.everycrsreport.com/reports/R44602.html#\_Toc459893458 //smarx, AZG]

Unlike State Department security assistance authorities that are broad and usually subject to a wide range of general conditions elsewhere in law, Title 10 security cooperation authorities are usually targeted, specifying the types of support or assistance that may be provided and the conditions associated with these types of assistance. One condition on security cooperation authorities (with certain exceptions) is the DOD Leahy Law (10 U.S.C. 2249e) prohibition on assistance to units of foreign security forces credibly believed to have committed gross violations of human rights. 23 Conforming to the Title 22 U.S.C. law vesting the Secretary of State with responsibility to exercise "continuous supervision and general direction" of military assistance, including military education and training, many security cooperation statutes require Secretary of State "concurrence" (i.e., approval) or other State Department input.24

#### Violation – The AFF is under Title 22

#### Voting issue for

#### 1 – Limits – Multiple different legal codes explode the topic

#### 2 – Ground – ‘Security cooperation’ is the stasis for NEG ground

## 2NC---OV

#### Topical AFF’s must be security cooperation under Title 22 – they operate under Title 22

#### They justify AFF’s without a stable agent that diplomatically partner with other countries or AFF’s that use some random miniscule agency

#### We justify AFF’s like AI Logistics and Cognitive Biotechnology, that’s best for

#### 1 – Limits – With a topic that lacks a good core neg generic, exploding AFF ground to include diplomacy and unlimited agencies would be a limits disaster

#### 2 – Ground – They skirt links to the few generics we have left like DOD Tradeoff and DOS CP, only our interp ensures stable ground for both sides

### 2NC – Security Cooperation – Title 10

#### DOD Security cooperation must be under Title 10 – DOS security assistance is under Title 22

Congressional Research Service ’21 [05/17/21; “Defense Primer: DOD ‘Title 10’ Security Cooperation,” CRS, <https://sgp.fas.org/crs/natsec/IF11677.pdf> //smarx, AZG]

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.

#### Title 10 is appropriated with the DOD and Title 22 is appropriated with the DOS – they are distinct approaches

Kelly ’10 [Terrance K.; Jefferson P. Marquis; Cathryn Quantic Thurston; Jennifer D.P. Moroney; Charlotte Lynch; 2010; Kelly, M.S.S. in strategic studies from U.S. Army War College, M.S. in computer and systems engineering from Rensselaer Polytechnic Institute; B.S. from the U.S. Military Academy, Ph.D. in mathematics from the Rensselaer Polytechnic Institute; “Security Cooperation Organizations in the Country Team,” RAND, <https://www.rand.org/content/dam/rand/pubs/technical_reports/2010/RAND_TR734.sum.pdf> //smarx, AZG]

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 byprogram 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 gen- eral separation between the two, resulting in distinct organizations and cultures and leading to stovepiped approaches to working with foreign countries.

### AT: Precision

#### 1 – Debatability outweighs on a topic without a single DA – Ukraine and Stratcon should logically thump everything

#### 2 – We are precise – our evidence is from a Congressional report and compares the authority of Title 10 and Title 22

#### 3 - Their [x] evidence isn’t precise because [explain]

## 2AC

### AT: Title 10

#### The DOD CAN do ‘security cooperation’ and ‘security assistance’ under Title 10 and Title 22

Congressional Research Service ’16 [08/23/16; "DOD Security Cooperation: An Overview of Authorities and Issues," CRS, <https://www.everycrsreport.com/reports/R44602.html#_Toc459893458> //smarx, AZG]

Over the past decade, the increasing scope, pace, and cost of Department of Defense (DOD) security cooperation missions have raised many questions about appropriate DOD and State Department roles and responsibilities in and the utility of such efforts. For some policymakers, DOD's new and expanded missions enable the United States to meet the challenges of the complex global security environment more effectively. As such, congressional approval of new DOD security cooperation statutes represents a necessary response to perceived shortcomings of the overarching legal regime through which, for more than 50 years, Congress has largely authorized and funded the State Department to lead and DOD to administer security assistance to foreign countries. Other policymakers, however, question whether DOD's growing emphasis on and authority to conduct security cooperation missions undermines the State Department's lead role in assisting foreign security forces and "militarizes" U.S. foreign policy.

Since the terrorist attacks of September 11, 2001, Congress has given DOD increasing authority to conduct a wide array of security cooperation programs under Title 10 of the U.S. Code, which governs the organization and operations of DOD and U.S. military forces, as well as through the annual National Defense Authorization Acts. DOD may conduct activities such as training, equipping, and otherwise supporting foreign military forces to fight terrorist groups or to enable them to participate in coalition or other operations. DOD may also conduct humanitarian assistance, military and government educational programs, and other initiatives to assist foreign militaries, as well as their governments and populations. Such activities are intended to encourage better relations between DOD personnel and representatives from foreign militaries, governments, and populations.

This report provides a general overview of current DOD Title 10 authorities to assist foreign governments, militaries, security forces, and populations funded by the DOD budget. It presents background information on the evolving DOD security cooperation mission and the recent development of the statutory framework through which DOD conducts security cooperation activities. It provides summary overviews of nine categories of security cooperation assistance and activities, including the amounts of congressionally authorized funding, where available, and any legislatively required State Department input.1 It discusses recent issues related to the development, implementation, sustainment, and coordination of security cooperation to support continuing congressional oversight. Two tables in the appendix provide information on current Title 10 security cooperation authorities. The first catalogs current security cooperation authorities, noting legislative mandates for State Department input and notification and reporting requirements. The second provides a snapshot of authorized and/or appropriated funding levels for select security cooperation authorities.2

Congress has several avenues of influence in the design, implementation, and oversight of U.S. security cooperation activities. Congress determines which activities and operations will be conducted, and it provides input on the selection of recipient countries, organizations, and groups. It defines the division of labor between DOD, the State Department, and other agencies, including specifying the modes of interagency collaboration. It determines the levels of assistance and appropriates funds. In addition, Congress sets conditions on how the funds may be used and, through its committees, oversees security cooperation activities by instituting reporting and assessment requirements.

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.

Background

The DOD role in U.S. assistance to train, equip, and otherwise support foreign military (and at times other security) forces has evolved over recent decades. Since military aid became a major component of U.S. foreign assistance to counter the rise of the Soviet Union after World War II, the State Department has historically exercised the lead in security assistance activities.5 Since 1961, Congress generally authorized military and other security assistance under Title 22 of the U.S. Code, funded it through the State Department budget, and charged the Secretary of State with responsibility to provide "continuous supervision and general direction" to ensure its coherence with foreign policy.6 With certain exceptions, security assistance was largely a secondary DOD mission.

Beginning in the 1980s, Congress began to expand gradually the scope and character of the statutory framework by authorizing DOD to directly train, equip, and otherwise assist foreign military and other security forces through new provisions in annual NDAAs, some codified to Title 10 of the U.S. Code. Following the September 11th attacks, U.S. government periodic planning documents indicated that the changing security environment presented a new set of challenges.7 Instead of combating nation-states, the U.S. military would increasingly face networks of non-state actors in areas where the United States was not necessarily conducting combat operations. To achieve success in these areas, successive Administrations judged that countering decentralized networks of violent extremists would require long, complex operations involving the U.S. military, other government agencies, and international partners.8 Accordingly, many in DOD and elsewhere maintained that the U.S. military needed to adopt an indirect approach that increased partner capacity (better known by the term "building partner capacity," or BPC) for a variety of purposes, to include: the more effective prosecution of counterterrorism operations, increasing the capacity of states to manage their own regional security challenges in order to prevent an eventual U.S. or international crisis intervention, and as an exit strategy for post-9/11 military campaigns.9 To implement such concepts, DOD requested that Congress grant new authorities to build the capabilities of partner nations and enhance interoperability with U.S. forces, some of which Congress granted.

#### Title 22 funds ‘security assistance’ OR ‘security cooperation’ – this is irrelevant

Mcraven ’11 [William H; 06/28/2011; United States Special Operations Command; “Military Nominations; Committee: Senate Armed Services,” CQ Congressional Testimony, <https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=8b727580-effd-4ca8-ad30-c0758f43bbf4&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A7W4W-KG20-YBWB-C000-00000-00&pdcontentcomponentid=138357&pdteaserkey=sr5&pditab=allpods&ecomp=rz2yk&earg=sr5&prid=eedc1c9a-753c-4b44-becb-b48f8c1b5f91> //smarx, AZG]

Training of foreign forces, as a general rule, must be conducted as a part of the Department of State Title 22 funded Security Assistance or Security Cooperation programs.

#### Security assistance is a subset of security cooperation

Kathleen J. McInnis & Nathan J. Lucas 15, Analyst in International Security & Section Research Manager, “What Is ‘Building Partner Capacity?’ Issues for Congress”, 12/18/2015, Congressional Research Service, <https://sgp.fas.org/crs/natsec/R44313.pdf> /lg

Security assistance, by contrast, is defined as a group of programs authorized by Title 22 of the U.S. Code, as amended, or other related statutes by which the United States provides defense articles, military training, and other defense-related services by grant, loan, credit, cash sales, or lease, in furtherance of national policies and objectives.17

Security assistance is a subset of security cooperation,18 and BPC, in its current formulation, appears to be associated with those security cooperation and assistance activities designed to enable weakened or fragile states to manage their own security challenges. Although all DOD aspects of security assistance programs are administered by DSCA, the agency is not responsible for the department's broader strategy and non-programmatic elements of security cooperation or building partner capacity.19

#### Security cooperation encompasses security assistance --- not the other way around

Nina M. Serafino 16, Specialist in International Security Affairs, “Security Assistance and Cooperation: Shared Responsibility of the Departments of State and Defense”, 05/26/2016, Congressional Research Service, <https://sgp.fas.org/crs/natsec/R44444.pdf> /lg

DOD uses an overarching term, “Security Cooperation,” to denote the State Department security assistance administered by DSCA as well as all other DOD “interactions with foreign defense establishments to build defense relationships.” This term addresses the lack of common terminology for DOD’s many noncombat activities and contacts, including not only the provision of defense articles and services, but also humanitarian assistance, exercises, and military-tomilitary contacts that benefit both U.S. and foreign forces. These “interactions” include programs to provide defense articles and services to foreign governments for which Congress provides DOD with specific authority, as well as programs and military exercises conducted under DOD’s organic Title 10 authority

Despite the formal DOD definition, personnel and entities within DOD use the term “security assistance” to include Title 10 assistance and activities. For instance, the name of the unit responsible for implementing Navy assistance and activities across the security cooperation spectrum is Naval Education and Training Security Assistance Field Activity (NETSAFA).

Some congressional documents do the same. For instance, Section 1211 of the FY2015 National Defense Authorization Act (NDAA, P.L. 113-291) requiring a biennial report on 19 Title 10 authorities or programs to train, equip, otherwise assist or reimburse foreign security forces refers to those authorities as security assistance.

#### Security Cooperation includes Security Assistance

Thomas K. Livingston 11, Air Force Fellow, “Building the Capacity of Partner States Through Security Force Assistance”, 05/05/2011, Congressional Research Service, https://sgp.fas.org/crs/natsec/R41817.pdf /lg

Security Cooperation (SC)

Activities undertaken by the Department of Defense to encourage and enable international partners to work with the United States to achieve strategic objectives. Includes all DOD interactions with foreign defense and security establishments, including all DOD-administered security assistance programs, that: Build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities. Develop allied and friendly military capabilities for self-defense and multinational operations. Provide Service members with peacetime and contingency access to host nations.

## 1NC---Defensive Only

#### Security Cooperation is only for defensive measures

CRS, 16 (8/23/16; “DOD Security Cooperation: An Overview of Authorities and Issues”; Every CRS Report <https://www.everycrsreport.com/reports/R44602.html#_Toc459893458>) //LVL

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.

#### Violation – the aff ( ) – that’s not defensive security cooperation

#### Voter for

#### Limits – allows the aff to justify any military action and move away from the DOD’s interpretation of security cooperation measures

#### Ground -- skirts core neg generic offense that is based on current security cooperation defense

## 2NC---Defensive

### AT: Funding=Offensive SC

#### Funding for security cooperation comes from defense operation funds

CRS, 16 ((8/23/16; “DOD Security Cooperation: An Overview of Authorities and Issues” Every CRS Report <https://www.everycrsreport.com/reports/R44602.html#_Toc459893458>) //LVL

Not all Title 10 and NDAA authorities have funding levels specified by authorization and/or appropriations legislation. Funding for some security cooperation authorities may be subsumed under a larger budget category or simply drawn from the defense-wide operations and maintenance budget, making identification of funding levels for difficult.

### AT: W/M

#### US Code defines military exchanges as between defensive organizations

Major Anthony V. Lenze, 17 (Judge Advocate, United States Army, The Judge Advocate General's Legal Center and School, United States Army, Charlottesville, Virginia; J.D., 2007; “ARTICLE: TRADITIONAL COMBATANT COMMANDER ACTIVITIES: ACKNOWLEDGING AND ANALYZING COMBATANT COMMANDERS' AUTHORITY TO INTERACT WITH FOREIGN MILITARIES”, Military Law Review, 225, 641. <https://advance-lexis-com.proxy.lib.umich.edu/api/document?collection=analytical-materials&id=urn:contentItem:5V3X-FKV0-01DR-M0RJ-00000-00&context=1516831>.) //LVL

10 U.S.C. § 168 defines military-to-military contacts as "contacts between members of the armed forces and members of foreign armed forces" through the following activities: (1) traveling contact teams, including any transportation expense, translation services expense, or administrative expense that is related to such activities; (2) The activities of military liaison teams; (3) Exchanges of civilian or military personnel between the Department of Defense and defense ministries of foreign governments; (4) Exchanges of military personnel between units of the armed forces and units of foreign armed forces; (5) Seminars and conferences held primarily in a theater of operations; (6) Distribution of publications primarily in a theater of operations; (7) Personnel expenses for Department of Defense civilian and military personnel to the extent that those expenses relate to participation in an activity described in paragraph (3), (4), (5), or (6); (8) Reimbursement of military personnel appropriations accounts for the pay and allowances paid to reserve component personnel for service while engaged in any activity referred to in another paragraph of this subsection."

### AT: Joint Operations

#### Joint operations are not a part of DOD security cooperation under the DSCA – operations can only respond to threats

USA Gov (“Defense Security Cooperation Agency; USA gov <https://www.usa.gov/federal-agencies/defense-security-cooperation-agency#:~:text=The%20Defense%20Security%20Cooperation%20Agency,to%20respond%20to%20shared%20challenges>; Accessed 7/11/22) //LVL

The Defense Security Cooperation Agency supports U.S. national security and foreign policy interests. They train, educate, advise, and equip foreign security forces to respond to shared challenges.

### AT: Cyber Example

#### US Code gives security programs the authority to conduct defensive cyber operations

Legal Information Institute (“10 U.S. Code § 333 - Foreign security forces: authority to build capacity” Cornell Law School Legal Information Institute <https://www.law.cornell.edu/uscode/text/10/333>; Accessed 7/11/22) //LVL

(a)Authority.—The Secretary of Defense is authorized to conduct or support a program or programs to provide training and equipment to the national security forces of one or more foreign countries for the purpose of building the capacity of such forces to conduct one or more of the following:

(1)Counterterrorism operations.

(2)Counter-weapons of mass destruction operations.

(3)Counter-illicit drug trafficking operations.

(4)Counter-transnational organized crime operations.

(5)Maritime and border security operations.

(6)Military intelligence operations.

(7)Air domain awareness operations.

(8)Operations or activities that contribute to an existing international coalition operation that is determined by the Secretary to be in the national interest of the United States.

(9)Cyberspace security and defensive cyberspace operations.

## 2AC---AT: Defensive Only

#### W/M – Defense Security Cooperation Agency announced security cooperation includes both offensive and defensive capabilities

Richard Bumgardner, 21 (9/3/21; Chief, Public Affairs Officer at USACE Transatlantic; “USASAC: Providing Strength in Cooperation” US Army <https://www.army.mil/article/249995/usasac_providing_strength_in_cooperation>) //LVL

In the past three years, William Slade, USASAC’s country program manager for the Baltics states, and members of the Army Security Assistance Enterprise have processed and implemented more than $1 billion in FMS cases to help assure the Baltic states could deter aggressive action by neighboring militaries. In major FMS announcements released by the Defense Security Cooperation Agency, this includes offensive and defensive capabilities to include Joint Light Tactical Vehicles (JLTV), UH-60M Black Hawk helicopters, Javelin missiles, and many other operational and tactical equipment items. These equipment items would also enable the Baltic states to gain significant interoperability with U.S. and NATO forces.

#### OCOs prove offensive capabilities are used as a part of NATO’s collective defense strategies – cyber policy proves

Erica D. Lonergan and Mark Montgomery, 22 (1/25/22; PhD in Political Science from Columbia, Assistant Professor in the Army Cyber Institute; Master’s degree in Modern History from Oxford University, Senior director and Fellow at the Foundation Defense of Democracies; “PRESSING QUESTIONS: OFFENSIVE CYBER OPERATIONS AND NATO STRATEGY” Modern War Institute <https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/>) //LVL

But the seeds were also planted in 2016 for NATO to consider a potential role for offensive cyber operations. That year, the alliance recognized cyberspace as a domain of military operations, comparable to land, sea, and air. At the 2018 Brussels summit, NATO began to more seriously consider offensive cyber operations. Specifically, NATO created the Cyberspace Operations Centre to coordinate requests for member states to provide offensive cyber effects through the Sovereign Cyber Effects Provided Voluntarily by Allies process. Following the 2018 summit, then-Secretary of Defense James Mattis stated in a press conference that five states—the United States, the United Kingdom, Denmark, the Netherlands, and Estonia—were contributing cyber forces to “help NATO fight in this important domain.” More recently, in June 2021, NATO convened in Brussels and committed to a Comprehensive Cyber Defence Policy. A key feature of the new policy is the prominent role of offensive cyber operations. In Brussels, member states committed to “employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats.” NATO’s shift to incorporating offensive cyber operations into existing strategy and policy has focused on integrating offensive effects into conventional military plans and operations in the context of a conflict. While NATO’s updated strategy is a positive development, its limited focus on conflict scenarios for employing cyber power fails to accurately account for the cyber threat environment NATO faces—particularly the mismatch between the alliance’s clear distinction between wartime and peacetime and the approach of adversaries like Russia, who adopt a competition-conflict continuum. Additionally, the focus on employing offensive cyber during a high-end conventional fight is also not consistent with how several NATO members are already engaged in gray zone offensive cyber operations.

#### CI: Security cooperation includes activities with the intent of promoting US interests and allied partnerships

CJCS, 17 (5/23/17; “Security Cooperation”; Joint Chief of Staff <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf>) //LVL

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.

#### Prefer our interp:

#### Most precise – we follow the DOD’s interpretation of security cooperation and it doesn’t exclude offensive capabilities

#### Reasonability – they have to prove we result in a limits explosion that has a ground differential they can’t prepare for

## 1AR---Defensive Only

#### Specifically joint operations include offensive and defensive missions

CJCS, 17 (5/23/17; “Security Cooperation”; Joint Chief of Staff <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf>) //LVL

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. Stability activities typically occur during all phases of an operation/campaign in balance with offensive and defensive operations. Normally, civil-military operations (CMO) and civil affairs operations are essential to stabilization efforts, especially for larger and more complex operations.

#### Warsaw Summit proves – defense and deterrence include offensive operations

Tomas Minarik (JUDr in Penal law from Charles University Prague; Head of International Organisations and Law unit; “NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit”; NATO Cooperative Cyber Defence Centre of Exellence <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/> ) //LVL

Second, the use of the word ‘deterrence’ in connection with cyberspace is significant, because it is another step towards the acceptance of offensive cyber capabilities as part of collective defence. However, linking deterrence to cyber defence is difficult. The line of argument is simple: how can you achieve deterrence when your adversaries are not afraid of you, because they do not know what offensive capabilities you have and when and how you would use them? Others view the term more broadly, and they are willing to admit that there exists something like ‘deterrence by denial’. The extension of deterrence to the cyber realm should be considered by NATO, but it relies primarily on the will of nations. Third, the idea of moving towards recognition of offensive cyber capabilities is supported by the statement that cyber defence will be integrated into operational planning and NATO’s operations and missions. As NCIA is already responsible for protecting NATO networks in an operational setting, this statement makes little sense if it only refers to passive capabilities. Nevertheless, no official commitment was made in this regard, as the Alliance continues to avoid public statements about offensive cyber capabilities.

### 1NC---SC---Arms + Exercises

#### Interpretation---security cooperation is arms transfers and military exercises.

Stephen Watts et al. 22, senior political scientist at the RAND Corporation focused on strategic competition and deterrence, force posture, security sector assistance, irregular warfare and stabilization, and long-term conflict trends, xx/xx/2022, Deterrence and Escalation in Competition with Russia, https://www.rand.org/pubs/research\_reports/RRA720-1.html \\SYang

Activities: We capture U.S. security cooperation activities using two measures: arms transfers and multilateral military exercises. As with the measure of “competitive arms transfers,” our measure of arms imports from the United States comes from SIPRI data. The use of this measure is intended to capture not only the materiel transfer but the training and related activities that usually accompany U.S. arms transfers. These data run from 1950 to 2010 in our sample. Our data on multilateral military exercises come from a data set compiled by the political scientist Vito D’Orazio from an examination of major news sources between 1970 and 2010.12 Although the SIPRI data provide a measure of the scale of U.S. assistance, the data on military exercises only indicate whether an exercise took place and where; they do not include details on the scale or purpose

#### Violation---[contextualize]

#### That’s a voter---

#### A---Limits---allowing other methods blows the lid off of topical affirmatives as any aff even remotely related to the military becomes topical (news flash---that’s a lot of things) ---that’s uniquely bad on a bidirectional topic with three topic areas.

#### B---Ground---any other interpretation allows the 2AC to spike out of arms-transfer based offense like the appeasement and deterrence DA and counterplans that PIC out---this topic has no neg generics which means our ground offense outweighs.

#### C---Topic Education---any other interpretation causes a race to the bottom to find the most irrelevant solvency advocates that mention the military which obfuscates learning about exercises and arms transfers which was the intention of the topic paper.

## 1NC---SC---Limiting Power

#### Security cooperation requires limiting a country’s freedoms and military power, especially in the context of NATO

Harald Müller 13, head of the Peace Studies Foundation of Hesse and Professor of International Relations at the University of Frankfurt who was the disarmament advisor to the former UN Secretary General Kofi Annan, “Chapter 24: Security Cooperation”, 01/10/2013, Handbook of International Relations, <https://dx.doi.org/10.4135/9781446247587.n24> /lg

Security cooperation implies relying on other states for national survival, which is hard to reconcile with exclusive reliance on self-help. In addition, security cooperation limits the freedom to act and constrains one's ability to maximize military power. Arms control aims at reducing offensive, destabilizing options, and enhanced transparency may reduce the chances of achieving surprise. In wartime alliances, mutual dependency is high. As a state's existence is at stake in war, relying on someone else is an existential issue; strategic choices have to be closely coordinated, and freedom of action might be lost. Peacetime alliances can be more relaxed and may be little more than token promises that might be broken in the moment of truth. But they may as well entail intimate structural cooperation or integration. The degree of mutual knowledge, transparency, and dependence within NATO is inexplicable, seen from the perspective of potential future hostilities. NATO member states put much more on the line than participants in average arms control or nonproliferation agreements: Alliance cooperation presents a puzzle as well.

#### Violation: the affirmative increases the military power of the USFG

#### Prefer our interpretation:

#### Limits – allowing affs that can either increase or decrease military constraints causes an explosion of affs

#### Education – the failure to provide a stasis point for research stalls the development of core neg generics

## 1NC---SC---Excludes NATO Exercises

#### Security cooperation is distinct from a NATO exercise --- incorrect terminology leads to decreased national security

Nathan L. Fenell 11, thesis for Master of Arts in International Studies, “Security Cooperation Poorly Defined”, 12/12/2011, The University of San Francisco, https://repository.usfca.edu/cgi/viewcontent.cgi?article=1020&context=thes

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.

#### **Violation: The aff is a NATO exercise**

#### Prefer our interpretation:

#### Limits – condensing the resolution down to a specific area is necessary to match this topic’s severe lack of neg positions

#### Real world education – the casual use of “security cooperation” as a “NATO exercise” leads to unintended negative consequences

## 1NC---SC---Fighting Crimes

#### Security cooperation means fighting crimes and exchanging expertise on narcotics, human trafficking, unlawful trade trade, and arms

UAE Government News 13, “UAE, Algeria ink agreement defining security cooperation”, 03/12/2013 /lg

Abu Dhabi: The UAE on Monday inked an agreement with North African country Algeria to define security cooperation on fighting all kinds of crimes as well as exchanging expertise and information on narcotics, human trafficking and unlawful trade, specifically in arms and ammunition, state media WAM reported.

Deputy prime minister and interior minister of the UAE Sheikh Saif bin Zayed Al Nahyan and minister for interior and local governments of Algeria Dahou Ould Kablia signed the agreement in capital city Abu Dhabi.

In addition to covering cooperation in fighting all kinds of crimes, including trade in illegal arms and human and drugs trafficking, the agreement establishes the legal framework and mechanisms of coordination between the UAE and Algeria in their mutual efforts to combat all kinds of crime and exchange expertise and information associated with security issues.

Furthermore, the agreement also calls for formulating a joint committee to follow up on the security partnership's progress.

#### Violation: the aff does not fight crime in any of the listed areas

#### Prefer our interpretation:

#### Limits – broad definitions make the negative research burden impossible because of the lack of topic disads

#### Ground – pinning down an interp to four specific areas provides the aff and neg with core stasis points

## 2NC---SC---Extensions

### 2NC---SC – DoD

#### Despite evolution, definitions of “security cooperation” maintain the necessity for DoD activities in all legal contexts

Captain Harry Parent et al 19, Captain Reed Lorch, Major Deidre Baker, Lieutenant Colonel Timothy Litka, Colonel Luisa Santiago, Colonel Anthony Adolph, & Colonel William Smoot, “Fostering Enduring Partnerships: An Overview of Security Cooperation Offices Through the Lens of Iraq”, 2019, Army Lawyer, Issue 2, p. 48-63 /lg

Security Cooperation

While this term was the product of the 1997 Defense Reform Initiative, and entered the DoD lexicon with the renaming of DSAA to DSCA in October 1998,14 security cooperation remained ill-defined until 9 June 2004, when it was first formally defined within Joint Publication 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.

That broad definition has continued to take shape, with 10 U.S.C. Ch. 16 § 301 currently defining security cooperation programs and activities of the DoD as meaning 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: 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 U.S. security interests. 6

Department of Defense Directive 5132.03, reissued on 29 December 2016, includes a definition of SC in conformity with the underlying U.S. Code provision, and, like the current definition for SA, specifies that SA is included within SC:

Security Cooperation. 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 also includes DoD-administered security assistance programs.

This definition received an additional minor modification in the 23 May 2017, Joint Publication 3-20, Security Cooperation, replacing the word "defense" relationships with "security" relationships.

#### Security cooperation must be administered by the DoD --- DSCA definition

Kathleen J. McInnis & Nathan J. Lucas 15, Analyst in International Security & Section Research Manager, “What Is ‘Building Partner Capacity?’ Issues for Congress”, 12/18/2015, Congressional Research Service, <https://sgp.fas.org/crs/natsec/R44313.pdf> /lg

According to DSCA, security cooperation refers to those activities undertaken by the Department of Defense to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DOD interactions with foreign defense and security establishments, including 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.15 Security cooperation is a core aspect of DOD's key planning processes, to include the Guidance for the Employment of the Force and Guidance for the Development of the Force.16

#### Security Cooperation necessitates DoD activity

Thomas K. Livingston 11, Air Force Fellow, “Building the Capacity of Partner States Through Security Force Assistance”, 05/05/2011, Congressional Research Service, https://sgp.fas.org/crs/natsec/R41817.pdf /lg

Security Cooperation (SC)

Activities undertaken by the Department of Defense to encourage and enable international partners to work with the United States to achieve strategic objectives. Includes all DOD interactions with foreign defense and security establishments, including all DOD-administered security assistance programs, that: Build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities. Develop allied and friendly military capabilities for self-defense and multinational operations. Provide Service members with peacetime and contingency access to host nations.

#### Security cooperation consists of DoD activities including training and exercises, foreign military sales and financing, officer exchange programs, educational opportunities, technical exchanges, and security force assistance.

Thomas K. Livingston 11, Air Force Fellow, “Building the Capacity of Partner States Through Security Force Assistance”, 05/05/2011, Congressional Research Service, https://sgp.fas.org/crs/natsec/R41817.pdf /lg

Build the Security Capacity of Partner States: Since the United States assumed the role of a leading security provider after the end of World War II, DOD has worked actively to build the defense capacity of allied and partner states. Doing so has also given the U.S. Armed Forces opportunities to train with and learn from their counterparts. These efforts further the U.S. objective of securing a peaceful and cooperative international order. Security cooperation activities include bilateral and multilateral training and exercises, foreign military sales (FMS) and financing (FMF), officer exchange programs, educational opportunities at professional military schools, technical exchanges, and efforts to assist foreign security forces in building competency and capacity. In today's complex and interdependent security environment, these dimensions of the U.S. defense strategy have never been more important. U.S. forces, therefore, will continue to treat the building of partners' security capacity as an increasingly important mission. Within the range of security cooperation activities, the most dynamic in the coming years will be security force assistance (SFA) missions: "hands on" efforts, conducted primarily in host countries, to train, equip, advise, and assist those countries' forces in becoming more proficient at providing security to their populations and protecting their resources and territories. In order to ensure that improvements in partner security forces are sustained, the Department must seek to enhance the capabilities and capacity of security institutions, such as defense ministries, that support fielded forces....246 [emphasis added]

### 2NC---SC – Excludes Hostilities

#### Security cooperation is a means to prevent armed conflicts, not to resolve them --- Afghanistan proves

Nathan L. Fenell 11, thesis for Master of Arts in International Studies, “Security Cooperation Poorly Defined”, 12/12/2011, The University of San Francisco, https://repository.usfca.edu/cgi/viewcontent.cgi?article=1020&context=thes

Currently a foreign policy that points to the doctrinal use of SC as the means of achieving U.S. foreign policy goals does not exist. A U.S. foreign policy that draws from defensive liberalism is an ideal way to shape the proper employment of a SC strategy. The National Security Strategy (NSS) is the first place where security cooperation emerges as a means to achieve security goals and the placement of SC in the NSS is appropriate; however, without a clear understanding of the definition of security cooperation, the DOD and DOS are improperly executing SC activities. The most visible SC strategy, executed improperly, is the PRT in Afghanistan.131 The use of SC as a means to achieve post reconstruction goals improperly aligns means and ends. SC is designed as a means to prevent armed conflict not as a means to resolve the conflict at the conclusion of hostilities.

### 2NC---SC – Excludes States (for DoS CP)

#### Security cooperation activities are purely federal

Lawrence Kapp & Nina M. Serafino 11, Specialist in Military Manpower Policy & Specialist in International Security Affairs, “The National Guard State Partnership Program: Background, Issues, and Options for Congress”, 08/15/2011, Congressional Research Service, <https://sgp.fas.org/crs/misc/R41957.pdf> /lg

A final area in which the SPP differs from active component security cooperation activities lies in the role of individual states in the relationship. Active component security cooperation activities are purely federal in nature; there is no connection with any U.S. state. SPP activities have both a federal and a state connection, and this latter relationship can be important from several perspectives. For the state and the foreign nation, the SPP provides a link between senior state and foreign nation officials. The adjutant general (the head of a state National Guard) is typically a senior official in his or her state government, normally heading up the state department of military affairs, and sometimes leading the state department of emergency management or homeland security.16 This can provide a conduit for the state and the foreign nation to develop relationships beyond that with the state National Guard—for example, enhancing economic ties or conducting educational exchanges. From the federal perspective, a strong relationship between a state and a foreign nation could potentially contribute to a stronger relationship between the United States and the foreign nation.17 On the other hand, conflicts of interest could conceivably develop between the state and the United States in their relationships with the partner nation.18

## 2AC---SC---DOD

### SC---AT: Excludes Civilians

#### Security Cooperation includes the use of armed forces and civilian employees of the DoD

Army LT. General Charles Hooper 18, Director of Defense Security Cooperation Agency, “THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES HOLDS A DISCUSSION ON STRENGTHENING ALLIANCES AND PARTNERSHIPS THROUGH DEFENSE COOPERATION”, 03/16/2018, Political Transcript Wire /lg

Last year DSCA created a workforce development directorate to focus on these efforts and among the accomplishments, what we're -- what we're trying to do is determine the scope of the Security Cooperation Workforce, something we have never done before, create a DOD wide defense competency assessment tool and develop revised education and training curriculum and a competency-based certification program.

And all of this is relatively new. The first thing we did was identify DOD personnel performing duties related to security cooperation and believe it or not, we had never done that before. So, we initially considered the Security Cooperation Workforce to be around 10,000 people.

The majority of which are Title 22 funded. However, since the expanded F.Y. '17 NDAA definition of Security Cooperation Workforce includes I am quoting here, "other members of the Armed Forces and civilian employees of the DOD who contribute significantly to the Security Cooperation programs and activities".

When we took that into account the number of Security Cooperation workers increased to over 18,000 people worldwide. Now this sounds like a lot but when you consider that it includes the implementing agencies, the Army, Navy, Air Force agencies that work for us, our Security Cooperation's personnel worldwide and the various other personnel in other departments that are focused on security cooperation, it does not seem like as much after all.

Moving forward workforce analysis will be a recurring function to ensure the DOD provides training and experience-based opportunities necessary to develop and maintain Security Cooperation's related competencies in the work -- competencies in the workforce.

This will ensure that the department has a Security Cooperation Workforce that can -- that is approved certified and has the capacity in both personnel and skills to properly performance its missions, provides appropriate support to the assessment, planning, monitoring, execution and evaluation of Security Cooperation.

### SC---Congressional Oversight (For Oversight DA)

#### Security cooperation necessitates Congressional oversight

Bolko J. Skorupski & Nina M. Serafino 16, research assistance & specialist in international security affairs, “DOD Security Cooperation: An Overview of Authorities and Issues”, 08/23/2016, Congressional Research Service, <https://sgp.fas.org/crs/natsec/R44602.pdf> /lg

Congress has several avenues of influence in the design, implementation, and oversight of U.S. security cooperation activities. Congress determines which activities and operations will be conducted, and it provides input on the selection of recipient countries, organizations, and groups. It defines the division of labor between DOD, the State Department, and other agencies, including specifying the modes of interagency collaboration. It determines the levels of assistance and appropriates funds. In addition, Congress sets conditions on how the funds may be used and, through its committees, oversees security cooperation activities by instituting reporting and assessment requirements.

## 1AR---SC---Extensions

### SC---AT: Only DoD

#### Security cooperation can include DSCA-administered State Department action

Nina M. Serafino 16, Specialist in International Security Affairs, “Security Assistance and Cooperation: Shared Responsibility of the Departments of State and Defense”, 05/26/2016, Congressional Research Service, <https://sgp.fas.org/crs/natsec/R44444.pdf> /lg

DOD uses an overarching term, “Security Cooperation,” to denote the State Department security assistance administered by DSCA as well as all other DOD “interactions with foreign defense establishments to build defense relationships.” This term addresses the lack of common terminology for DOD’s many noncombat activities and contacts, including not only the provision of defense articles and services, but also humanitarian assistance, exercises, and military-tomilitary contacts that benefit both U.S. and foreign forces. These “interactions” include programs to provide defense articles and services to foreign governments for which Congress provides DOD with specific authority, as well as programs and military exercises conducted under DOD’s organic Title 10 authority

#### Security cooperation is shared between the DoD and DoS

Major Nicholas R. Simontis 13, chief of strategy at Third Army/U.S. Army Central with an MA in security studies from Kansas State University and an MMAS in theater operations from the School for Advanced Military Studies, “SECURITY COOPERATION: AN OLD PRACTICE FOR NEW TIMES”, 29/03/2013, School of Advanced Military Studies, <https://apps.dtic.mil/sti/pdfs/ADA589722.pdf> /lg

While security cooperation is a shared effort between DOD and DOS, DOD has, by a significant margin, the preponderance of personnel and organizational structure that comprise the security cooperation infrastructure. DOD defines security cooperation as “all DOD interactions with foreign defense and security establishments to build defense relationships that promote specific US security interests, develop allied and friendly military and security capabilities for internal and external defense and multinational operations, and provide U.S. forces with peacetime and contingency access to the HN [host nation].”14 It is important to note that the DOD definition includes developmental and humanitarian assistance activities focused on enhancing foreign governments’ abilities to care for their people. The goal of all these activities is to reduce or eliminate factors leading to a crisis or conflict that requires U.S. intervention.15 Security assistance activities are a subset of security cooperation and deal principally with foreign military financing (FMF), foreign military sales (FMS), and international military education and training (IMET) activities. The Deputy Undersecretary of Defense for Policy has overall responsibility for the execution of DOD’s security cooperation activities, which DSCA administers.

#### Security cooperation includes DoD-administered security assistance under DoS authority

Ronald H. Reynolds 19, DPA, “The Management of Security Cooperation”, 2019, Defense Institute of Security Cooperation Studies, <https://permanent.fdlp.gov/gpo61490/2019_01_39thEd/39thEd.pdf> /lg

While all of the programs previously mentioned are authorized under 22 U.S.C, or Title 22, and are under the general control of the Department of State (DoS), the Department of Defense (DoD) administers many of them. Since Title 10 U.S. Code Section 301 defines security cooperation programs and activities of DoD as any program or interaction of DoD with the security establishment of a foreign country to build capabilities, to provide access or to build relationships, many of the previously described FAA and AECA-authorized security assistance programs administered by DoD in accordance with the SAMM fall under the broad definition of security cooperation. The following is a categorization of programs, and a brief explanation, based upon a partial list presented in the 2016 DoD Guidance for Security Cooperation. For more detail on the different programs that can be found under each category access and download the ‘Security Cooperation Programs’ book found on the DISCS website or use the SC Programs Viewer on the Security Assistance Network Web (SANweb):

## Neg---Interp---SC---State of Being

#### Security cooperation refers to actions aimed at ensuring security as a state of being.

Rita Floyd 19, Senior Lecturer in Conflict and Security at the Department of Political Science and International Studies at the University of Birmingham (UK). Her work on securitisation theory, environmental security and IR theory has appeared in a number of peer-reviewed journals including most recently in the Review of International Studies. Her monograph The Morality of Security: A Theory of Just Securitization was published by Cambridge University Press in 2019, 2-4-2019, "Security cooperation as a primary institution of western international society", https://www-tandfonline-com.proxy.lib.umich.edu/doi/full/10.1080/14781158.2021.1876015 \\SYang

In order to understand what is meant by security cooperation it is necessary to break down this concept into its components. Security tends to have one of two meanings. On the one hand, it refers to the condition of feeling and being secure,13 which is achieved when states and individuals enjoy freedom from fear (i.e. negative peace) and want (comprehensive human security). On the other hand security refers to a particular form of politics, to wit the high politics of security that may involve an extraordinary policy response, or at least the credible threat thereof. Importantly, security politics may or may not lead to greater overall security as, in Jonathan Herington's14 terms, ‘a state of being’, but – for the most part – security action is motivated by the idea to achieve or increase security as a state of being in international society. Depending on the type and nature of the threat, this may or may not involve the use of military force.15 In security cooperation, security thus refers to defensive actions aimed at ensuring security as a state of being.

## Aff---General

### 2AC – Security Cooperation

#### CI – Security cooperation includes defense relationships, enhancing military capabilities, internal and external security efforts, interoperability, and great power competition with Russia and China

Congressional Research Service ’21 [05/17/21; “Defense Primer: DOD ‘Title 10’ Security Cooperation,” CRS, <https://sgp.fas.org/crs/natsec/IF11677.pdf> //smarx, AZG]

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.

# NATO

### 1NC---NATO---Civilian and Military

#### Interpretation---NATO is both a civilian and military institution---topical affirmatives must interact with both aspects.

David Nauta 17, 11-10-2017, "The International Responsibility of NATO and its Personnel during Military Operations", https://brill.com/view/book/9789004354647/B9789004354647\_004.xml, Brill, Chapter 4, accessed 7-8-2022 \\SYang

NATO consists of two main types of institutional structures: a civilian structure and a military structure. The civilian structure is responsible for policy- and decision-making which provides for the functioning of the Organization both internally and externally. The military structure is involved in the planning and execution of military operations. All NATO operations are decided upon by the civilian structure and carried out by military structure. It means that both parts of NATO participate in the initiation, planning and execution of NATO operations.

#### Violation---the affirmative only uses the [civilian/military] structures of NATO.

#### That’s a voter---

#### A---Limits---allowing affirmatives to pick one or the other blows the lid off of limits by tripling the number of total affirmatives---that’s uniquely bad in an aff biased topic with three resolutional areas that’s also bidirectional.

#### B---Ground---allowing aff teams to spike out of core neg offense by picking one or the other decimates neg ground in a world with no generic DAs.

#### C---Topic Education---understanding NATO’s functioning requires comprehensive knowledge of both the civilian and military aspects---the only way to access that is in-depth debates over affirmatives that use both.

### 1NC---NATO---Member States

#### Interpretation---NATO means the 30 member states.

Dictionary.com 22, Dictionary.com is an online dictionary whose domain was first registered on May 14, 1995, accessed July 4, 2022, “NATO”, https://www.dictionary.com/browse/NATO \\SYang

North Atlantic Treaty Organization: a political and military alliance of countries in Europe and North America established in Washington, D.C. (1949) for the purpose of collective defense against aggression, comprising Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Portugal, the United Kingdom, the United States, Greece, Turkey, Germany, Spain, the Czech Republic, Hungary, Poland, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, Slovenia, Albania, Croatia, Montenegro, and North Macedonia.

#### Violation---the affirmative cooperates with states outside of the 30 NATO members.

#### That’s a voter---

#### A---Limits---any other interp blows the lid off of topical affirmatives as NATO interacts with practically every country

#### B---Ground---core negative ground is disads to NATO mechanisms, PICs out of NATO, and so on---that’s key in a topic with no neg generics.

#### C---Topic Education---allowing non-NATO member states causes a race to the bottom to collaborate with the most obscure countries and skews debate away from education about NATO members.

#### At best they’re extra-T---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

### 2NC---NATO---Member States

#### The USFG agrees. Plus their interpretation is just obviously absurd and totally arbitrary---NATO means NATO.

US 22, the U.S. Mission to the North Atlantic Treaty Organization is the official representation of the United State of America to the North Atlantic Treaty Organization, accessed July 4, 2022, “About NATO”, https://NATO.usmission.gov/about-NATO/ \\SYang)

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

#### More ev.

Kimberly Amadeo et al. 22, expert on U.S. and world economies and investing, March 6, 2022, “What is NATO?”, https://www.thebalance.com/NATO-purpose-history-members-and-alliances-3306116 \\SYang

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.

#### NATO says it is the group of 30 countries.

The North Atlantic Treaty Organization 22, a military collective defense alliance including 30 European and North American countries that might come up in the 2022-2023 high school policy debate topic, May 10, 2022, “10 things you need to know about NATO”, https://www.NATO.int/cps/en/NATOhq/126169.htm, official NATO website \\SYang

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

#### “Is” means to be the same thing.

Merriam Webster English Dictionary 22, American company that publishes reference books and is especially known for its dictionaries, “be”, https://www.merriam-webster.com/dictionary/be \\SYang \*\*Note: dictionary entry for “be”. “is” is a form of “be”\*\*

to have identity with : to constitute the same idea or object as

#### NATO only contains 30 countries---it’s an alliance---countries that aren’t party to the treaty aren’t part of the alliance.

Jesus Jimenez 22, breaking news reporter for The New York Times, “What Is NATO and Which Countries Are Members?”, https://www.nytimes.com/article/what-is-NATO.html, published in the New York Times Online Edition \\SYang

What is NATO?

The mutual-defense alliance was established in 1949, after World War II, by the United States, Canada and 10 European countries.

The treaty for which the alliance is named has 14 articles, by which all NATO members must abide. The most prominent is Article 5, which declares that an attack against one member state is an attack against them all.

That article placed Western Europe under U.S. protection in the face of a Soviet Union that was cementing its domination over Central and Eastern Europe and appeared then only to be growing in power and ambition.

After the Soviet Union’s collapse in the early 1990s, the alliance took on a wider role. NATO forces — made up of troops volunteered by member states — operated as peacekeepers in Bosnia in the 1990s, and bombed Serbia in 1999 to protect Kosovo, where the alliance still has troops.

Which countries are in NATO?

In addition to the United States and Canada, 10 other countries became part of NATO in 1949: Belgium, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal and Britain.

Europe, facing energy shortages as Russia cuts gas shipments, moves to bail out providers.

A team of Ukrainian medics navigates life and death on the battlefield.

For many who have fled Ukraine’s war-battered east, there is no turning back.

Since then, 18 more European powers have joined: Albania, Bulgaria, Croatia, the Czech Republic, Estonia, Germany, Greece, Hungary, Latvia, Lithuania, Montenegro, North Macedonia, Poland, Turkey, Romania, Slovakia, Slovenia and Spain.

### 2NC---NATO---Ukraine Violation

#### NATO is only those 30 countries---not Ukraine---prefer evidence with intent to exclude.

CNN 22, the Cable News Network is a multinational cable news channel, January 28, 2022, “What is NATO and when does it act?”, https://www.cnn.com/2022/01/27/world/NATO-explainer-intl-cmd/index.html \\SYang

Twelve founding countries -- the United States, Canada, the United Kingdom, France and eight other European nations -- signed the North Atlantic Treaty in 1949, pledging to protect each other by political and military means.

Over the decades since, the alliance has grown to include a total of 30 members.

In alphabetical order, they are: Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxemburg, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, the UK and the US.

Ukraine is not a member of NATO, but has long hoped to join the alliance. This is a sore point for Russia, which sees NATO as a threat and vehemently opposes the move.

### 2NC---NATO---AT: Partner States

#### NATO is an *alliance*---that’s not the same thing as partnerships.

Claudette Roulo 19, writer for the Department of Defense, March 22, 2019, “Alliances vs. Partnerships”, https://www.defense.gov/News/Feature-Stories/story/Article/1684641/alliances-vs-partnerships/, official Department of Defense website \\Syang

Alliance, partnership, partnership, alliance. It seems like those terms are used interchangeably by Defense Department officials in every other speech. However, those officials are choosing their words carefully, because in the world of international relations, alliances and partnerships are two very different things.

Alliances

Alliances are formal agreements between two or more nations. In national defense, they're promises that each nation will support the other, particularly during war.

Some examples of alliances that the U.S. is in include NATO — the North Atlantic Treaty Organization (with 28 other countries), NORAD — the North American Aerospace Defense Command (with Canada), ANZUS — the Australia, New Zealand and U.S. Security Treaty, and the Moroccan-American Treaty of Friendship — which is America's oldest unbroken treaty.

Treaties are the documents that seal the deal on alliances, so sometimes you might hear the term "treaty ally." Things like international boundaries, trade rules, human rights and even postal arrangements can also be set by treaties.

Some treaties make room for alliances to grow. For example, the Atlantic Treaty, which founded NATO, says that membership is open to any "European state in a position to further the principles of this treaty and to contribute to the security of the North Atlantic area."

And in fact, the newly named nation of North Macedonia is well on its way to doing just that. The formal approval protocol is awaiting signatures from the 29 nations in NATO, a process that’s expected to wrap up by the end of this year or early next year.

Partnerships

Partnerships are less formal than alliances. Often called "strategic partnerships," they help build relationships between nations or organizations like militaries. Like alliances, they benefit the members of the partnership, but they can be short-term and don't involve a treaty.

## Affirmative

### 2AC---C/I---NATO = Partner States

#### C/I---NATO empirically does a large majority of cooperation with global partners which are crucial to alliance functioning---their evidence doesn’t have *intent to exclude* and skews debate away from the core of NATO functioning---especially relevant as NATO 2030 is reorienting the organization towards *cooperation with global partners*.

The North Atlantic Treaty Organization 21, a military collective defense alliance including 30 European and North American countries that might come up in the 2022-2023 high school policy debate topic August 25, 2021, “Relations with partners across the globe”, https://www.NATO.int/cps/en/NATOhq/topics\_49188.htm, official NATO website \\SYang

NATO has nine “partners across the globe” or “global partners”, which the Alliance cooperates with on an individual basis. NATO’s global partners include Afghanistan, Australia, Colombia, Iraq, Japan, the Republic of Korea, Mongolia, New Zealand and Pakistan. NATO’s engagement with global partners is taking on increasing importance in a complex security environment, where many of the challenges the Alliance faces are global and no longer bound by geography.

The NATO 2030 agenda agreed by NATO Leaders at the NATO Brussels 2021 Summit seeks to strengthen NATO’s global cooperation with like-minded partners, especially with its global partners, to defend the rules-based international order and institutions, to set international norms and standards in space and in cyberspace, and on new technologies and global arms control.

Since 2016, NATO has increasingly engaged politically with its four Asia-Pacific partners – Australia, Japan, the Republic of Korea and New Zealand – notably through meetings of the North Atlantic Council, including a first meeting at the level of foreign ministers in December 2020, to discuss the shift in the global balance of power and the rise of China.

NATO is also intensifying dialogue and cooperation with Colombia.

Global partners have access to the full range of activities NATO offers to all partners guided by an Individual Partnership Cooperation Programme. They work with NATO on a range of common cross-cutting security challenges such as cyber defence, counter-terrorism, non-proliferation and resilience.

Some partners participate in NATO’s military operations, while many have benefited from NATO’s expertise in areas such as building defence capacity, and defence training and education.

NATO also consults with other non-member countries, which have no bilateral programme of cooperation (for example, China, Brazil, Ghana, India, Singapore) in particular on regional security dynamics.

At the NATO Brussels Summit in June 2021, Allies agreed to strengthen NATO engagement with key global actors and other new interlocutors beyond the Euro-Atlantic area, including those from Africa, Asia and Latin America.

Wider cooperation

In today’s complex security environment, NATO’s relations with partners across the globe offers many advantages to Allies and partners alike. NATO’s practical cooperation with its global partners includes cross-cutting global challenges such as cyber defence, maritime security, humanitarian assistance and disaster relief, non-proliferation, defence science and technology, and Women, Peace and Security. Some partners participate in NATO’s military operations, while many have also benefited from NATO’s expertise in areas such as building defence capacity, and defence training and education.

Political consultation and intelligence-sharing is fundamental to the way NATO works with its global partners, just as it is among the 30 Allies. Political dialogue is a key tool for fostering regional understanding and exchanging expertise between Allies and their global partners. This enriches NATO’s situational awareness in areas beyond its direct neighbourhood, and it ensures that global partners understand NATO’s positions and are able to contribute to policy discussions on common security challenges. This is increasing in importance as many of today’s new security challenges are no longer bound by geography, such as in cyber space, space and climate change. Political dialogue also assists in establishing and developing practical cooperation with these partners.

Political dialogue with NATO’s global partners take place in many different formats, including at NATO Headquarters in Brussels, Belgium. Just as Allied consultations take place in a broad range of committees and at different levels, so too do several global partners participate in these committees on a regular basis, from the level of ministers to technical working groups. For example, NATO’s four Asia-Pacific partners – Australia, Japan, the Republic of Korea and New Zealand – participate on a regular basis in discussions in the Political Committee and in the North Atlantic Council.

At the most senior level, the Secretary General, the Deputy Secretary General, the Chair of the Military Committee and NATO’s Strategic Commanders meet with global partners’ Heads of State and Government, foreign ministers, defence ministers, as well as other high-level officials.

Support for NATO-led operations

The support provided by global partners and other countries to NATO-led operations has made a significant contribution to international peace and security.

In Afghanistan, a number of global partners such as Australia, the Republic of Korea and New Zealand, made important contributions to the NATO-led International Security Assistance Force (ISAF) from 2003 to 2014. Many continued to work alongside Allies in the follow-on Resolute Support Mission to train, advise and assist the Afghan security forces and institutions. Some countries supported stabilisation efforts in Afghanistan without being involved in combat. This includes Japan, which funded a large number of development projects and dispatched liaison officers, and Pakistan that provided ground and air lines of communication to resupply the mission . In 2020, the Republic of Korea served as the co-chair of the Afghan National Army Trust Fund Board.

Evolution of relations

NATO has maintained a dialogue with countries that are not part of its partnership frameworks, on an ad-hoc basis, since the 1990s. However, NATO’s involvement in areas outside of its immediate region – including Afghanistan and Libya – has increased the need and opportunities for enhanced global interaction. Clearly, the emergence of global threats requires the cooperation of a wider range of countries to successfully tackle challenges such as terrorism, proliferation, piracy or cyber attacks. Dialogue with these countries can also help NATO avert crises and, when needed, manage an operation throughout all phases.

Since 1998, NATO has invited countries across the globe to participate in its activities, workshops, exercises and conferences. This decision marked a policy shift for the Alliance, allowing these countries to have access, through the case-by-case approval of the North Atlantic Council, to activities offered under NATO’s structured partnerships. These countries were known as “Contact Countries”.

Significant steps were taken at the 2006 Riga Summit to increase the operational relevance of NATO’s cooperation with countries that are part of its structured partnership frameworks as well as other countries around the world. These steps, reinforced by decisions at the 2008 Bucharest Summit, defined a set of objectives for these relationships and created avenues for enhanced political dialogue, including meetings of the North Atlantic Council with ministers of the countries concerned, high-level talks, and meetings with ambassadors. In addition, annual work programmes (then referred to as Individual Tailored Cooperation Packages of Activities) were further developed.

At the 2010 Lisbon Summit, Allies agreed to develop a more efficient and flexible partnership policy, in time for the meeting of Allied foreign ministers in Berlin in April 2011. To this end, they decided to:

streamline NATO’s partnership tools in order to open all cooperative activities and exercises to partners and to harmonise partnership programmes;

better engage with partners across the globe who contribute significantly to security and reach out to relevant partners to build trust, increase transparency and develop practical cooperation;

develop flexible formats to discuss security challenges with partners and enhance existing fora for political dialogue; and

build on improvements in NATO’s training mechanisms and consider methods to enhance individual partners’ ability to build capacity.

Following the 2010 Lisbon Summit and NATO’s subsequent revision of its partnership policy in April 2011, the global context has changed significantly. As NATO became increasingly confronted with new defence and security challenges such as cyber attacks, disinformation, disruptive technologies and the erosion of arms control regimes, NATO recognised the importance of adapting to these new security challenges, including working closer together with NATO’s partners.

This increasing engagement with NATO’s like-minded partners, regardless of geographic location, on the basis of the shared values of democratic freedoms, rule of law and human rights, allows Allies to discuss relevant developments in the regions with partners, and increase their situational awareness and understanding of strategic issues on relevant global developments.

In June 2020, NATO Secretary General Jens Stoltenberg launched his outline for NATO 2030. In order for NATO to keep its Allies safe in a more uncertain world, the Secretary General stated that NATO must “stay strong militarily, be more united politically, and take a broader approach globally.” NATO taking a more global approach means working even more closely with like-minded partners to develop coherent, strong, unified and collective responses to defend our values in a world of increased global competition.

The global pillar of NATO 2030 is particularly relevant to NATO’s engagement with its four Asia-Pacific partners – Australia, Japan, the Republic of Korea and New Zealand. As the challenges confronting the Euro-Atlantic area and the Asia-Pacific region are increasingly converging, it is vital for NATO and its four close partners in the Asia-Pacific region to enhance cooperation and dialogue to support security in both regions, but also to work together to strengthen the international rules-based order. In December 2020, for the first time, the four Asia-Pacific partners participated in a NATO Foreign Ministerial Meeting, where NATO Allies discussed the shift in the global balance of power and the rise of China with the Asia-Pacific partners, as well as with Finland, Sweden and the European Union High Representative/ Vice President of the European Commission.

At the 2021 Brussels Summit, Allies agreed to increase dialogue and practical cooperation between NATO and existing partners, including partners in the Asia-Pacific, and to strengthen NATO engagement with key global actors and other new interlocutors beyond the Euro-Atlantic area, including from Africa, Asia and Latin America.

### 2AC---C/I---Distinct From Member States

#### C/I---NATO is an independent international organization with international legal personality---that means *it’s separate from its member states*---prefer the best comparative ev.

David Nauta 17, 11-10-2017, "The International Responsibility of NATO and its Personnel during Military Operations", https://brill.com/view/book/9789004354647/B9789004354647\_004.xml, Brill, Chapter 5, accessed 7-8-2022 \\SYang

This chapter examined the existence of international legal personality of NATO. Legal personality is relevant to the responsibility of NATO and its personnel during military operations. Without international legal personality, NATO cannot be responsible. Unfortunately, there is little jurisprudence on the concept of international legal personality. In 1949, the ICJ formed an Opinion on the personality of the un, but remained vague on how this was determined. This resulted in various theories on how legal personality is acquired. The two mainstream theories in academic literature are the ‘subjective theory’ and ‘objective theory’, which both give explanations on how international legal personality can be determined to exist, but also have received criticism. The practical approach of Klabbers’ ‘presumptive personality’ reconciles to some degree both theories.88 This theory presumes the existence of international legal personality of an international organization if it performs acts that can only be explained on the basis of international legal personality. This chapter has examined NATO’s legal personality on the basis of the two mainstream theories, but also inclined towards the ‘presumptive theory’ to give a practical answer. Some authors doubt whether the Alliance has legal personality.89 These authors argue that NATO has not acted on the international level. The often-used example in this respect is the compensation by the us (in lieu to NATO) to China for the damages suffered during NATO’s intervention in Kosovo. Other arguments denying the international legal personality of NATO is the fact that NATO takes its decision by consensus, leading to believe that the Alliance does not have any “will” of its own. These doubts would be to some degree valid, if the focus was on the earlier years of the NATO. During the Cold War – and probably during its first non-article 5 operation as well – it may have been difficult to consider that the Alliance has international legal personality. NATO’s static defence operations against the former Soviet Union did not require an autonomous role separate from its member States. The member States were fully capable to independently devise military plans and coordinate these with each other. The establishment of SACEUR in 1952, which integrated military forces, marked the beginning of a transformation, but NATO started to evolve into an organization with legal personality only after the Cold War. Since then, the Alliance has gone through a significant transformation, as described in Chapters 3 and 4. The Organization has concluded international agreements with States and other international organizations. NATO and its personnel enjoy privileges and immunities in its member States, but also in Afghanistan, Iraq, in the States of the former Yugoslavia and in various other mission areas. It should not be ruled out that the Alliance might bring and receive international claims in the future if the exercise of the jurisdiction by the courts would be made possible. It is not required that an international organization show all the indicia of international legal personality. If this were the case, barely any international organization would have such status in international law. NATO is presumed to have international legal personality on the basis of the fact that it has concluded international agreements and that the organization and its personnel enjoy privileges and immunities. This presumption may be rebutted if there is evidence to the contrary. Practice of States and international organizations, as well as the jurisprudence of international courts and tribunals, confirm the presumption that NATO has international legal personality. The military intervention in the former Yugoslavia gave rise to several claims for damages resulting from NATO military operations. Yugoslavia filed complaints against several member States of NATO, while individuals turned their claims for damages to individual member States of NATO instead to NATO itself.90 The respondent States in both cases argued that the claims should have been filed against NATO – on the basis of that it had international legal personality – instead of the individual nations. These early cases are not indicative of either the existence or non-existence of international legal personality, but of the absence of NATO’s locus standi in the courts. Claimants may have chosen to start their proceedings against individual States, so to avoid their claim being regarded non-admissible. International courts and tribunals have confirmed NATO’s legal personality. Both the ICTY and the ICC came to this conclusion in relation to NATO operations in respectively the Balkans and Libya. International organizations, including the UN, have addressed NATO in relation to alleged breaches of international obligations binding upon the organization. The UN International Commission of Inquiry, notably, addressed NATO – and not individual member States – with respect to airstrikes in Libya that may have caused incidental loss of civilian life and damage to civilian infrastructure.91 Finally, States have confirmed NATO’s legal personality in the ILC’s commentary to the Articles on Responsibility of International Organizations, where they stated that “NATO is an international organization within the meaning of draft article 2(a) of the draft articles, and as such a subject of international law. It possesses international legal personality as well as treaty-making power”.92 The scepticism regarding the international legal personality of NATO diminished gradually from the 1990s. Academic writers, States and international organization increasingly argue in favour of the Alliance’ status under international law. Even NATO itself had to become convinced of its own personality. The out-of-area operations required the conclusion of Status of Force Agreements (SOFAs) with third States. NATO aptly took the initiative and concluded SOFAs with Bosnia-Herzegovina, Afghanistan, Libya and other countries, thereby affirming its status in international law. In conclusion, NATO certainly meets several indicia of international legal personality as is evidenced by its performance of actions on the international level, notably treaty-making power and privileges and immunities. The existence of international legal personality is – in a way – also confirmed by the practice of States and other international organizations. Recent academic literature furthermore supports this conclusion.

### 1AR---C/I---Distinct From Member States

#### Consensus goes aff---it’s indisputable that the NATO has ILP---Portugal, France, Ottawa Treaty, and more.

Marten Zwanenburg 5, professor of Law During Military Operations at the Faculty of Law at the University of Amsterdam, April 15, 2005, “Accountability of peace support missions”, https://brill.com/view/title/11419 [\\SYang](file:///\\SYang) \*\*corrected for typos

There is no similar international judicial authority with regard to the international legal personality of NATO. The constitutive instrument of the organization does not expressly provide that it has legal personality in international law. Explicit recognition is not the only way in which international legal personality is conferred on international organizations. Application of the objective as well as application of the subjective theory of international legal personality leads to the conclusion that NATO is an international legal person." The organization is a permanent association of states established by the 1949 North Atlantic Treaty with the lawful object of collective self-defense. It is equipped with organs, the most important of which is the North Atlantic Council. The functions of the organization are distinct from those of the member states. The most recent statement of these functions is in section 10 of the 1999 Strategic Concept of the organization.'? The organization exercises powers on the international plane, notably treaty-making power. Article 25 of the 1951 Ottawa treaty on the status of the organization for example provides that the North Atlantic Council acting on behalf of the organization may conclude supplementary agreements with member states. The organization also concludes international agreements on other issues with member states" and with non-member states." There is also state practice supporting legal personality of the organization. In the Banliouic case before the European Court of Human Rights (ECHR) the French government argued that a bombardment during Operation Allied Force was not imputable to its member states but to NATO as an organization with an international legal personality separate from that of the respondent states. The challenge of the admissibility of the case by all the respondent states on the ground that the ECHR would be determining the rights and obligations of NATO itself also points in this direction. This challenge assumes that NATO itself has rights and obligations under international law, which can only be the case if the organization has international legal personality. Trial Chambers of the International Criminal Tribunal for the former Yugoslavia (ICTY) have also treated NATO as an international legal person separate from its member states. Trial Chamber I in the Todorovic case ordered the NAC to disclose to the defense copies of documents and the identity of certain individuals in connection with the arrest of the accused." The order was based on article 29 of the ICTY Statute which provides that states shall cooperate with the Tribunal. The Trial Chamber stated that: A purposive construction of the Statute yields the conclusion that such an order should be as applicable to collective enterprises of States as it is to individual States; Article 29 should, therefore, be read as conferring on the International Tribunal a power to require an international organization or its competent organ such as SFOR to cooperate with it in the achievement of its fundamental objective of prosecution of persons responsible for serious violations of international humanitarian law, by providing the several modes of assistance set out therein.?" In the Legality of the Use of Force cases before the IC] several of the respondent states explicitly mentioned that NATO is an international legal person during the hearings held in April 2004. Portugal drew attention to NATO's development since its establishment, in particular the institutionalization of the organization." It maintained that "NATO is an international organisation in the strict sense, with its own international legal personality."> France referred to the criteria for international legal personality identified in the Reparations for Injuries case. It submitted that under these criteria NATO possesses international legal personality." The applicant accepted NATO's international legal personality. However, it maintained that this personality is "limited" on the basis of NATO's founding instrument and other NATO documents.:"

#### The NATO’s status as an independent organization is so well established that the EU is considered to have legal personality as a result of agreements with the NATO.

Martin Reichard 4, member of the Austrian Mission to NATO, dealing with Civil Emergency Planning, South East Europe, Trust Funds, and EU-NATO relations, February 2004, “Some Legal Issues Concerning the EU-NATO Berlin Plus Agreement”, https://www.researchgate.net/publication/233708215\_Some\_Legal\_Issues\_Concerning\_the\_EU-NATO\_Berlin\_Plus\_Agreement, Nordic Journal of International Law (73) \\SYang

Concerning the particular subject matter of the Berlin Plus, it is moreover difficult to see how, in the process of building a common security and defence policy, the EU should exercise its functions, given its present lack of technological, logistic and infrastructure resources in the military sphere, without being able to rely on external help, such as from NATO.76 This factual deficiency arguably makes international legal personality for the EU a priori indispensable, at least on a functional basis, and limited to the subject matter of the agreement. Indeed, in the time preceding the conclusion of the Berlin Plus agreement, such military support from NATO to the European Union was expected to be eventually realized through conclusion of a binding international agreement." In conclusion, legal personality in the specific case of the Berlin Plus can therefore be implied from the Union's powers enshrined in the relevant provisions on external representation in Title V of the TEU, mainly Articles 18 and 24. This is a case of the general principle of implied powers. NATO's quality as a subject of international law is today undisputed. 79 Even though it has until recently not endeavoured to conclude treaties on the international level, " it has for a long time had agreements with its member states on its status in their respective internal legal systems.'

#### The NATO functions as an independent entity, specifically an international organization with international legal personality---it has an independent volition, isn’t subject to authority, and---this means *all of their interpretations* that they read in the block are WRONG because the *organization is separate from its member states*---prefer the only comparative evidence that does a comprehensive legal analysis.

David Nauta 17, 11-10-2017, "The International Responsibility of NATO and its Personnel during Military Operations", https://brill.com/view/book/9789004354647/B9789004354647\_004.xml, Brill, Chapter 4, accessed 7-8-2022 \\SYang \*\*text shrunk for readability and figures 2 and 3 omitted

This chapter describes the current institutional framework of NATO and the decision making process for its operations. This will provide further understanding of the powers of NATO and the relationship between NATO and the member States, which is relevant for the question of attribution of conduct of personnel to NATO, troop contributing nations or other international organizations such as the UN. Moreover, the overview provides in insight on whether NATO is an entity separate from its member States, i.e. whether it meets the indicia of an international organization with international legal personality. The conclusions in this chapter will be used further on in Chapters 5 and 7. Paragraph 4.2 gives a brief outline of the various organs of the Alliance, their composition, tasks and their position within the NATO structure. The intention of providing this outline is to facilitate understanding of the political-military structure and how hierarchically NATO is organised. Paragraph 4.3 examines the relationship between NATO and its member States and NATO’s decision-making process. Since the North Atlantic Council (NAC), in which all the member States participate, is the highest political decision-making organ of NATO, it is appropriate to examine both the relationship between NATO and States as well as NATO’s decision-making process. It is important to discuss the decision-making process in the NAC to establish to whom a wrongful act can be attributed: to NATO, to its member States or to both. It can also assist in establishing in which situations – i.e. under which conditions – NATO member States and / or NATO as an international organization will be held responsible. This paragraph will, additionally, examine the relationship between NATO and non-NATO member States, for the same reasons as indicated above and because non-member States regularly participate in NATO-led operations. The outline is followed by an analysis of the relationship between NATO and the UN. The choice to limit the analysis to the relationship between NATO and the UN is made in order to avoid an overly generic or exhaustive study on relationships between NATO and other international organizations or such organizations in general. Moreover, the relationship with the UN is the more straightforward choice to examine as the member States made explicit reference in the Washington Treaty to the context and position NATO takes within the UN system. The context is established by referring to Article 51 of the UN Charter – the right to take collective action against an armed attack – which forms the basis for the establishment of NATO. The Washington Treaty also acknowledges the primary role of the UN Security Council in the maintenance and restoration of international peace and security. Moreover, since NATO relies for its non-article 5 crisis response operations – which consist of the majority of NATO-led operations – on a mandate or authorization from the UN Security Council, the relationship between NATO and the UN is of relevance here. Finally, from a practical point of view, the UN is likely one of the most important partners of NATO. 4.2 Current Institutional Framework of NATO 4.2.1 Introduction NATO consists of two main types of institutional structures: a civilian structure and a military structure. The civilian structure is responsible for policy- and decision-making which provides for the functioning of the Organization both internally and externally. The military structure is involved in the planning and execution of military operations. All NATO operations are decided upon by the civilian structure and carried out by military structure. It means that both parts of NATO participate in the initiation, planning and execution of NATO operations. 4.2.2 The Civilian Structure a The North Atlantic Council The Washington Treaty stands out for its brevity, with a mere 14 articles and does expand a great deal on the structure, tasks and responsibilities of the Alliance. The treaty establishes only one organ, the North Atlantic Council (NAC), and attributes the necessary powers to implement the treaty.1 The NAC is the highest decision-making organ in the Organization. The Council is composed of the representatives of all Member States, which holds regular meetings at the level of Foreign- or Defence Ministers (Ministerials), Heads of States (Summits) or Permanent Representatives. As such, the NAC is the most important organ for the member States to express their views and to take collective decisions on political issues of the Alliance. This feature is of relevance to determine whether NATO has international legal personality. An indication that an international organization has international legal personality is – according to the theory of ‘objective legal personality’ which is further described in Chapter 5 – that an organization is not subject to the authority of any other State or organised community. Since the NAC is not subject to the authority of another legal entity other than the participating States, the assumption is that NATO has international legal personality.2 The Washington Treaty does not prescribe the way the Council should take its decisions, but the NAC adopted consensus as the standard. This translates to decisions being adopted without a formal voting procedure, provided that no member raises any formal objection.3 The decision-making process of NATO is described more elaborately when this book examines the relationship between the member States and NATO in paragraph 4.3. It is relevant to note here that decision-making through consensus is both seen as an argument in favour and against the existence of international legal personality of the Alliance. Arguments against such personality put emphasis on the fact that NAC decisions are collective decisions made by its member States, which assumes that the NAC expresses the will of the member States, rather than the Organization. On the other hand, member States have a right to express objections that they may have and block any decision, making the NAC’s decisions entirely reliant on the common agreement of all member States, rather than that of one State. The introduction of the “silence procedure” and opting-out mechanism enhances the autonomy of the Organization – referred to later in this chapter – and alludes to the possibility that NATO may have a volonté distincte from its member States. A volonté distincte, or ‘separate will’, may indicate under certain legal theories that the Organization has international legal personality. It is held here that the consensus rule on itself is not an indicator of either the existence or non-existence of international legal personality. Rather, a more distinguishing factor is to examine in how far the member States retain control in the decision-making process taken by the NAC. A conclusion on the existence of international legal personality of the Alliance will be given in Chapter 5. The Washington Treaty does not prescribe the span of topics which the NAC can decide upon. The Council’s authority is generally confined to the aim of NATO, which is to “safeguard the freedom, common heritage and civilization of their peoples” and to “promote stability and well-being in the North-Atlantic Area”. In that respect, the Washington Treaty leaves ample room for interpretation and discretion in decision-making.6 The founders have left to the discretion of the Council to “set up such subsidiary bodies as may be necessary.”7 The NAC created a variety of subsidiary bodies, of which the most important here are the Secretary General, the Military Committee and the various organs of the NATO Command Structure. b The Secretary General The Secretary General leads a unified international secretariat to assist the plenary organ – the NAC – and to serve as the Chairman of the Council.8 As such, he is the chief executive of NATO and responsible for promoting and directing the process of consultation and decision-making within the Alliance.9The Secretary General is supported by the International Staff, forming the so-called “civilian structure”. The Secretary General is also the representative for external relations. He maintains relationships on the level of Ministers of Foreign Affairs, - Defense and Heads of State during the operations.10 The Secretary General is usually the signatory for international agreements binding the Alliance, e.g. the exchange of letters with the Afghan authorities relating to the Status of ISAF Personnel in Afghanistan is signed on the side of the Alliance by the Secretary General.11 4.2.3 The Military Structure NATO’s military structure consists of the Military Committee, supported by its International Military Staff, and the NATO Command Structure. a The Military Committee The Military Committee (MC) is composed of the highest national military representatives from each Member State, assisting the Council with military expertise12 and works under the overall political authority of the NAC.13 It assists and advises the NAC on military matters and provides military guidance to the NATO Strategic Commanders of the NATO Command Structure. The MC takes its decisions by consensus; this way full commitment is achieved in both the military as well as the political requirements and objectives of the mission. The MC plays an important role in the drafting of NATO strategic concepts and advises the Council of the military situation in countries were NATO is conducting operations. The role of the Chairman of the MC is to represent and defend the consensus-based advice to the NAC. The Military Committee is supported by the International Military Staff. The Committee is an essential link between the political and military structure of NATO. The Military Committee provides the NAC with military advice agreed by all Chiefs of Defence. The consensus among the highest military authorities of NATO represents a firm commitment that the operation is militarily achievable with the forces available from the nations. b The NATO Command Structure The NATO Command Structure consists of two Strategic Commands, Allied Command Operations and Allied Command Transformation. In 1950, the NAC created the Supreme Allied Commander Europe (SACEUR)14 and gave it the responsibility to “organize [national units assigned to him] into an effective integrated defence force”.15 Currently, SACEUR is responsible for the planning and commanding all NATO-led operations. He is bound by the political constraints given by the NAC, who maintains political oversight of operations. The command structure enables NATO to plan and execute operations while maintaining strategic military and political coherence throughout the chain of command. SACEUR has at his disposition various subordinate commands which makes up Allied Command Operations, or ACO. ACO includes two Joint Force Commands (JFC Brunssum and JFC Naples), each of which is capable to plan, conduct and sustain a major joint operation16 at the operational level. There are also three other specialised commands (Air Command, Land Command and Maritime Command) directly under SACEUR’s command, which provide support to the Joint Force Command, but are also able to plan, conduct and sustain a smaller joint operation by themselves and report directly to SACEUR. Supreme Allied Command Transformation has the lead role for the transformation of NATO’s military structure, forces, capabilities and doctrines in order to improve the military effectiveness of the Alliance. SACT does not have a specific role in commanding operations and will not be further examined in detail as it is not of particular relevance to NATO’s responsibilities during its operations. In NATO-led operations, SACEUR will appoint one of its subordinate headquarters to plan and execute the mission (figure 2). One of the Joint Force Commands, or – in case of a smaller mission, the Maritime-, Land- or Air Command – can establish a headquarters in the mission area that will be responsible for running of day-to-day operations. SACEUR will retain Operational

<<<FIGURES 2 AND 3 OMITTED>>>

Command (i.e. the authority to assign missions or tasks, to deploy units and to reassign forces)17 over the mission, while delegating Operational Control (i.e. the authority to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time, or location) to the subordinate headquarters (figure 3).184.3 The Relationship between NATO and Its Member States and the Decision-making Process There is considerable debate on the status of NATO in international law. Some view NATO as an organization independent from its members, capable of having a will of its own.19 Other studies see NATO as a trans-Atlantic forum where member States meet to discuss global security issues.20 As such, NATO is not capable of acting independently and would be deprived of international legal personality. Consequently, if NATO is not a subject of international law, it can not bear international rights and obligations and does not have responsibility under international law. Those studies which hold the view that NATO is a forum or a mere Alliance of like-minded States rather than an independent international organization, base their arguments primarily on the process in which member States take decisions in the North Atlantic Council (NAC). NATO takes decisions by consensus of all the member States and therefore there is no real autonomy of the organization. The consensus rule by itself is not an indicator of international legal personality, as was discussed above. The measure by which the member States control the organization through this decision-making procedure is a better indicator for establishing whether the organization has international legal personality.21 For this reason, the relationship between NATO and its member States and the degree in which member States control decisions made by NATO is further examined below. This chapter will focus on three areas, the consensus-rule in NATO’s decision making, the planning of operations and the contribution of forces to the Alliance. 4.3.1 Consensus-rule NATO decisions are made by consensus, after discussion and consultation among member countries.22 A decision reached by consensus is an agreement reached by common consent. It is important to differentiate between decision-making based on consensus and unanimity. Unanimity requires an actively stated vote in favour of a measure, which the Alliance does not seek. Actually, there is no voting at all in NATO’s decision-making process. Instead, decisions are taken when there is an absence of objection by any member State. Member States can express their objections either privately with the Secretary General, raise them during NAC meetings, or even go public with their disagreement.23 Of course, each choice comes at a political cost. Hence, the role of the Secretary General is essential to maintain the cohesion of the Alliance. To this end, the Secretary General may employ a tactic called the “silence-procedure”. This procedure allows States to reach consensus on those topics that are politically sensitive for some of the member States. It entails that a decision will be automatically passed by the NAC after a stated time-period set by the Secretary General, unless a member State objects by sending a formal letter to the Secretary General thereby breaking the silence.24 In some cases, the political cost for an opposing member State’s representative of openly being identified as blocking the decision may outweigh the benefit of seeing the proposed action stopped. In those cases, a member State may prefer not to block the decision, but rather mitigate its concerns through caveats for its forces or even to choose not to participate fully in the operation. The silence-procedure has proven useful in situations where domestic opposition exists in the member States for a certain military intervention. In Operation Allied Force, public disagreement would have placed NATO member States in a conflict before world media and would play in favour for President Milosevic. The silence procedure allowed Member States not needing to take a public position and permitted NATO to move forward.25 Similarly, the silence procedure provided Germany – which faced public opposition regarding a military intervention in Libya – in an opportunity to avoid to take publicly a position regarding the decision in favour of NATO’s Operation Unified Protector.26 The silence procedure shows that the Alliance can continue to move forward even with the dissociation of one or more of the member States. The decision making procedure is not – by itself – an argument that NATO lacks autonomy and, hence, international legal personality. As stated above, the autonomy depends on the degree of control that the member States exercise over the organization. The consensus procedure illustrates that there is no requirement for member States to exercise such control and thereby allowing the Organization to enjoy a certain degree of autonomy. Member States are also free to choose which operations they prefer to participate in. In case a member State has concerns regarding a specific mission, it may decide not to participate in the mission with military forces and materiel, while at the same time choose not to block any decision relating to the operation. In this regard it is also worth mentioning that in some situations, the Troop Contributing Nations’ involvement in the decision making process is limited to the decision whether or not to participate with military forces, without having any role in the formulation of the political aspects of a mission. States which are not members of NATO may contribute with military forces to a NATO-led mission. NATO relies extensively on the contribution of forces from so-called “Non-NATO Contributing Nations (NNCN)”. These are States which are not parties to the Washington Treaty and are not members of NATO, but are willing to contribute forces to a NATO-led operation. From the earliest operations, NNCN have contributed to NATO operations in a substantial manner, notably Russia as the single largest contributor. As of September 2008, approximately 62,500 personnel were deployed in 5 NATO-led operations of which 4,300 personnel were provided by 16 NNCN.27 The Political Military Framework regulates the participation of NNCN in NATO operations. The process starts with an expression of interest by the NNCN in contributing to a specific NATO-led operation. Participation is dependent upon NAC approval, and, once approved, NNCN enter into technical agreements with NATO to work out security, technical and financial issues.28 NNCN will be consulted on all aspects of the operation, but do not have decision making power on, for instance, the concept of the operation, rules of engagement and periodic mission reviews.29 NNCN do not have any political influence on the mission as they do not take part in the decision making process at the NAC, but to allow SACEUR to have Operational Command and Control over their military forces. Even though the NAC enlarged the influence of NNCN in the operations they choose to participate in and are consulted and offered the opportunity to put forward views on all relevant issues of the operations, NATO, still retains full political decision-making authority.30 This shows that NATO as an international organization can act, to a certain extent, independently from States participating in the operation, in particular with respect to NNCN. 4.3.2 Planning Process of NATO Operations A second area where the particular nature of the relationship between NATO and the member States becomes apparent is during the operational planning process. It would be fair to conclude that NATO was effectively an instrument of the member States until the early 1990s. During the Cold War-period, the planning of operations was limited to the development of several regional Standing Defence Plans against one identified potential aggressor. These plans were preapproved by the NAC. The Defence Planning Committee31 set so-called “Force Goals” to which member States commit their forces for a period of 6 years. Member States annually reported on how they intended to meet these requirements.32 Overall, the decisions were taken at the capitals without much need of NATO’s involvement other than being a forum where discussions could take place. NATO relied on the same planning processes that existed during the Cold War for its first “non-article 5” operations in the early 1990s. And in fact, there was no real need to change the planning processes, as the first operations were fairly straightforward. They consisted of monitoring of an arms embargo (e.g. operation Maritime Monitor) or a no-fly zone (e.g. operation Sky Monitor). Neither, the IFOR, SFOR and KFOR required much involvement of NATO in the planning of the operation, as most of the forces were provided by a leader framework nation, which would take the responsibility for organizing the forces necessary in a specific sector. For instance, in implementing the Dayton Peace Agreement, Bosnia-Herzegovina was divided into 3 regions for which each a lead nation was assigned to carry out the operation.33 The planning of ISAF and NATO Training Mission in Iraq (NTM-I) operations was much more complex. These operations took place much farther away from NATO’s borders adding complexity in logistical planning and defence expenditure. They also took place in much less benign environments. Moreover, both operations went beyond the monitoring of a cease-fire and included tasks such as counter-insurgency activities, reconstruction of civil infrastructure and mentoring of government officials. The increased complexity of the operations required a more sophisticated planning process than the pre-delegation model that was used in previous operations. In the current planning process, when tasked by the NAC, SACEUR will conduct a formal assessment of the identified crisis and will give considerations on the use of the NATO military instrument to assist with a situation resolution. The NAC may then task SACEUR to develop military response options. Subsequently, the NAC may decide whether SACEUR should provide a concept of operations within the political direction given by the Council.34 The member States rely heavily on the planning done by SACEUR’s staff, as its integrated system analysis, planning and assessment tools,35 congregated databases on capabilities and availability of member States’ forces36 and doctrine37 provide planning capabilities that are not easily replicated in the national Ministries of Defense. The planning process does not alter the national autonomy of the member States or their ‘veto’ power at the NAC. The member States retain their authority to disapprove certain proposals and to halt or change a given course of action. However, the incremental decision-making process and the unique planning capabilities of NATO make it more difficult for member States to refuse participation on general grounds and discourages uncooperative behaviour.38 This observation leads to the conclusion that even though the member States retain sovereign control over NATO’s actions, the degree of control is limited on general political aspects of a mission and not on the specifics of each aspect of the operation. 4.3.3 The Command and Control Relationship The third and the last area that is examined here with respect to the relationship between NATO and its member States is the command and control relationship. NATO does not have military forces permanently assigned to the Organization. When a mission is deemed necessary, NATO will request nations to contribute the required forces and materiel to the mission. Nations will inform NATO on their contributions and transfer part of their authority over their forces to Alliance.39 Authority is then delegated throughout the organization at various levels. The degree of authority that each of the levels exercises is defined by the ‘command and control’ structure set in place.40 ‘Command’ is the authority to direct, coordinate or control armed forces to achieve particular objectives. ‘Control’ is the authority to organise, direct and coordinate the activities of the forces assigned to implement orders and directives. NATO differentiates between three levels of command and control, ranging from (a) Full Command, (b) Operational Command and Control and (c) Tactical Command and Control. States normally retain “Full Command”, which is the authority that covers every aspect of military and administration. It is very uncommon for States to transfer Full Command to NATO or any other international organization or State. Full Command includes the authority to decide to participate in a certain mission and to withdraw from participation in accordance with the terms agreed to. It also includes the authority to take administrative and disciplinary measures against personnel of its own armed forces.41 As described in Chapter 2, the Commander of the Kosovo Force ( COMKFOR) did not have the authority to take disciplinary measures against personnel that violated his order not to frequent prostitutes in Kosovo or to be engaged in the act of human trafficking. COMKFOR was dependent on the sending States to ensure that such regulations are enforceable through national disciplinary sanctions.42 States that contribute forces to NATO operations normally will transfer “Operational Command and Control” to the Alliance. Operational Command is the authority to assign missions or tasks, to deploy units and to reassign forces.43 It is the authority needed to effectuate the overall strategic objectives of the whole operation. Operational Control is the authority to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time, or location. This includes the authority to issue binding directives for forces assigned to his command. For example, as illustrated in Chapter 2, the tactical directive issued by COMISAF that restrained the use of force by troops assigned to him is an example of operational control. COMKFOR similarly had the authority to limit the frequenting certain bars and locales by KFOR personnel is the exercise of operational control. ‘Tactical Command’ is also transferred by TCNs to SACEUR. SACEUR usually delegates tactical command to subordinate command. Tactical Command is the authority to assign tasks to forces for the accomplishment of the mission, and Tactical Control is the detailed and local direction and control of movements or manoeuvres necessary to accomplish missions or tasks assigned. TCNs will ordinarily transfer Operational Command and Control to NATO, while retaining Full Command – including Administrative Control – over their forces. The transfer follows a formal procedure, which entails the TCN sending SACEUR a ‘transfer of authority message’. This message describes which units are placed under command of NATO and which level of authority is being transferred. After the transfer of command to NATO, the nations are not able to exercise control over their forces anymore, except by re-assuming command and thereby effectively taking their forces out from the mission. States may, however, issue limitations and restriction on the use of their forces, i.e. ‘national caveats’ and ‘red-card holdership’.44 In few instances, TCNs have re-assumed command over their forces during a NATO operation. As described in Chapter 2 of this book, Canada reassumed command over its forces during ISAF, when it assessed that the transfer of detainees captured by Canadian forces to the government of Afghanistan would pose them to the risk of being tortured. The transfer of authority over forces from States to NATO has relevant consequences to the question of responsibility for wrongful conduct during NATO operations, in particular to the aspect of attribution. Attribution of a wrongful act to NATO depends on whether NATO has international legal personality and whether the wrongful act was under the effective control of NATO. These issues are examined more elaborately in Chapters 5 and 7 of this book. It is relevant to note here that when TCNs place their forces at the disposal of NATO, they transfer the authority to assign missions or tasks, to deploy units and to reassign forces. This means that NATO exercises effective control over these forces with respect to mission-related tasks. This effective control, however, may be undermined by the issuance of national caveats, limitations or interference by the TCN involved or when the TCN decides to re-assume command over its forces. NATO’s command and control relationship also illustrate the relationship that the Alliance has with its member States and other TCNs. Nations transfer the authority over their forces to NATO, which indicates that the Alliance has a large degree of autonomy, even if nations still retain the possibility to re-assume command over their forces and the fact that they can impose limitations and restrictions on the use of the forces. 4.4 The Relationship between NATO and the UN NATO’s constituent document refers in several places to the UN, the UN Security Council and the UN Charter, showing the commitment of the founding members to the principles of the United Nations. Certain founding States even suggested to define NATO as a ‘regional arrangement’ in reference to Chapter  viii of the UN Charter.45 Under Chapter viii of the UN Charter, the UN Security Council may utilise such arrangements or agencies for enforcement action under its authority. This suggestion was, however, opposed46 as it could be interpreted as making NATO’s enforcement measures subject to a veto in the UN Security Council, rendering NATO’s existence absurd.47 Any reference to Chapter viii of the UN Charter was therefore intentionally omitted, leaving only Article 51 of the UN Charter as a basis for military action(s) of NATO under Article 5 of the Washington Treaty. NATO was not considered to become an organization that would be used to implement measures taken by the UN Security Council in accordance with Chapter vii of the UN Charter. The perception that NATO could not be a vehicle for the UN Security Council to implement its mandates, changed after the fall of the Soviet Union, when an institutionalised relationship between NATO and the UN started to emerge. The United Nations was involved in peacekeeping operations since 195648 and saw an enormous increase in missions from 1989.49 These operations were entirely conducted under UN command and control, without participation of any other international organization. Member States would be requested to provide troops and materiel to a un-led mission. The personnel were placed at the disposal of the UN, which were characteristically identified as “blue-helmets”. With the increased demand for missions, the UN turned to lead nations and international organizations to take over some of the burden to plan and lead peacekeeping and peace-enforcements missions. NATO became an important partner for the UN as the UN lacked the resources to implement its peace enforcement measures. NATO, on its turn, found the participation in the UN missions important as it was trying to redefine its tasks and activities and to transform its structure to meet the security challenges which occurred in the post-Cold War period. An important aspect defining the un-NATO relationship in the context of peace operations is the detailed guidance given by the UN Security Council regarding the mandate and the objectives to be achieved of a specific peace operation. The UN Security Council can authorise member States or international organizations50 to implement a specific mandate. In earlier UN Security Council resolutions, this mandate contained detailed guidance on how the objectives of the operation were to be achieved. For instance, UNSCR 1244(1999) listed eight specific areas for which the NATO-led Kosovo Force was made responsible.51 More recent UN Security Council resolutions leave a fair amount of discretionary power to the mandated entity to decide on how it will attain the objectives, basically authorizing to “take all necessary measures” to fulfil the mandate.52 The Security Council does not impose a specific command relationship or hierarchy between the UN and the mandated entity. However, in certain situations it requires States or international organization to coordinate with the UN Secretary General on the measures taken to implement the mandate or to report on the progress of the operation periodically.53 NATO and the UN cooperated quite successfully during operations in the Balkans. Initially, NATO enforced UN Security Council’s embargo on weapons in the Adriatic Sea54 and a no-fly zone over Bosnia-Herzegovina.55 The cooperation intensified when the Alliance provided air support to the United Nations Protection Force, or unprofor.56 Close air support provided by NATO was made conditional on the approval by the UN, which strained the relationship between the two organizations. Politically divergent views between the UN and NATO on the air support to UNPROFOR resulted in a time lag in the taking of decisions or resulted in no decisions at all. The observed difficulties led to future operations being more independent from each other. For instance, KFOR was placed outside UNMiK’s command and had a separate mandate.57 Subsequent operations also showed that NATO operations and UN operations in the same area have distinct mandates, tasks and command structure. In Iraq, the NATO Training Mission-Iraq (NTM-I) is separated from the UN Assistance Mission for Iraq (UNAMI) and in Afghanistan, the United Nations Assistance Mission in Afghanistan – a peacekeeping mission focusing on recovery and reconstruction58 – was separate from ISAF’s more stand-alone character with its own mandate and its own command structure.59 In 2005, the Alliance proposed a framework agreement with the UN to create a more structured relationship between the two organizations.60 In September 2008, this proposal resulted in a Joint Declaration between the UN and NATO on their mutual cooperation, in particular in the field of information sharing and operational coordination and support.61 Paragraph 4 of the Declaration stipulates that: Understanding that this framework should be flexible and evolving over time, we agree to further develop the cooperation between our organizations on issues of common interest, in, but not limited to, communication and information-sharing, including on issues pertaining to the protection of civilian populations; capacity-building, training and exercises; lessons learned, planning and support for contingencies; and operational coordination and support. In conclusion, The UN Security Council is the only institution to authorise the use of force to maintain or restore international peace and security. A UN Security Council resolution is the legal basis for NATO to conduct non-article 5 crisis response operations, that involve the use of force. UN Security Council resolutions will continue to govern NATO’s non-article 5 operations, but the Alliance remains independent from the United Nations in aspects of command and control in NATO operations. The Security Council will not have any authority regarding the command and control of forces in NATO-led operations. The UN can not assign missions or tasks to NATO personnel, to deploy units or to reassign the forces. This authority will be vested in the commander that has Operational Command, which is SACEUR. This aspect is relevant to the question of responsibility of NATO for violations of international law and will be further examined in Chapter 7. 4.5 Conclusions This chapter has described the institutional framework of NATO. Member States are represented in the North Atlantic Council (NAC), which is the highest political organ of the Alliance. Decisions on NATO operations are taken by the Council through consensus. The Secretary General of the Alliance is responsible for steering this process of consultation and has several tools at its disposal to achieve consensus, in particular the so-called ‘silence procedure’. Consensus and the silence procedure show that NATO enjoys a degree of autonomy from its member States, as the Alliance can function even without full agreement of all of the members. The NAC, its supporting International Staff and the civilian agencies constitute the civilian structure of the Alliance. The military structure consists of the Military Committee, supported by the International Military Staff, the two Supreme Commands and international military headquarters subordinate to them. Supreme Allied Commander Europe commands NATO operations. SACEUR has “operational command and control” over the military forces assigned to him by the Troop Contributing Nations, which could either be member States or States that are not member to NATO (Non-NATO Contributing Nations, or NNCN). Two aspects are relevant to note here. First, States that participate in NATO-led operations transfer a significant degree of control over military forces to NATO. Chapter 7 will examine in more detail whether the degree of control transferred to NATO by States equates to ‘effective control’. If NATO does have effective control over conduct of forces placed at its disposal, the conduct can be attributed to NATO. Secondly, it is relevant to note that the participation of NNCN in NATO-led operations show that NATO is a separate entity from its member States. NNCN do not take part in the decision-making process at the political level and neither have operational command and control over their forces once they are placed under the authority of SACEUR. This illustrates that NATO can act separately from its member States and enjoys a high degree of autonomy. This feature – further examined in Chapter  5  – speaks in favour of the existence of international legal personality of NATO.

#### ICJ and member states agree.

Alain Pellet 1, Professor of International Law at the University of Paris X-Nanterre and member of the International Law Commission, December 1, 2001, “L’imputabilité d’éventuels actes illicites – Responsabilité de l’otan ou des Etats membres, inTomuschat”, https://brill.com/view/title/10865 , Kosovo and the international community: A legal assessment, The Netherlands: Martinus Nijhoff, p. 198. [\\SYang](file:///\\SYang) \*\*Translated to English with Google Translate. Original text in French.

The question is therefore left entirely open. 14 The fact remains that, in the absence of certainty and given the extreme rarity of the practice, one can at least use the draft of the C.D.I. by analogy and, in particular, on the one hand articles 4 to 9 and 11 of the preliminary draft of 2000 (which correspond to articles 5 to 10 of the draft of 1996), which relate to the attribution strictly speaking, and , above all, Articles 16 to 19 (27 to 28 old) These latter envisage three hypotheses in which the "responsibility of a State with regard to the act of another State" may be engaged. One clearly seems to have to be discarded: that of coercion (envisaged by the new article 18); it seems absurd to consider that the Member States of NATO were able to exert on it a constraint leading it to commit one or more internationally wrongful acts, and vice versa. Two possibilities therefore remain. That of complicity (aid or assistance in the commission of an internationally wrongful act - new article 16) and that of "direction and [du] control exercised in the commission of an internationally wrongful act" (article 17 new). In both cases, it seems to me that you have to ask yourself "who controls whom?" (article 17) and "who is an accomplice of whom?" (section 16). In other words, does NATO control the member states? or are the states controlling NATO? Firstly; and is NATO the accomplice of the Member States? or the contrary? on the other hand. Asked in this way, the questions are a little reminiscent of the children's game that is called in France "I hold you, you hold me by the goatee" ... And, to tell the truth, it is possible to support, reasonably, one as the other of the two theses. Member states control NATO - they make the decisions within its bodies and it depends on them for its financial resources, ammunition and men. But NATO controls its Members in the sense that they act on and in accordance with its decisions. That said, an essential element, clearly highlighted in Professor Stein's communication16 and which constitutes the starting point of the 1995 resolution of the Institute of International Law on "The legal consequences for Member States of non-performance by international organizations of their obligations towards third parties",17 must be taken into account: NATO is an international organization and, as such, it enjoys international legal personality.18 It is true that it is rather special organization, the institutionalization of which has been empirical and progressive. legal capacity and privileges and immunities, all of which led the International Court of Justice, with regard to the United Nations, to conclude, in its opinion of 11 April 1949 relating to Reparations for damage suffered in the service of the United Nations, that she was an "international person". "This means that the Organization is a subject of international law, that it has the capacity to be the holder of international rights and duties and that it has the capacity to avail itself of its rights by way of international claim".20 Moreover, this responsibility is objective,21 which means that it forms a screen between the Organization and not only its Member States, not only the third States which have recognized it, but also vis-à-vis other States, in much the same way that a State exists independently of the recognitions of which it is the object. Counterpart of the right belonging to the Organization to seek the responsibility of other subjects of international law, it can also be the addressee of a claim, in particular when an internationally wrongful act can, as in this case, be attributed to it. It alone bears the responsibility for its own acts and it seems impossible - except to deny, in reality, its international legal personality - that the responsibility of its Members be sought for its operations or "through it".

### 1AR---AT: Member States Only---Topic Education DA

#### NATO empirically does a large majority of cooperation with global partners which are crucial to alliance functioning---their evidence doesn’t have *intent to exclude* and skews debate away from the core of NATO functioning---especially relevant as NATO 2030 is reorienting the organization towards *cooperation with global partners*.

The North Atlantic Treaty Organization 21, a military collective defense alliance including 30 European and North American countries that might come up in the 2022-2023 high school policy debate topic, August 25, 2021, “Relations with partners across the globe”, https://www.NATO.int/cps/en/NATOhq/topics\_49188.htm, official NATO website \\SYang

NATO has nine “partners across the globe” or “global partners”, which the Alliance cooperates with on an individual basis. NATO’s global partners include Afghanistan, Australia, Colombia, Iraq, Japan, the Republic of Korea, Mongolia, New Zealand and Pakistan. NATO’s engagement with global partners is taking on increasing importance in a complex security environment, where many of the challenges the Alliance faces are global and no longer bound by geography.

The NATO 2030 agenda agreed by NATO Leaders at the NATO Brussels 2021 Summit seeks to strengthen NATO’s global cooperation with like-minded partners, especially with its global partners, to defend the rules-based international order and institutions, to set international norms and standards in space and in cyberspace, and on new technologies and global arms control.

Since 2016, NATO has increasingly engaged politically with its four Asia-Pacific partners – Australia, Japan, the Republic of Korea and New Zealand – notably through meetings of the North Atlantic Council, including a first meeting at the level of foreign ministers in December 2020, to discuss the shift in the global balance of power and the rise of China.

NATO is also intensifying dialogue and cooperation with Colombia.

Global partners have access to the full range of activities NATO offers to all partners guided by an Individual Partnership Cooperation Programme. They work with NATO on a range of common cross-cutting security challenges such as cyber defence, counter-terrorism, non-proliferation and resilience.

Some partners participate in NATO’s military operations, while many have benefited from NATO’s expertise in areas such as building defence capacity, and defence training and education.

NATO also consults with other non-member countries, which have no bilateral programme of cooperation (for example, China, Brazil, Ghana, India, Singapore) in particular on regional security dynamics.

At the NATO Brussels Summit in June 2021, Allies agreed to strengthen NATO engagement with key global actors and other new interlocutors beyond the Euro-Atlantic area, including those from Africa, Asia and Latin America.

Wider cooperation

In today’s complex security environment, NATO’s relations with partners across the globe offers many advantages to Allies and partners alike. NATO’s practical cooperation with its global partners includes cross-cutting global challenges such as cyber defence, maritime security, humanitarian assistance and disaster relief, non-proliferation, defence science and technology, and Women, Peace and Security. Some partners participate in NATO’s military operations, while many have also benefited from NATO’s expertise in areas such as building defence capacity, and defence training and education.

Political consultation and intelligence-sharing is fundamental to the way NATO works with its global partners, just as it is among the 30 Allies. Political dialogue is a key tool for fostering regional understanding and exchanging expertise between Allies and their global partners. This enriches NATO’s situational awareness in areas beyond its direct neighbourhood, and it ensures that global partners understand NATO’s positions and are able to contribute to policy discussions on common security challenges. This is increasing in importance as many of today’s new security challenges are no longer bound by geography, such as in cyber space, space and climate change. Political dialogue also assists in establishing and developing practical cooperation with these partners.

Political dialogue with NATO’s global partners take place in many different formats, including at NATO Headquarters in Brussels, Belgium. Just as Allied consultations take place in a broad range of committees and at different levels, so too do several global partners participate in these committees on a regular basis, from the level of ministers to technical working groups. For example, NATO’s four Asia-Pacific partners – Australia, Japan, the Republic of Korea and New Zealand – participate on a regular basis in discussions in the Political Committee and in the North Atlantic Council.

At the most senior level, the Secretary General, the Deputy Secretary General, the Chair of the Military Committee and NATO’s Strategic Commanders meet with global partners’ Heads of State and Government, foreign ministers, defence ministers, as well as other high-level officials.

Support for NATO-led operations

The support provided by global partners and other countries to NATO-led operations has made a significant contribution to international peace and security.

In Afghanistan, a number of global partners such as Australia, the Republic of Korea and New Zealand, made important contributions to the NATO-led International Security Assistance Force (ISAF) from 2003 to 2014. Many continued to work alongside Allies in the follow-on Resolute Support Mission to train, advise and assist the Afghan security forces and institutions. Some countries supported stabilisation efforts in Afghanistan without being involved in combat. This includes Japan, which funded a large number of development projects and dispatched liaison officers, and Pakistan that provided ground and air lines of communication to resupply the mission . In 2020, the Republic of Korea served as the co-chair of the Afghan National Army Trust Fund Board.

Evolution of relations

NATO has maintained a dialogue with countries that are not part of its partnership frameworks, on an ad-hoc basis, since the 1990s. However, NATO’s involvement in areas outside of its immediate region – including Afghanistan and Libya – has increased the need and opportunities for enhanced global interaction. Clearly, the emergence of global threats requires the cooperation of a wider range of countries to successfully tackle challenges such as terrorism, proliferation, piracy or cyber attacks. Dialogue with these countries can also help NATO avert crises and, when needed, manage an operation throughout all phases.

Since 1998, NATO has invited countries across the globe to participate in its activities, workshops, exercises and conferences. This decision marked a policy shift for the Alliance, allowing these countries to have access, through the case-by-case approval of the North Atlantic Council, to activities offered under NATO’s structured partnerships. These countries were known as “Contact Countries”.

Significant steps were taken at the 2006 Riga Summit to increase the operational relevance of NATO’s cooperation with countries that are part of its structured partnership frameworks as well as other countries around the world. These steps, reinforced by decisions at the 2008 Bucharest Summit, defined a set of objectives for these relationships and created avenues for enhanced political dialogue, including meetings of the North Atlantic Council with ministers of the countries concerned, high-level talks, and meetings with ambassadors. In addition, annual work programmes (then referred to as Individual Tailored Cooperation Packages of Activities) were further developed.

At the 2010 Lisbon Summit, Allies agreed to develop a more efficient and flexible partnership policy, in time for the meeting of Allied foreign ministers in Berlin in April 2011. To this end, they decided to:

streamline NATO’s partnership tools in order to open all cooperative activities and exercises to partners and to harmonise partnership programmes;

better engage with partners across the globe who contribute significantly to security and reach out to relevant partners to build trust, increase transparency and develop practical cooperation;

develop flexible formats to discuss security challenges with partners and enhance existing fora for political dialogue; and

build on improvements in NATO’s training mechanisms and consider methods to enhance individual partners’ ability to build capacity.

Following the 2010 Lisbon Summit and NATO’s subsequent revision of its partnership policy in April 2011, the global context has changed significantly. As NATO became increasingly confronted with new defence and security challenges such as cyber attacks, disinformation, disruptive technologies and the erosion of arms control regimes, NATO recognised the importance of adapting to these new security challenges, including working closer together with NATO’s partners.

This increasing engagement with NATO’s like-minded partners, regardless of geographic location, on the basis of the shared values of democratic freedoms, rule of law and human rights, allows Allies to discuss relevant developments in the regions with partners, and increase their situational awareness and understanding of strategic issues on relevant global developments.

In June 2020, NATO Secretary General Jens Stoltenberg launched his outline for NATO 2030. In order for NATO to keep its Allies safe in a more uncertain world, the Secretary General stated that NATO must “stay strong militarily, be more united politically, and take a broader approach globally.” NATO taking a more global approach means working even more closely with like-minded partners to develop coherent, strong, unified and collective responses to defend our values in a world of increased global competition.

The global pillar of NATO 2030 is particularly relevant to NATO’s engagement with its four Asia-Pacific partners – Australia, Japan, the Republic of Korea and New Zealand. As the challenges confronting the Euro-Atlantic area and the Asia-Pacific region are increasingly converging, it is vital for NATO and its four close partners in the Asia-Pacific region to enhance cooperation and dialogue to support security in both regions, but also to work together to strengthen the international rules-based order. In December 2020, for the first time, the four Asia-Pacific partners participated in a NATO Foreign Ministerial Meeting, where NATO Allies discussed the shift in the global balance of power and the rise of China with the Asia-Pacific partners, as well as with Finland, Sweden and the European Union High Representative/ Vice President of the European Commission.

At the 2021 Brussels Summit, Allies agreed to increase dialogue and practical cooperation between NATO and existing partners, including partners in the Asia-Pacific, and to strengthen NATO engagement with key global actors and other new interlocutors beyond the Euro-Atlantic area, including from Africa, Asia and Latin America.

### 1AR---AT: Member States Only---NATO Card

#### The *MOST IMPORTANT* players are members---that implies *members aren’t the ONLY players IN NATO.*

The North Atlantic Treaty Organization 22, a military collective defense alliance including 30 European and North American countries that might come up in the 2022-2023 high school policy debate topic, accessed July 7, 2022, “What is NATO?”, https://www.NATO.int/NATO-welcome/, official NATO website \\SYang

The most important players in the North Atlantic Treaty Organization are the member countries themselves.

#### This means that we’re either ahead on the predictability debate because it’s literally the first thing on the *“What is NATO?” official webpage for NATO* OR at worst it’s a wash---that means you look to the implications of each model for *topic education* next---we’re winning that the model including partner states is better for topic education---it’s contextual to the functioning of NATO and crucial to understanding IR.

### 1AR---C/I---“is”

#### Their interpretation of NATO’s use of the word “is” is reductionist and straight up incorrect.

* Not sure why I put this card in here at all.

Writing Explained 22, some website that teaches grammar, "Is vs. Are – What’s the Difference?", https://writingexplained.org/is-vs-are-difference, accessed 7-7-2022 \\SYang

What does is mean? Is is a form of the verb to be, which indicates a state of existence or functions as an auxiliary verb. Is is the third-person singular present tense of to be.

Here are some example sentences,

Andy is a lying, backstabbing, two-faced, good-for-nothing jerk, and I refuse to invite him to the ice cream social.

That car is a waste of your money; you should look for a newer one with fewer miles.

Abigail is building a tiny house with her husband, Carl.

Antoine Griezmann has insisted he is happy at Atletico Madrid following renewed reports linking him with a big money move to Manchester United. –International Business Times

#### Take the example of “that car is a waste of your money”---everyone agrees that this is grammatically correct---that doesn’t mean the car is *SOLELY* a waste of your money---it’s also a mode of transportation. The same thing applies to *ALL* their interpretations of NATO---it IS a group of 30 countries, but not SOLELY a group of 30 countries---it also includes *partner countries.*

# In the Area

## 1NC

#### Interpretation: “In the area” means *all of* the activities

Law Insider, No Date, "In the area Definition," Law Insider, https://www.lawinsider.com/dictionary/in-the-area//jc

In the area means all of the activities. Examples of In the area in a sentence In the area of sustainability, Raiffeisen KAG also attends so-called “stakeholder forums” which provide an excellent platform for a dialogue with stakeholders such as suppliers, clients, employees, representatives of authorities and other investors. In the area of business dialogues, Raiffeisen KAG distinguishes between pro-active and reactive engagement. In the area between roadways of a divided highway, including crossovers.

#### Violation: The aff only does one sector

#### That’s a voter:

#### A --- Limits --- any other interp explodes the topic as there are infinitely more specifics about each individual sector as opposed to all three

#### B --- Ground --- core negative ground CPs/DAs and solvency deficits to NATO’s activities over cybersecurity, AI, and biotech --- that’s key in a topic with no neg generics.

#### C --- Topic Education --- allowing non-AI affs causes a race to the bottom find the most arbitrary specifics about individual sectors and skews the debate from learning about NATO’s activities

## 2NC

### 2NC---AT: “One or More”

#### Plain English agrees that one or more means more

Martin Lassen, No Date, ""One Or More Is" or "One Or More Are": Which Is Correct?," Grammarhow, https://grammarhow.com/one-or-more-is-or-one-or-more-are///jc

“One or more” is used to talk about something that is either equal to one or any number greater than that. It’s always used in a context that means more than one but without any real indication of whether one might be the correct number. Generally, if you say “one or more,” it means you’re unsure what the number you’re talking about is exactly. It can refer to “one,” but you’re usually confident that it should refer to a few more as well.

#### Grammar outweighs --- it determines meaning, making it a pre-requisite to predictable ground and limits – and, without it, debate is impossible

Allen 93 (Robert, Editor and Director – The Chambers Dictionary, Does Grammar Matter?)

Grammar matters, then, because it is the accepted way of using language, whatever one’s exact interpretation of the term. Incorrect grammar hampers communication, which is the whole purpose of language. The grammar of standard English matters because it is a codification of the way using English that most people will find acceptable.

#### General consensus

English Language & Usage Stack Exchange, 12-1-2016, "Which is correct: "one or more is" or "one or more are"?," https://english.stackexchange.com/questions/13284/which-is-correct-one-or-more-is-or-one-or-more-are//jc

The Cambridge Guide to English Usage says: For most writers the choice depends on whether you’re thinking of a single case or general principle. Usage commentators in the UK and the US have been inclined to say it should be plural; and the Harper–Heritage usage panel voted heavily in its favor (78%). Yet Webster’s English Usage (1989) found ample American evidence for the singular construction, and it’s just as common as the plural in British data from the BNC. Writers using the singular take their cue from one, whereas the plural-users are responding to those [people] or the [things]. (BNC stands for British National Corpus. It is a computer database of 100 million words.)

#### Experts agree it takes a plural form

Danjuma Danladi, 05-14-2019, "The Copyeditor s Handbook A Guide for Book Publishing and Corporate Communications Second Edition," University of California Press, <https://www.academia.edu/32834137/The_Copyeditor_s_Handbook_A_Guide_for_Book_Publishing_and_Corporate_Communications_Second_Edition>//jc

Rule 18, page 345

One or more x. The expression one or more always takes a plural verb. One or more files are missing. One or more of these reports are out of sequence.

### Other Cards

#### “In” means throughout

Oxoden 1866 (Ashton, Reverend and Honorary Canon of Canterbury, “Our Church and Her Services”, p. 67, Google Books) //jc

Thirdly, that His will may be done by us here on earth, as it is done by saints and angels in the world above. We say "in earth," and not on earth; for the word in means throughout—that is to say, in every part of the earth.

## 2AC

## We Meet

#### Our plan spills over to security cooperation on all 3 eventually, but our aff is key to kickstarting it

### W/M: AI K2 Biotech

#### AI is the future of biotech

Catherine Shaffer, 4-1-2020, "Artificial Intelligence Is Helping Biotech Get Real," GEN - Genetic Engineering and Biotechnology News, https://www.genengnews.com/insights/trends-for-2020/artificial-intelligence-is-helping-biotech-get-real/

Artificial intelligence (AI) may sound futuristic, but it already exists in many everyday technologies. For example, it gives our handheld devices voice and facial recognition capabilities. AI is also making its presence felt in biotechnology, where it has become integral to many aspects of drug discovery and development. AI applications in biotech include drug target identification, drug screening, image screening, and predictive modeling. AI is also being used to comb through the scientific literature and manage clinical trial data. By leveraging machine learning, AI can manage disparate clinical trial datasets, enable virtual screening, and analyze vast amounts of data. Besides reducing clinical trial costs, AI can gain otherwise unobtainable insights and feed them back into the drug development process. AI technologies to serve the biotech industry are being developed by several companies. Their services are rapidly becoming indispensable as older methods like classical statistical analysis or manual image scanning reach their practical limits.

### W/M: AI K2 Cybersecurity

#### AI is an essential part of cybersecurity

Gaurav Belani, No Date, "Artificial Intelligence in Cybersecurity," No Publication, https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

The cyberattack surface in modern enterprise artificial intelligence graphics Source environments is massive, and it’s continuing to grow rapidly. This means that analyzing and improving an organization’s cybersecurity posture needs more than mere human intervention. AI and machine learning are now becoming essential to information security, as these technologies are capable of swiftly analyzing millions of data sets and tracking down a wide variety of cyber threats — from malware menaces to shady behavior that might result in a phishing attack. These technologies continually learn and improve, drawing data from past experiences and present to pinpoint new varieties of attacks that can occur today or tomorrow. In this post, we’ll review the use of AI in cybersecurity (both good and bad), along with what the experts and executives have to say about this matter.

### W/M: Cybersecurity K2 Biotech

#### Cybersecurity key to Biotech

Frank Van, 3-23-2021, "How cybersecurity helps biotech companies prepare for successful IPO," No Publication, https://www.ey.com/en\_nl/life-sciences/how-cybersecurity-helps-biotech-companies-prepare-for-successful-ipo

Biotech companies should incorporate a solid cybersecurity posture as they progress from entrepreneurial start-up towards public listing. In brief The ‘bad guys’ are always looking for their next target. Companies preparing to list create a lot of buzz, and draw the attention of these bad guys. Cybersecurity has become a business imperative. As every biotech company is unique, a cybersecurity program needs to be customized to their specific risks. By understanding their cybersecurity posture, biotech companies can make better decisions towards a more secure future. Publicly listed biotechs: attractive targets for cyber criminals One thing cyber criminals, hacktivists, nation states and other malicious actors have in common is that they generally do their homework, looking for the next opportunity and target. Biotech entrepreneurs that are leading their companies towards successful initial public offerings (IPOs), draw attention to themselves through media announcements and investment community buzz. Consequently, as also shown in the visual below, these companies are commonly targeted for their intellectual property, financial information and other sensitive assets, their “crown jewels.” Today, cybersecurity is no longer just a technology or risk issue. It has become a strategic business imperative. A cyber breach or data leak would be detrimental right before an IPO – a critical time when the integrity of your company and your brand needs to be perceived as positively as possible. [AD OMITTED] Defining the right cybersecurity approach The right cybersecurity program helps defend a company by defining and developing controls that enable stable growth, safeguard critical assets, reduce the likelihood of a breach, or to help recover quickly should there be an incident. It’s best to develop a cybersecurity strategy and program that suits a specific company’s needs and environment, with best practices and recommendations that are essential for pre-IPO companies. By taking a proactive approach to managing cybersecurity risk, you’ll send a positive message to existing and future investors, board members and other key stakeholders: not only do you care about innovation and generating value but you care enough to protect it.

## 2AC---C/I

### 2AC---C/I: “part of”

#### “In the area” means part of it

Cambridge Dictionary, No Date, "area," Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/area//jc

a subject or activity, or a part of it: Principal growth in the past year has been in the area of new technology in manufacturing and medical settings. He looked continually for ways to expand his startup firm's area of expertise

### 2AC---C/I: “one OR more”

#### The topic reads “in one or more”

#### *Or* means there is an alternative and we can choose

TheFreeDictionary, No Date, "Legal Dictionary: Or," https://legal-dictionary.thefreedictionary.com/Or//jc

or

conj. either; in the alternative. It is often vital to distinguish between "or" and "and." Example: Title to the Cadillac written "Mary or Bill Davidson" means either one could transfer the car, but if written "Mary and Bill Davidson," both must sign to change title.

# Artificial Intelligence

# T: AI Submarines

## Indicts

### AT: Groen

#### Groen is a borderline miscut---definitely doesn’t have to intent to include. Groen says the US will develop AI standards, and also do security cooperation---that doesn’t mean AI standards is part of security cooperation. Plus, limits DA---they can’t pick and choose, if their reading of Groen is correct, then education norms, AI ethics, AI policy, AI governance, and best practice is all topical---that’s basically anything that’s tangentially related to AI. [WE READ GREEN]

2AC Groen ‘20

(Michael S. Groen, Director, Joint Artificial Intelligence Center, “Joint Artificial Intelligence Center Director Briefs Reporters on Efforts to Scale AI,” pg online @ https://www.defense.gov/News/Transcripts/Transcript/Article/2427955/joint-artificial-intelligence-center-director-briefs-reporters-on-efforts-to-sc/ //um-ef)

<<<GRAY HIGHLIGHTING FOR REFERENCE>>>>

One thing we note is that stovepipes don't scale, so we will work through our partners in the AI Executive Steering Group and the -- and the subcommittees of that group, to integrate and focus common architectures, AI standards, data-sharing strategies, educational norms, and best practice for AI implementation. We'll continue to work across the department on AI ethics, AI policy, AI governance, and we'll do that as a community. We'll also continue to work with like-minded nations to enhance security cooperation and interoperability through our AI partnership for the – for defense. All of the JAIC’s work comes back to that enabling, that broad transformation across the department. We want to help defense leaders see that AI is about generating essential warfighting advantages. AI is not IT (information technology). It's not a black box that a contractor's going to deliver to you. It's not some digital gadget that an IT rep will show you how to log into.

#### Also, this card is not precise by any interpretation---it’s a transcript of Groen at a press conference---not an officially published statement, and he has exterior incentives to quantify his field as security cooperation because it makes the JAIC sound more credible---he’s the director of the JAIC.

### AT: Pfau

#### Pfau doesn’t say what they think---OOPS---says AI would use data from ML models in the context of the aff---that’s effects T at best---that’s bad because we would have to concede solvency for them to get there---it allows unpredictable aff advantages, makes neg prep impossible, and mixes burdens. [WE READ GREEN]

2AC Pfau ‘21

(Lieutenant Andrew Pfau, USN, is a submariner serving as an instructor at the U.S. Naval Academy. He is a graduate of the Naval Postgraduate School and a recipient of the Rear Admiral Grace Murray Hopper Computer Science Award, “A ROADMAP TO SUCCESSFUL SONAR AI,” pg online @ https://cimsec.org/tag/asw/ //um-ef)

Dataset Curation

Artificial Intelligence and Machine Learning are often conflated and used interchangeably. Artificial Intelligence refers a field of computer science interested in creating machines that can behave with human-like abilities and can make decisions based on input data. In contrast, Machine Learning, a subset of the AI filed, refers to computer programs and algorithms that learn from repeated exposure to many examples, often millions, instead of operating based on explicit rules programmed by humans.4 The focus in this article is on topics specific to ML models and systems, which will be included as parts in a larger AI or autonomous system. For example, an ML model could classify ships from passive sonar data, this model would then feed information about those ships into an AI system that operates an Unmanned Underwater Vehicle (UUV). The AI would make decisions about how to steer the UUV based on data from the sonar ML model in addition to information about mission objectives, navigation, and other data.

### AT: Wang

#### Wang’s from 2009---plus it’s talking about ML being key to AI research---not being part of AI itself---it’s a pre-requisite, but not part of it.

2AC Wang 09 Ph.D. from Beijing Institute of Technology Professor with the School of Information and Electronics, BIT(Hua, 12-19-2009, "A Brief Review of Machine Learning and Its Application," International Conference on Information Engineering and Computer Science, https://ieeexplore.ieee.org/abstract/document/5362936)HS

<<<GRAY HIGHLIGHTING FOR REFERENCE>>>>

With the popularization of information and the establishment of the databases in great number, and how to extract data from the useful information is the urgent problem to be solved. Machine learning is the core issue of artificial intelligence research, this paper introduces the definition of machine learning and its basic structure, and describes a variety of machine learning methods, including rote learning, inductive learning, analogy learning , explained learning, learning based on neural network and knowledge discovery and so on. This paper also brings foreword the objectives of machine learning, and points out the development trend of machine learning. Learning is the main hallmark of human intelligence and the basic means to obtain knowledge. Machine learning is the fundamental way to make the computer intelligent. R.Shank has said: "If a computer can not learn, it will not be called intelligent." Since learning is an integrative mental activity with memory, thinking, perception, feeling, and other mental activities closely related. So, researchers from different fields give a different interpretation with different disciplines respectively, and give some different points of view. II. MACHINE LEARNING Machine learning is a subject that studies how to use computers to simulate human learning activities, and to study self-improvement methods of computers that to obtain new knowledge and new skills, identify existing knowledge, and continuously improve the performance and achievement. Compared with human learning, machine learning learns faster, the accumulation of knowledge is more facilitate the results of learning spread easier. So, any progress of human in the field of machine learning, will enhance the capability of computers, thus have an impact on human society

### AT: MIT

#### Thanks for reading this card, it flows neg---it concedes both that ML is only a subfield and that AI needs to imitate intelligent human behavior---that spots us our T interp that AI is fully autonomous---that’s NOT the aff.

2AC MIT 22—Massachusetts Institute of Technology (MIT Sloan, 6-29-2022, "Machine learning, explained," https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained)HS

<<<GRAY HIGHLIGHTING FOR REFERENCE>>>>

Machine learning is a subfield of artificial intelligence, which is broadly defined as the capability of a machine to imitate intelligent human behavior. Artificial intelligence systems are used to perform complex tasks in a way that is similar to how humans solve problems. The goal of AI is to create computer models that exhibit “intelligent behaviors” like humans, according to Boris Katz, a principal research scientist and head of the InfoLab Group at CSAIL. This means machines that can recognize a visual scene, understand a text written in natural language, or perform an action in the physical world. Machine learning is one way to use AI. It was defined in the 1950s by AI pioneer Arthur Samuel as “the field of study that gives computers the ability to learn without explicitly being programmed.”

## T-Interps

### 1NC---SC---Must be DOD

#### Interpretation---“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

#### Violation---AI submarines are made by government contractors like Boeing---that’s not the DOD.

* Maybe also a substantial violation if we have one of those?

Kyle Mizokami 19,

The U.S. Navy has awarded a contract to Boeing for four Extra-Large Unmanned Underwater Vehicles (XLUUVs). In other words: giant drone subs.

The unmanned submarines, called Orcas, will be able to undertake missions from scouting to sinking ships at very long ranges. Drone ships like the Orca will revolutionize war at sea, providing inexpensive, semi-disposable weapon systems that can fill the gaps in the front line—or simply go where it’s too dangerous for manned ships to go.

The contract, announced today, stipulates Boeing will get $43 million for “fabrication, test, and delivery of four Orca Extra Large Unmanned Undersea Vehicles (XLUUVs) and associated support elements.” That’s just over ten million bucks per boat.

#### That’s a voter---

#### A---Limits---allowing other agencies blows the lid off of topical affirmatives as squirrelly 2A’s will write affirmatives using random components of the government---that’s uniquely bad on a bidirectional topic with three topic areas.

#### B---Ground---any other interpretation allows the 2AC to spike out of DOD-based offense like the tradeoff DA and counterplans that compete off of agency like the DOS counterplan---this topic has no neg generics which means our ground offense outweighs.

#### C---Topic Education---any other interpretation causes a race to the bottom to use the most irrelevant parts of the USFG which obfuscates learning about true mil-to-mil interactions which was the intention of the topic paper.

#### At best they’re extra-T because they use the manufacturer---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

### 1NC---SC---Must be DSCA

#### Interpretation*---*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]

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.

#### Violation---the aff uses the Naval Meteorology and Oceanography Command---that’s a separate part of the DOD.

Jonathan B. Holloway 22, Commander, Naval Meteorology and Oceanography Command (CNMOC), “Naval Oceanography is DOD’s Leading UUV Authority”, <https://www.navy.mil/Press-Office/News-Stories/Article/2946198/naval-oceanography-is-dods-leading-uuv-authority/> \\SYang

STENNIS SPACE CENTER, Miss. —— Underwater warfare, as a physical-battlespace, has grown in parallel to current technological innovation, expanding use of unmanned underwater vehicles (UUV), and the U.S. Naval Meteorology and Oceanography Command (Naval Oceanography) has prepared—over the last 150 years—to be the nation’s leading authority for all things UUV.

Naval Oceanography uses an assortment of UUVs to collect environmental-battlespace data which create real-time, predictive models for operational purposes to the U.S. Navy’s Fleet—where each UUV is utilized based on its unique capability.

“We [Naval Oceanography] have participated in surges of 50 and 100 unmanned vehicles in past years and this year we expect to deploy up to 200 unmanned underwater vehicles over the Atlantic Ocean to better characterize the complex ocean currents,” said Rear Admiral Ron Piret, Commander, Naval Meteorology and Oceanography Command (CNMOC).

Naval Oceanography is home to the 24-hour, seven-days a week Glider Operations Center—a UUV program established in 2010 of civilian pilots who command and control an inventory of over 130 Littoral Battlespace Sensing-Gliders (LBS-G).These buoyancy-driven UUVs are deployed globally, using satellite communication to set predetermined locations in collecting data.

#### That’s a voter---

#### A---Limits---any other interpretation blows the lid off of topical affirmatives as 2A’s will race to find the most obscure parts of the federal government which is uniquely bad on a bidirectional topic with three topic areas.

#### B---Ground--- any other interpretation allows the 2AC to spike out of DSCA-based offense like the DSCA tradeoff DA and counterplans that compete off of sub-agency---this topic has no neg generics which means our ground offense outweighs.

#### C---Topic Education---

#### At best they’re extra-T---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

### 1NC---AI---Fully Autonomous

#### Interpretation---AI refers exclusively to completely autonomous technologies.

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.

#### Violation---UUVs aren’t even close to fully autonomous---we’re still in the process of transitioning and developing norms.

Dr. Alix Valenti 22, defense and security freelance journalist for Armada International, January 17, 2022, "Dead Reckoning – Pathways to USV/UUV Autonomy", https://www.armadainternational.com/2022/01/dead-reckoning-pathways-to-usv-uuv-autonomy/, Armada International, accessed 7-11-2022 \\SYang

‘Autonomous’, ‘unmanned’, ‘uncrewed’, ‘lean manning’… over the past few years, the defence world has seen a proliferation of terms emerge to refer to the progressive removal of humans from naval vessels. And, as is usually the case with most buzzwords entering a new domain, most of these terms have been used interchangeably to underpin the evolution of Unmanned Surface Vehicles (USV) and Unmanned Underwater Vehicles (UUV).

The reality, of course, is far more complex. Behind the concepts of USVs and UUVs lie different levels of autonomy, with different degrees of human involvement for different missions and with each degree of autonomy/human involvement comes a range of operational opportunities and technological challenges.

Unpacking Autonomy

“When we talk about ‘autonomy’ we need to have a common language,” Matthew Hunt, product line director Mine Warfare Systems at Thales, told AI. “This is important because if it is fully autonomous, capable of sensing and reacting to its environment, it is a totally different tool to an automated clockwork system following pre-defined patterns underwater.” Depending on the level of autonomy, the systems will be more or less complicated, will integrate different technologies and may be used in different operational contexts.

In a White Paper titled Navigating the Ethical Use of Autonomous Weapons Systems, published in June 2020, the BMT Group presents an overview of the different levels of control. It draws from the Maritime Autonomous Surface Ships (MASS) UK Industry Conduct Principles and Code of Practice, as well as from a number of other reports, to define six levels: manned, operated, directed, delegated, monitored and autonomous.

“Moving to fully autonomous, however, continues to present fundamental ethical challenges,” said Jake Rigby, research and development lead for Defence and Security at BMT.

For Hunt, it means that these systems must fulfil the three Ts: Trust that the system will work every time the way it is expected to; and, Technology and Time, that is, the ability for navies to quickly adapt to fast-paced technological advances by working closely with industry.

As such, presently, the increasing number of USV and UUV programmes undertaken by tier one navies across the world span across the first levels of autonomy. They feature systems that range from being remotely operated by navy crew to platforms that can be programmed to carry out pre-defined monitored missions autonomously. The latter does not, however, equal full levels of autonomy: the human is still in the loop and the parameters of each mission are very clearly defined in advance. Autonomy extends to navigation, data gathering and data transfer only.

#### That’s a voter---

#### A---Limits---allowing anything tangentially related to AI blows the lid off of topical affirmatives and leads to practically every piece of military technology being considered a topic area---that’s uniquely bad on a bidirectional topic with three areas.

#### B---Ground---any other interpretation decimates core neg ground by spiking out of AI links and AI bad with “we’re not fully autonomous”---that’s especially bad when there’s literally no disads and NATO bad is terminally non-unique.

#### C---Topic Education---any other interpretation loses the brightline for the definition of AI and causes a race to the bottom for the most obscure and irrelevant types of technology---that obfuscates education about true EDTs.

#### They’re also extra-T because submarines are more than just AI---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

### 2NC---AI---Fully Autonomous---Violation

#### “Pre-Programmed instructions”---doesn’t sound like AI to me.

British Aerosystem Services 21, British multinational arms, security, and aerospace company based in London, England and the largest defence contractor in Europe, Carbon dated April 15, 2021, “What are Autnomous UUVs?”, https://www.baesystems.com/en-us/definition/what-are-autonomous-uuvs \\SYang

Designed to operate below the water’s surface in both littoral (coastal) areas and the open sea, Autonomous UUVs have no crew aboard and are capable of carrying out missions using a mix of reconfigurable pre-programmed instructions, sensor-responsive directives, and, when near the surface, GPS navigation. They are similar to Remotely-Operated Underwater Vehicles (ROVs), but ROVs are piloted by a human on another nearby water craft via a tether, while Autonomous UUVs operate independent of a human pilot, so there is no tether. These unmanned submersibles simply perform their assigned mission, then return to pre-programmed coordinates with no human intervention.

#### There are five levels of UUV autonomy---only the fifth meets our interpretation---no UUVs come even close to the fifth.

[Simon Watson](https://pubmed.ncbi.nlm.nih.gov/?term=Watson%20S%5BAuthor%5D), [Daniel A. Duecker](https://pubmed.ncbi.nlm.nih.gov/?term=Duecker%20DA%5BAuthor%5D), and [Keir Groves](https://pubmed.ncbi.nlm.nih.gov/?term=Groves%20K%5BAuthor%5D) 20, Department of Electrical and Electronic Engineering, The University of Manchester; Department of Electrical and Electronic Engineering, The University of Manchester; Department of Electrical and Electronic Engineering, The University of Manchester, October 30, 2020, “Localisation of Unmanned Underwater Vehicles (UUVs) in Complex and Confined Environments: A Review”, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7663020/> \\SYang

UUV operation is not a binary choice between fully manual or fully autonomous, rather there are different levels of autonomy (LoA) [[35](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7663020/#B35-sensors-20-06203)]. For this work, we will adopt and adapt the six levels of autonomy proposed for surgical robots in [[36](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7663020/#B36-sensors-20-06203)].

0. No Autonomy—the UUV is entirely tele-operated by a human.

1. Robot Assistance—the UUV provides some automated functionality, for example staying at a set depth (set by the operator) or prohibiting the operator to maneuver into obstacles. The operator is still in full control of the UUV.

2. Task Autonomy—the UUV is able to execute motions under the guidance of the operator. For example way-points could be set to which the UUV will travel with no further input from the operator.

3. Conditional Autonomy—the UUV generates task strategies, but requires a human to select which one to undertake. For example, when exploring an environment, the UUV may identify several different routes to take, with the human selecting the most appropriate one.

4. High Autonomy—the UUV can plan and execute missions based on a set of boundary conditions specified by the operator. The operator does not require to select which one the UUV should do, however they are there to oversee the task execution.

5. Full Autonomy—the UUV requires no human input at all. It is deployed into the environment and left with no operator oversight.

[Table 2](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7663020/table/sensors-20-06203-t002/) shows current mission activities that are undertaken by UUVs and their levels of autonomy. Inspection tasks are currently conducted in all environments except for modern nuclear storage facilities. Limited maintenance and repair activities are conducted in legacy nuclear storage ponds, liquid storage tanks and on offshore assets. The highest level of autonomy achieved is 1, where the UUV is able to automate basic functions, such as staying at a given depth. There are no autonomous activities undertaken in any of the environments.

#### The technology doesn’t even exist yet---no takebacks. [WE READ GREEN]

1AC Wilson 19 – J.R. Wilson has been a full-time freelance writer, focusing primarily on aerospace, defense and high technology, since 1992, when he finished a four-year assignment as North American Group Editor for the UK-based Jane’s Information Group. A 1971 graduate of the University of Missouri School of Journalism, he spent eight years with United Press International before joining McDonnell Douglas Astronautics Co. as head of public relations for the space sector. ("Unmanned submarines seen as key to dominating the world’s oceans," Military Aerospace, 10-15-2019, https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence, Accessed 7-1-2022, LASA-SC)

The Spanish and British empires dominated the world in large part by dominating the oceans. Nazi Germany and Imperial Japan were major sea powers during World War II by adding submarines to their surface fleets.

That combination remains the key to sea power today, dominated by the U.S. Navy, with 68 nuclear-powered submarines, 11 aircraft carriers, and more than 450 other ships like destroyers, cruisers, and support ships.

In recent years, China has overtaken the U.S. in numbers, with more than 500 ships, including 75 submarines and three aircraft carriers, of which about half has been built since 2010. Still, China’s open-ocean naval capability lags far behind the U.S. No other navy in the world comes close to the U.S. or China. Now a new era in naval power is emerging — unmanned vehicles.

Nearly two decades into the 21st Century, both nations are putting significant effort into adding autonomous and semi-autonomous platforms to their surface and subsurface naval forces. The underwater realm is the most difficult because of the limitations of underwater communications, which makes some form of artificial intelligence (AI) mandatory.

China has been uncharacteristically open about its intentions for AI, from an announced underwater city inhabited and operated entirely by robots to official government goals of capitalizing on AI to transform their military into the strongest in the world.

While Chinese government spending on AI research is far greater than that of the U.S., however, a large percentage of global effort is coming from the U.S. commercial sector, on which the Pentagon relies heavily for technology advances. Still, Chinese companies also are increasing their AI investments.

The influence of massive spending on developing AI for undersea systems portends the greatest change in military sea power since the introduction of nuclear-powered vessels.

“Equipping our military vessels with a higher-level of artificial intelligence is the answer to the increasing size and complexity of data to be processed as well as the need to reduce staff,” says Dominique Giannoni, an executive at Thales Underwater Systems in Valbonne, France.

China autonomous undersea efforts

In a rare July 2018 interview with the South China Morning Post, Lin Yang, director of a classified program at the Shenyang Institute of Automation in Shenyang, China, says her country has plans to develop new-generation military underwater robots by 2021. His 912 Project’s goal is to develop AI-driven unmanned submarines to handle surveillance, mine laying, and attack missions.

Western China-watchers say the Chinese navy has several AI-enabled vessels in development — with a focus on autonomous submarines — as part of a major push to overtake U.S. dominance in the Indo-Pacific region and beyond. That includes 100-foot long extra-large unmanned underwater vehicles (XLUUVs) intended for deployment early in the next decade.

Another civilian project is China’s most ambitious undersea AI effort to date, with significant military potential. In 2018, China announced it was working on an AI-run underwater base, equipped with autonomous submarines to extend its reach.

According to published reports, the submarines would deploy for investigation and scientific surveillance missions, then return to the unmanned base to download data and recharge. The base itself, located on the ocean floor as deep as 36,000 feet, also would conduct research on the immediate area, process and fuse all collected data, and transmit the results to a surface ship or land station.

No location for the base or a timetable for its deployment have been released, but, given the speed with which China is developing AI across the board, and especially for undersea applications, the first elements are expected in the near future.

While being promoted as a major advance in research on undersea life and topography, the military potential of such long-endurance unmanned cooperative systems cannot be ignored.

China must “grasp the changes of national security circumstances, speed up preparations for military struggle, including battle planning, capacity building and command system building,” Chinese President Xi Jinping said in a speech during a naval inspection in Qingdao, China, according to China Daily.

Russia also is putting considerable effort into AI, but is not believed to be anywhere near the level of the U.S. or China.

U.S. autonomous undersea programs

The 2020 Pentagon budget request cites advances of potential adversaries in asking for major funding increases for autonomous weapons programs. Requests include a ten-fold increase in spending on large unmanned surface vessels by the Navy and more than 50 percent more for Army robotics development. The requests total $3.7 billion on unmanned systems across the services, plus another $900 million on AI.

The Embracing Artificial Intelligence in Undersea Warfare session at the Navy Submarine League’s Submarine Technology Symposium in May summarized the U.S. Navy’s increasing focus on AI — especially undersea:

“As the current submarine force trusts mechanical and electrical technology to execute the mission, the future force will need to trust AI to extract and exploit actionable patterns among an ocean of data,” the session says. “The advent of big data and deep learning technology has rendered signal detection and classification an increasingly automated process. Furthermore, advances in autonomous navigation have enabled unmanned platforms to operate alone or in swarms.

“It will be critical for the 21st century that the undersea fleet advance in its AI capabilities, develop algorithms that are intuitive and explainable, cultivate users’ trust in AI, and design future systems around the use of AI. Meanwhile, we must also recognize our adversaries’ disruptive AI capabilities and develop appropriate countermeasures against them.”

Despite technological strides in AI, unmanned maritime vessels face a host of new and potentially disabling challenges — especially in underwater applications. A 2014 Rand Corp. research paper on Designing Unmanned Systems with Greater Autonomy looked at how AI is being implemented — and researched for future application — across the board for unmanned systems. The report also noted the unique challenges facing UUV autonomy.

“Achieving and maintaining communication with underwater vehicles and even with surface vehicles is technically challenging, especially at longer ranges. Water attenuates radio waves and other wireless signals that can easily be used at long range in air-to-ground or air-to-air communications,” the report stated. “This means that high-bandwidth communications underwater are largely impractical using traditional communication technologies.”

“Although there has been some experimentation with laser communications for underwater applications, laser communications systems are expensive and consume considerable amounts of power. Because of these communications limitations, UUVs that do not require continuous communications links are essential. For example, autonomous path planning is needed to avoid underwater obstacles and unanticipated terrain features.”

### 1NC---AI---All of it.

#### Interpretation---topical affirmatives must engage with all aspects of the field of artificial intelligence.

#### “in”

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

#### “the”

Kentucky Supreme Court 3 (Opinion in Kotila v. Com., 114 SW 3d 226 - Ky: Supreme Court 2003. Google scholar caselaw, date accessed 9/26/21)

Whether a conviction under this statute requires possession of all (as opposed to any) of the chemicals or equipment necessary to manufacture methamphetamine under some manufacturing process is a matter of statutory construction. First, we examine the language of the statute, itself. United States v. Health Possibilities, P.S.C., 207 F.3d 335, 338-39 (6th Cir.2000) ("The starting point in a statutory interpretation case is the language of the statute itself."). Obviously, the multiple manufacturing methods and the availability of a broad range of readily available chemicals and equipment necessary for each manufacturing process militates against itemizing within the statute all of the possible chemical and equipment combinations by which methamphetamine could be manufactured. Nevertheless, KRS 218A.1432(1)(b) does not read "[p]ossesses chemicals or equipment," or "[p]ossesses some of the chemicals or equipment," or "[p]ossesses any of the chemicals or equipment." It reads "[p]ossesses the chemicals or equipment for the manufacture of methamphetamine." The presence of the article "the" is significant because, grammatically speaking, possession of some but not all of the chemicals or equipment does not satisfy the statutory language. "The" is "[u]sed as a function word before a plural noun denoting a group to indicate reference to the group as a whole." Webster's Third New International Dictionary 2369 (1993).

In decisions spanning three different centuries, the appellate courts of this Commonwealth have found use of the word "the" to have a significant effect upon meaning. See Revenue Cabinet v. Hubbard, Ky., 37 S.W.3d 717, 719-20 (2000) ("[U]se of the definite article `the' indicates that the statute refers to the entire body and not to discrete parts or components ...."); Cardwell v. Haycraft, Ky., 268 S.W.2d 916, 918 (1954) (the trial court's contributory negligence instruction was erroneous in that it contained the definite article "the" before the words "proximate cause" and "such language indicates that `the sole' rather than `a contributing' cause was meant."); Schardein v. Harrison, 230 Ky. 1, 18 S.W.2d 316, 319 (1929) ("[I]f the makers of the Constitution had intended to qualify the word `office' [in Ky. Const. § 161] they would have inserted the definite article `the' before `office.'") (quotation omitted); Sheriff of Fayette v. Buckner, 11 Ky. (1 Litt.) 126, 128 (1822) (holding that legislative act referencing "the clerk of the court" intended a particular clerk of court referenced elsewhere in the legislation). For similar interpretations by other jurisdictions, see, e.g., State Farm Fire & Cas. Co. v. Old Republic Ins. Co., 466 Mich. 142, 644 N.W.2d 715, 718 (2002); Patricca v. Zoning Bd. of Adjustment, 527 Pa. 267, 590 A.2d 744, 751 (1991); McClanahan v. Woodward Constr. Co., 77 Wyo. 362, 316 P.2d 337, 341-42 (1957); Williams v. McComb, 38 N.C. (3 Ired. Eq.) 450 (1844) ("[G]rammatically speaking, `The,' is a definite article before nouns, which are specific or understood, and is used to limit or determine their extent."). We are directed by the General Assembly to construe our statutes "according to the common and approved usage of language." KRS 446.080(4). Following that directive, we construe "the chemicals or equipment" to mean all of the chemicals or all of the equipment necessary to manufacture methamphetamine.

#### Violation---Machine learning is a tool used by AI---at worst it’s not AI at all, and at best it’s effects T because AI uses ML---effects T is a voter because it allows arbitrary, contrived aff advantages, makes neg prep impossible by spiking out of core links, and mixes burdens.

Wayne Thompson, Hui Li and Alison Bolen 22, Chief Data Scientist at SAS and a globally renowned presenter, teacher, practitioner and innovator in the fields of data mining and machine learning; Senior Staff Scientist at SAS; editor at SAS; xx/xx/2022, “Artificial intelligence, machine learning, deep learning and beyond”, https://www.sas.com/en\_us/insights/articles/big-data/artificial-intelligence-machine-learning-deep-learning-and-beyond.html \\SYang

Machine learning automates analytical model building. It uses methods from neural networks, statistics, operations research and physics to find hidden insights in data without being explicitly programmed where to look or what to conclude.

A neural network is a kind of machine learning inspired by the workings of the human brain. It’s a computing system made up of interconnected units (like neurons) that processes information by responding to external inputs, relaying information between each unit. The process requires multiple passes at the data to find connections and derive meaning from undefined data.

Deep learning uses huge neural networks with many layers of processing units, taking advantage of advances in computing power and improved training techniques to learn complex patterns in large amounts of data. Common applications include image and speech recognition.

Computer vision relies on pattern recognition and deep learning to recognize what’s in a picture or video. When machines can process, analyze and understand images, they can capture images or videos in real time and interpret their surroundings.

Natural language processing is the ability of computers to analyze, understand and generate human language, including speech. The next stage of NLP is natural language interaction, which allows humans to communicate with computers using normal, everyday language to perform tasks.

While machine learning is based on the idea that machines should be able to learn and adapt through experience, AI refers to a broader idea where machines can execute tasks "smartly."

Artificial Intelligence applies machine learning, deep learning and other techniques to solve actual problems.

#### That’s a voter---

#### A---Limits---allowing anything tangentially related to AI blows the lid off of topical affirmatives and leads to practically every piece of military technology being considered a topic area---that’s uniquely bad on a bidirectional topic with three areas.

#### B---Ground---any other interpretation decimates core neg ground by spiking out of AI links and AI bad with “we do something that AI needs but don’t develop the final product”---that’s especially bad when there’s literally no disads and NATO bad is terminally non-unique.

#### C---Topic Education---any other interpretation loses the brightline for the definition of AI and causes a race to the bottom for the most obscure and irrelevant types of technology---that obfuscates education about true EDTs.

#### They’re also extra-T because submarines are more than just AI---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

### 2NC---AI---All of it.---Violation

#### Their authors are straight-up wrong and paid off---at worst, if they’re right, then search, reasoning, planning, language processing, and more count as AI---that’s a huge limits DA.

Alfonso Reyes 20, CTO at Oil Gains Analytics LLC, December 17, 2020 “Why Machine Learning is not Artificial Intelligence?” https://oilgains.medium.com/why-machine-learning-is-not-artificial-intelligence-61b174a3c9a2 \\SYang

It is simple: because ML is only a contributing branch of AI. If we follow Norvig and Russell book -and other authors-, saying that machine learning is equivalent to artificial intelligence is grossly misleading. ML is a contributing discipline of AI, just like search, reasoning, planning, decision making, natural language processing, vision, and robotics.

For instance, ML by itself cannot be intelligent because lacks reasoning, planning, logic, and doesn’t interact with the environment. ML detects patterns and performs predictions based on statistical analysis of data using math based algorithms. These algorithms are not intelligent per se.

Intelligence is much more than that.

Stating that ML is part of AI dramatically lowers the bar of what John McCarthy meant by AI. Chapter two of the AIAMA (Artificial Intelligence: A Modern Approach) book -which counts five editions- contains examples and schematics of what an AI agent is. In essence, an AI agent perceives its environment by means of sensors, and acts upon the environment through actuators; in between these two, there is logic, reasoning, decision making that makes the agent act autonomously, correcting itself with no human intervention.

The figure is my crude attempt of explaining what the AI contributors are (brown).

The view of AI by Peter Norvig and Stuart Russell (2010)

<<<FIGURE OMITTED>>>

Background

Our first instinct would bring us to say Machine Learning is a subset of Artificial intelligence. Then, starts getting fuzzy and nebulous when we find papers, articles, posts claiming to be on Artificial intelligence. You start reading them and turns out they are about Machine Learning or Data Science. At this point we just don’t know, if the author(s) made the mistake by ignorance (didn’t research or read enough literature), or purposely tried to deceive readers. Commercialism also plays a huge part in all this. Although, Machine Learning has had -still has- tremendous achievements to show, marketing and PR departments prefer to call it Artificial intelligence.

Books on artificial intelligence DO NOT do that. They are written by scientists -generally- with strong ethical codes.

So, today’s Artificial intelligence, Machine Learning, and Data Science atmosphere is charged with false stories, inflated achievements. That’s bad for all of us. Because in the end what we receive is pseudo-science.

Science is hard — it’s supposed to be. Artificial intelligence, at the top of the food chain, was one of the ultimate frontiers. I’m sure John McCarthy would not agree to qualify a linear regression, a neural network, or a bare robot, as being Artificial intelligence. Of course, they could be AI with the right combination of AI components. Machine Learning is only one of them.

## 1NC---Semi-Autonomous

#### Interpretation: “Artificial Intelligence” is distinct from semiautonomous weapons

CRS Report, 12-01-2020, "Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems," Congressional Research Service, https://sgp.fas.org/crs/natsec/IF11150.pdf//jc

Definitions. There is no agreed definition of lethal autonomous weapon systems that is used in international fora. However, Department of Defense Directive (DODD) 3000.09 (the directive), which establishes U.S. policy on autonomy in weapons systems, provides definitions for different categories of autonomous weapon systems for the purposes of the U.S. military. These definitions are principally grounded in the role of the human operator with regard to target selection and engagement decisions, rather than in the technological sophistication of the weapon system. DODD 3000.09 defines LAWS as “weapon system[s] that, once activated, can select and engage targets without further intervention by a human operator.” This concept of autonomy is also known as “human out of the loop” or “full autonomy.” The directive contrasts LAWS with humansupervised, or “human on the loop,” autonomous weapon systems, in which operators have the ability to monitor and halt a weapon’s target engagement. Another category is semi-autonomous, or “human in the loop,” weapon systems that “only engage individual targets or specific target groups that have been selected by a human operator.” Semiautonomous weapons include so-called “fire and forget” weapons, such as certain types of guided missiles, that deliver effects to human-identified targets using autonomous functions. The directive does not cover “autonomous or semiautonomous cyberspace systems for cyberspace operations; unarmed, unmanned platforms; unguided munitions; munitions manually guided by the operator (e.g., laser- or wire-guided munitions); mines; [and] unexploded explosive ordnance,” nor subject them to its guidelines.

#### Violation: PGMs are semi-autonomous

Heather Roff, 1-16-2015, "Autonomous or 'Semi' Autonomous Weapons? A Distinction Without Difference," HuffPost, https://www.huffpost.com/entry/autonomous-or-semi-autono\_b\_6487268//jc

We have roughly four functions on a weapons system: trigger, targeting, navigation, and mobility. We might think of these functions like a menu that we can order from. Semi-autonomous weapons have at least one, if not three, of these functions. For instance, we might say that the Samsung SGR-1 has an "autonomous" targeting function (through heat and motion detectors), but is incapable of navigation, mobility or triggering, as it is a sentry-bot mounted on a defensive perimeter. Likewise, we would say that precision guided munitions are also semi-autonomous, for they have autonomous mobility, triggering, and in some cases navigation, while the targeting is done through a preselected set of coordinates or through "painting" a target through laser guidance.

#### That’s a voter:

#### A --- Limits --- any other interp explodes the topic as there are infinitely more semiautonomous systems as opposed to AI

#### B --- Ground --- core negative ground are to NATO artificial intelligence, CPs about AI, and so on --- that’s key in a topic with no neg generics.

#### C --- Topic Education --- allowing non-AI affs causes a race to the bottom find the most arbitrary weapon system and skews debate away from education about Artificial Intelligence.

## 1NC---Autonomous

#### Interpretation: Artificial Intelligence is different from autonomous robotics

Mike Ball, 11-12-2020, “Artificial Intelligence vs Autonomy for Mobile Robotics,” Unmanned Systems Technology, <https://www.unmannedsystemstechnology.com/2020/11/artificial-intelligence-vs-autonomy-for-mobile-robotics///jc>

Autonomy and artificial intelligence (AI) are often used interchangeably in conversation and in the media. These two concepts, however, are quite different in practice. Understanding the difference between AI and autonomy will help your company to make the most practical choices for greater productivity now and in the future. At Inertial Sense, we specialize in integrating AI, machine learning and autonomous systems to create the right solutions for our clients’ autonomous robotic systems needs. Artificial Intelligence vs. Autonomy Artificial intelligence applications and autonomy are both valuable tools in the industrial environment. These technologies can be used independently or can work together to achieve the desired results. Here’s an easy way to breakdown the differences between the two: autonomous robotics = task completion and AI = problem-solving. Autonomous robotics systems are designed for use in predictable environments to complete tasks within a specific, usually pre-planned, environment. Sensors are of critical importance in providing robots with detailed and accurate information about their location within the domain. Autonomous robotics systems rely on these sensors to navigate their environments and to perform their tasks quickly and effectively. Autonomous devices and systems can be powered by conventional software or by AI systems that allow them to learn and adapt as they operate. Artificial intelligence is defined by Yale University as “building systems that can solve complex tasks in ways that would traditionally need human intelligence.” This typically involves machine learning technologies and the use of highly advanced sensors to collect information about the environment and to allow the system to react appropriately to external stimuli.

#### Violation: The aff is about autonomous weapons

#### That’s a voter:

#### A --- Limits --- any other interp explodes the topic as there are infinitely more autonomous systems as opposed to AI

#### B --- Ground --- core negative ground are to NATO artificial intelligence, CPs about AI, and so on --- that’s key in a topic with no neg generics.

#### C --- Topic Education --- allowing non-AI affs causes a race to the bottom find the most arbitrary weapon system and skews debate away from education about Artificial Intelligence.

## 2NC---Definitions

### 2NC---Generic

#### Semi-autonomous weapons are excluded from international community debates about AI

Ingvild Bode, 2-16-2021, "Artificial Intelligence, Weapons Systems and Human Control," E-International Relations, https://www.e-ir.info/2021/02/16/artificial-intelligence-weapons-systems-and-human-control///jc

However, questions about the nature and quality of human control raised by these existing systems are not part of the ongoing discussion on AWS among states at the UN-CCW. In fact, states using automated weapons continue to actively exclude them from the debate by referring to them as ‘semi-autonomous’ or so-called ‘legacy systems.’ This omission prevents the international community from taking a closer look at whether practices of using these systems are fundamentally appropriate.

### 2NC---PGMs

#### Not only are PGMs not considered AI, BUT AI is also an active problem to PGM resource allocation – prefer our sources from actual Congressional Research

CRS Report, 06-11-2021, "Precision-Guided Munitions: Background and Issues for Congress," Congressional Research Service, https://sgp.fas.org/crs/weapons/R45996.pdf//jc

Emerging factors that may affect PGM programs. Another potential issue for Congress is how DOD’s programs for developing and procuring PGMs might be affected by emerging factors such as

* the U.S. withdrawal from the Intermediate Nuclear Force (INF) treaty;96
* new U.S. military operational concepts for countering Chinese A2/AD forces in the Indo-Pacific region, such as the Army’s new Multi-Domain Operations (MDO) operational concept and the Marine Corps’ new Expeditionary Advanced Base Operations (EABO) concept, both of which possibly feature the potential use of such weapons from island locations in the Pacific as a way of countering China’s A2/AD forces; and
* emerging technologies such as hypersonics and artificial intelligence (AI).

## 2AC

### W/M

#### W/M: Semi-Autonomous systems were discussed in the Twenty-Ninth AAAI Conference on Artificial Intelligence

Shlomo Zilberstein, 03-04-2019, "Twenty-Ninth AAAI Conference on Artificial Intelligence," AAAI Publications, https://www.aaai.org/ocs/index.php/AAAI/AAAI15/paper/viewPaper/9920//jc

The vision of populating the world with autonomous systems that reduce human labor and improve safety is gradually becoming a reality. Autonomous systems have changed the way space exploration is conducted and are beginning to transform everyday life with a range of household products. In many areas, however, there are considerable barriers to the deployment of fully autonomous systems. We refer to systems that require some degree of human intervention in order to complete a task as semi-autonomous systems. We examine the broad rationale for semi-autonomy and define basic properties of such systems. Accounting for the human in the loop presents a considerable challenge for current planning techniques. We examine various design choices in the development of semi-autonomous systems and their implications on planning and execution. Finally, we discuss fruitful research directions for advancing the science of semi-autonomy.

### C/I – Semi-Autonomous systems

#### C/I: All AI is semiautonomous

Travis N Rieder et al, 06-xx-2020, "Artificial Intelligence in Service of Human Needs: Pragmatic First Steps Toward an Ethics for Semi-Autonomous Agents," PubMed, https://pubmed.ncbi.nlm.nih.gov/32228385///jc

The ethics of robots and artificial intelligence (AI) typically centers on "giving ethics" to as-yet imaginary AI with human-levels of autonomy in order to protect us from their potentially destructive power. It is often assumed that to do that, we should program AI with the true moral theory (whatever that might be), much as we teach morality to our children. This paper argues that the focus on AI with human-level autonomy is misguided. The robots and AI that we have now and in the near future are "semi-autonomous" in that their ability to make choices and to act is limited across a number of dimensions. Further, it may be morally problematic to create AI with human-level autonomy, even if it becomes possible. As such, any useful approach to AI ethics should begin with a theory of giving ethics to semi-autonomous agents (SAAs). In this paper, we work toward such a theory by evaluating our obligations to and for "natural" SAAs, including nonhuman animals and humans with developing and diminished capacities. Drawing on research in neuroscience, bioethics, and philosophy, we identify the ways in which AI semi-autonomy differs from semi-autonomy in humans and nonhuman animals. We conclude on the basis of these comparisons that when giving ethics to SAAs, we should focus on principles and restrictions that protect human interests, but that we can only permissibly maintain this approach so long as we do not aim at developing technology with human-level autonomy.

### W/M – PGM specific

#### PGMs are now considered AI

Jon Harper, 10-7-2019, “JUST IN: Pentagon Contemplating Role of AI in Missile Defensse,” National Defense, https://www.nationaldefensemagazine.org/articles/2019/10/7/pentagon-contemplating-role-of-ai-in-missile-defense//jc

Artificial intelligence is expected to play a critical role in helping the United States counter emerging missile threats, according to experts. Traditional types of ballistic missiles are being superseded by more advanced systems. They include more maneuverable and precision-guided ballistic missiles, low-flying cruise missiles and hypersonic weapons that can travel at speeds of Mach 5 or faster, Missile Defense Agency Director Vice Adm. Jon Hill noted Oct. 7 during remarks at the Center for Strategic and International Studies in Washington, D.C. “The unpredictability … is very challenging,” he said. “It challenges your sensor architecture, it challenges your fire control and it challenges the methods by which you engage. So I do believe that we are at an inflection point in how we're going to defend not only the homeland, but our forward-deployed forces and our friends and allies. And we have to think differently.” AI can help the Defense Department as it tries to tackle the problem, he said.

#### Prefer it as it is within the context of the topic

Abhijit Singh, 09-21-2016, "Is China Really Building Missiles With Artificial Intelligence?," No Publication, <https://thediplomat.com/2016/09/is-china-really-building-missiles-with-artificial-intelligence///jc>

With rising security challenges in the global commons, there is growing interest in the subject of “intelligent” weapons systems. This is especially so in the maritime realm, where recent studies have shown that precision-guided weaponry and networked systems are likely to play an increasingly important role. Even while accepting autonomous systems as the future of maritime warfare, however, many find the subject of “intelligent weapon systems” to be deeply contentious. A good point of departure for the discussion on autonomous combat systems is a recent report in the Chinese media about the development of a family of cruise missiles with artificial intelligence (AI) capabilities. In August this year, a Chinese daily reported that China’s aerospace industry was developing tactical missiles with inbuilt intelligence that would help seek out targets in combat. The “plug and play” approach, a Chinese aerospace executive pointed out, could potentially enable China’s military commanders to launch missiles tailor made for specific combat conditions. Oddly enough, no clarifications were offered for what “tailor made cruise missiles with high levels of artificial intelligence and automation” really meant. Apart from reiterating China’s global leadership status in the field of artificial intelligence, the Chinese source did not provide any insight into the specific nature of autonomous capability being developed. The issue for many naval commanders is the dichotomy between the theoretical definition of Artificial Intelligence and its popular interpretation. Technically, AI is any onboard intelligence that allows machines in combat to execute regular tasks, allowing humans more time to focus on demanding and complex missions. Modern-day combat requires war-fighters to operate with the active assistance from sensors and systems. In theory, AI provides the technology to augment human analysis and decision-making by capturing knowledge that can be re-applied in critical situations. It purports to change the human role from “in-the-loop” controller to “on-the-loop” thinker who can focus on a more reflective assessment of problems and strategies, guiding rather than being buried in execution detail. [AD OMITTED] In practice, however, Artificial Intelligence is a term used for a combat system that has the ability to take targeting decisions. This is more in the nature of “who to target,” as opposed to “how to target,” which is anyway a task that guided missiles have been performing with some precision. It’s worth emphasizing that maritime forces remain skeptical of autonomous weapon systems with independent targeting capability. In the nautical realm, the launch of a missile on an enemy platform is an act of war. The decision to execute a missile launch is the exclusive preserve of the command team (led by the ship’s captain), which must independently assess the threat and act in pursuit of war objectives. [AD OMITTED] Despite several advancements allowing for a more precise targeting of platforms, the logic of maritime operations hasn’t fundamentally changed. As a result, naval missiles haven’t been invested with any serious intelligence to make command decisions to target enemy units. While their ability to strike targets has been radically enhanced — through the use of superior onboard gyros, computing systems, and track radars — the basic mode of operation of cruise missiles remains the same. To be sure, Artificial Intelligence is considered indispensable in the development of new-age naval weapons, in particular hypersonic missiles. After China’s recent high-speed (over Mach 10), “extreme maneuvers” hypersonic tests, it is amply clear that future combat missions will require a human-machine interface on an unprecedented scale; which is why four other Asian states — Japan, India, South Korea, and Taiwan — have been developing supersonic and hypersonic systems. Each one of them has expressed an aspiration for a sophisticated maritime force, with long range sensors, armor protection, precision weapons, and networking technologies. Yet none has been developing naval missile systems with artificial intelligence.

# Biotechnology

# T: Cognitive Biotech

### Notes

#### Aff cards from the original file are really, really, bad---three out of four literally fail the control-F test for biotech, while the only card that mentions biotech doesn’t mention the aff at all. With that being said, I found some decent aff cards, and the only neg cards I found are even worse than the original aff cards put out.

## Indicts

### AT: Jain

#### Jain works at a biotech company and isn’t an academic researcher---this takes out any claim to a precision internal link they have and means you should heavily err neg---they are most definitely paid off to categorize as many things as biotech as possible---Jain PharmaBiotech probably does BCI technologies. Also, Switzerland isn’t even in NATO which decimates their contextual precision. Independently, this card doesn’t mention brain-computer interfaces a single time---all it says is that neurobiotech is biotech and neurology together---that’s meaningless because it doesn’t provide a single example.

### AT: Schwab

#### Huge precision DA---Schwab is the founder of the World Economic Forum---its certainly not contextually precise in any of the core topic areas of NATO, or emerging tech or legally precise. Independently, this card is a borderline miscut---it just says neurobiology is making strides in human biology---LITERALLY doesn’t even say the word biotechnology in the card a single time.

### AT: Jarchum

#### OOPS---fails the control-F test for biotech---that’s embarrassing---uses the word neurotechnology---most power-tagged card of all time---literally says nothing about biotechnology, just that neurotechnology exists and BCIs are one kind of it.

### AT: Haggenmiller

#### OOPS---fails the control-F test for biotech---that’s embarrassing. Independently I don’t know what they think this card gets them---it just describes the aff without even mentioning anything close to a definition of biotechnology---we already know the aff exists---thanks for wasting twenty seconds.

## T-Interps

### 1NC---Biotech---No BCIs

#### Interpretation---BCIs aren’t biotechnology.

Isabella Grandic 19, feminist activist and organizer, January 16, 2019, “Human Intelligence is Worth Imitating”, https://tinyurl.com/383axkj5 \\SYang

But we’ve entered a remarkable time in history. We have technologies like VR AR, brain-computer interfaces, biotechnology and quantum computing set to solve some of the world’s biggest issues. Perhaps the craziest, most innovative technology, modelled based on the neural networks of the human brain, is artificial intelligence. AI is going (notice I didn’t say “might” or “has the potential to”) disrupt every single industry.

#### Violation---the aff is BCIs.

#### That’s a voter---

#### A---Limits---allowing any non-biotech technologies blows the lid off of topical affirmatives as anything becomes topical ---that’s uniquely bad on a bidirectional topic with three topic areas.

#### B--Topic Education---any other interpretation causes a race to the bottom to find the most irrelevant technology related to biology that obfuscates learning.

### 2NC---Biotech---No BCIs

#### The army votes neg.

Lisbeth Perez 21, MeriTalk and MeriTalk State and Local Government Staff Reporter covering the intersection of government and technology, September 9, 2021, “Emerging Tech is Critical to Supporting the Future Soldier, ARL Officials Say”, <https://tinyurl.com/3bpr4mfs> \\SYang

Tomorrow’s troops will draw on biotechnology and brain-computer interfaces, augmented reality headsets and adaptive camouflage, and other tools barely dreamt of by today’s soldiers. The U.S. Army Research Laboratory (ARL) continues to look broadly across the swath of technologies critical to supporting the Army today and in the future, according to ARL officials on September 8 at a Defense One webinar.

#### NRC votes neg.

National Research Council 12, operating arm of the United States National Academies of Sciences, Engineering, and Medicine, “Human Performance Modification”, <https://nap.nationalacademies.org/catalog/13480/human-performance-modification-review-of-worldwide-research-with-a-view> \\SYang

The National Research Council will form an ad hoc committee to focus on developmental capabilities in the general area of human performance modification. The committee will perform an initial review of the literature, select the most promising areas, and identify the lead players (state or non-state) in those areas. Areas of investigation include biotechnology, brain-computer interfaces, cognitive enhancement, electronics, nanotechnology, and neural implants. This does not preclude additional areas uncovered during the course of the study. The committee will exclude conventional pharmaceuticals and exoskeletons per the sponsor’s direction.

### 2AC---C/I---Biotech = BCIs

#### C/I---Biotechnology includes brain-computer interfaces.

Hannah Gallagher 21, Corporate Associate at Winston & Strawn LLP and JD recipient from Washington University, xx/xx/2021, “Regulating the Sixth Sense: The Growing Need for Forward-Looking Data Privacy and Device Security Policy as Illustrated by Brain-Computer Interfaces”, <https://openscholarship.wustl.edu/law_journal_law_policy/vol66/iss1/12/>, published in Washington University Journal of Law and Policy \\SYang

BCI is an emerging biotechnology that could allow elective brain augmentation. This is an extreme but logical extension of the existing trend towards invasive consumer technology products. From stationary desktop computers to portable laptops to smart phones which have essentially become fifth limbs for many of today’s consumers121 to the Internet of Things (IoT) devices that are becoming increasingly prevalent in homes (e.g., Alexa, Nest, smart refrigerators, doorbell cameras, etc.), connected devices—and the data that they collect—are becoming integrated into more and more aspects of consumers’ daily lives.

#### Prefer it---

#### A---Precision---Gallagher is a legal expert writing on the legal implications and relevance of BCIs---that’s the most legally precise.

#### B---Topic Education---BCIs is one of only two biotech affs that’s been put out---framer’s intent was that we learned about biotech---that means every aff with a solvency advocate is extremely valuable.

#### C---Aff Ground---invert your conceptions of the importance of aff/neg ground---biotech is supposed to be a third of the topic but we’re a month into camp and no one has read a biotech aff---it’s try or die to save the topic.

### 1AR---C/I---Biotech = BCIs

#### More ev.

Allison Henry 22, member of the Vanderbilt Institute for Global Health at Vanderbilt University Medical Center, March 22, “Brain Computer Interfaces: The Future of Healthcare is Now”, <http://vanderbiltvanguard.com/2022/03/brain-computer-interfaces-the-future-of-healthcare-is-now/> \\SYang

At the intersection between neuroscience, medicine, and technology lies arguably one of the most groundbreaking developments of this century: brain computer interfaces, or BCIs. BCIs are systems that bridge the nervous system and modern-day biotechnology to significantly improve the quality of life for users. From cochlear implants and prosthetic limbs to video game systems that are more accessible to those with neurological disabilities, BCIs have been designed for a variety of purposes, both medical and recreational, and consequently are of great interest in biomedical and technological fields of research.

# Additional Violations

### 1NC---Biotech---Industries

#### Interpretation---Biotechnology has to involve industries.

Lilian Nyanjui ND, researcher specializing in microalgae, heavy metals and related pollution, phytoremediation, and water resources engineering, “What is Biotechnology”, https://www.academia.edu/10359485/What\_is\_Biotechnology \\SYang

The concept of 'biotech' or 'biotechnology' encompasses a wide range of procedures (and history) for modifying living organisms according to human purposes going back to domestication of animals, cultivation of plants, and "improvements" to these through breeding programs that employ artificial selection and hybridization. Modern usage also includes genetic engineering as well as cell and tissue culture technologies. Biotechnology is defined by the American Chemical Society as the application of biological organisms, systems, or processes by various industries to learning about the science of life and the improvement of the value of materials and organisms such as pharmaceuticals, crops, and livestock. In other words, biotechnology can be defined as the mere application of technical advances in life science to develop commercial products. Biotechnology also writes on the pure biological sciences (genetics, microbiology, animal cell culture, molecular biology, biochemistry, embryology, cell biology). And in many instances it is also dependent on knowledge and methods from outside the sphere of biology including:

#### The USfg is the three branches.

White House 18, official website of the White House, carbon dated September 17, 2018, “Our Government”, https://www.whitehouse.gov/about-the-white-house/our-government/ \\SYang

The Federal Government is composed of three distinct branches: legislative, executive, and judicial, whose powers are vested by the U.S. Constitution in the Congress, the President, and the Federal courts, respectively.

#### Violation---if they’re not extra-T on T-USfg then they don’t meet.

#### That’s a voter---

#### A---Limits---allowing other methods blows the lid off of topical affirmatives as aff’s that don’t use industries become topical ---that’s uniquely bad on a bidirectional topic with three topic areas.

#### B---Ground---any other interpretation allows the 2AC to spike out of industry-based offense like the econ DA and counterplans that PIC out or solely use the government---this topic has no neg generics which means our ground offense outweighs.

#### C---Topic Education---any other interpretation causes a race to the bottom to find the most irrelevant solvency advocates that obfuscates learning.

#### If they meet T-biotech then they’re Extra-T---that’s a voter for limits, clash, and fairness---any other model justifies infinite extra-topical planks.

### 1NC---Biotech---Production

#### Interpretation---biotech means the use of living organisms and biological processes in industrial production.

* Caselist = anything that cooperates with NATO on manufacturing using biological processes. A lot of food related things, maybe new tech like spider web armor, not sure what else.
* Could also be a counter-interp since as of now I’m not really sure what aff this excludes.

Elena Myshak 18, linguistic researcher specializing in the term biotechnology, xx/xx/2018, “DEFINITION OF THE TERM “BIOTECHNOLOGY””, https://www.ceeol.com/search/article-detail?id=884606, published by Editura Pro Universitaria, 2018 issue 4, pg. 142-149 \\SYang

Until 1971, this term was used mainly in the food industry and agriculture. At the moment, there are many interpretations of the concept, but in general they all boil down to one thing: in the traditional understanding of biotechnology, this is an interdisciplinary field that has arisen at the junction of biological, chemical and technical sciences; it is the use of living organisms and biological processes in industrial production. Thus, biotechnology is an integration of natural and technical sciences that studies the possibilities of using living organisms and biological processes for the production and processing of various valuable substances and products. Today, biotechnology is among the top priorities of scientific and technological progress, being a vivid example of “high technology”. As noted above, there is no consensus in the literature regarding the definition of biotechnology as a science. M. Bekker (1979) in his book “Introduction to Biotechnology” defines biotechnology as a section of the science of obtaining biosynthesis products. A. Sasson defined biotechnology as a technological process implemented using biological systems – living organisms and living cell components. By definition, the European Biotechnology Federation (1980), biotechnology is the combined use of biochemistry, microbiology and chemical technology for the technological (industrial) use of the beneficial properties of microorganisms and tissue cultures. In other words, biotechnology is a human-directed complex of methods for obtaining society-friendly target products using biological agents of microorganisms, viruses, animal and plant cells, as well as using extracellular substances and cell components. These definitions are mostly correct, but the range of sciences, the practical results of which are embodied in biotechnology is much broader. In 1983, at the congress of the socialist countries on biotechnology in Bratislava, the following definition was made: “biotechnology is a science that develops the scientific basis for large-scale implementation of the processes of obtaining various substances and means of environmental protection using biocatalysts”. At the moment, there is no consensus in understanding biotechnology. It is interpreted as a set of methods and techniques for obtaining products and phenomena that are useful to humans with the help of biological agents; special social activities of human transformation of the world and himself through the use of biological processes and agents; the science “about the methods of obtaining target products using biosynthesis, controlled by environmental parameters or genetic engineering manipulations, or a combination of these effects”.

#### Violation---[CONTEXTUALIZE]

#### That’s a voter---

#### A---Limits---allowing other methods blows the lid off of topical affirmatives as any aff even remotely related to anything biological becomes topical (news flash---that’s basically everything related to people) ---that’s uniquely bad on a bidirectional topic with three topic areas.

#### B---Ground---any other interpretation allows the 2AC to spike out of manufacturing-based offense like the econ DA and counterplans that PIC out, as well as Ks of extracting value from biological processes---this topic has no neg generics which means our ground offense outweighs.

#### C---Topic Education---any other interpretation causes a race to the bottom to find the most irrelevant solvency advocates that mention the word biology which obfuscates learning about true biotech which was the intention of the topic paper.

#### At best they’re extra-T because they do things other than manufacturing---that’s a voter for limits, clash, and fairness---any other model justifies infinite extra-topical planks.

### Interp---Biotech---Production

#### MW agrees.

Merriam Webster English Dictionary 22, American company that publishes reference books and is especially known for its dictionaries, “biotechnology”, https://www.merriam-webster.com/dictionary/biotechnology \\SYang

Definition of biotechnology

1: the manipulation (as through genetic engineering) of living organisms or their components to produce useful usually commercial products (such as pest resistant crops, new bacterial strains, or novel pharmaceuticals)

#### Case list---developing or reducing the development of GMOs, bioweapons, and pharmaceuticals among any other products that involve living components.

#### More ev.

Organisation for Economic Co-operation and Development 1, intergovernmental organization with 38 member countries, founded in 1961 to stimulate economic progress and world trade, November 2, 2001, “Biotechnology, single definition”, https://stats.oecd.org/glossary/detail.asp?ID=219#:~:text=Biotechnology%20is%20defined%20as%20the,of%20knowledge%2C%20goods%20and%20services, official OECD glossary \\SYang

Biotechnology is defined as the application of science and technology to living organisms as well as parts, products and models thereof, to alter living or non-living materials for the production of knowledge, goods and services.

#### More ev and more affs for the caselist.

John E. Smith 9, Emeritus Professor of Applied Microbiology in the Institute of Pharmacy and Biomedical Sciences, University of Strathclyde, xx/xx/2009, “Biotechnology”, https://www.cambridge.org/core/books/biotechnology/20C1C1DA5F97D24C7159564CCD95225E, published by Cambridge University Press \\SYang

Biotechnology is in essence the deciphering and use of biological knowledge. It is highly multidisciplinary since it has its foundations in many disciplines including biology, microbiology, biochemistry, molecular biology, genetics, chemistry and chemical and process engineering. It may also be viewed as a series of enabling technologies that involve the practical application of organisms (especially microorganisms) or their cellular components to manufacturing and service industries and environmental management. Historically, biotechnology was an artisanal skill rather than a science, exemplified in the manufacture of wines, beers, cheeses, etc. where the techniques of manufacture were well worked out and reproducible, while the biological mechanisms were not understood. As the scientific basis of these biotechnology processes has developed this has led to more efficient manufacturing of the traditional processes that still represent the major financial returns of biotechnology, i.e. bread, beers, wines, cheeses, etc. Modern biotechnological processes have generated a wide range of new and novel products including antibiotics, vaccines and monoclonal antibodies, the production of which has been optimised by improved fermentation practices. Biotechnology has been further revolutionised by a range of new molecular biology innovations, allowing unprecedented molecular changes to be made to living organisms. The increasing understanding of genomics and proteomics has led to the creation of a vast range of transgenic microorganisms, agricultural (genetically modified) crops and animals, and major new recombinant protein drugs, and has revolutionised activities in the traditional food and drinks industries. In the environment, biotechnology innovations are creating major advances in water and land management and also remediating the pollution generated by over-industrialisation

### 2NC---Biotech---AT: Precision

#### Prefer debatability---there’s no expert consensus on the definition of the term---that means there is no most precise definition and you default to evaluating which model is better for debate.

* This card includes the section cut for the 1NC/2AC biotech = production card

Elena Myshak 18, linguistic researcher specializing in the term biotechnology, xx/xx/2018, “DEFINITION OF THE TERM “BIOTECHNOLOGY””, https://www.ceeol.com/search/article-detail?id=884606, published by Editura Pro Universitaria, 2018 issue 4, pg. 142-149 \\SYang

The concept of “biotechnology”

The formation of the terminological system of the innovation-technical discourse is directly related to the term biotechnology, which comes from the Greek words bios — life, techne — art, logos — word, teaching, science. Today, this concept underlies a significant part of innovative research and it is present in the overwhelming majority of scientific papers in this disciplinary segment. The concept of “biotechnology” appeared in our language relatively recently. The term “biotechnology” proposed in 1917 by K. Ereki meant “types of work in which certain products are produced from raw materials using living organisms”. Despite the capacious reflection of the essence of the technology, such an understanding did not stick, and therefore the term was used in two ways for a long time: some used it in connection with the fermentation process, others meant the person and his practical activity in order to optimize tools, conditions and the labor process. Until 1971, this term was used mainly in the food industry and agriculture. At the moment, there are many interpretations of the concept, but in general they all boil down to one thing: in the traditional understanding of biotechnology, this is an interdisciplinary field that has arisen at the junction of biological, chemical and technical sciences; it is the use of living organisms and biological processes in industrial production. Thus, biotechnology is an integration of natural and technical sciences that studies the possibilities of using living organisms and biological processes for the production and processing of various valuable substances and products. Today, biotechnology is among the top priorities of scientific and technological progress, being a vivid example of “high technology”. As noted above, there is no consensus in the literature regarding the definition of biotechnology as a science. M. Bekker (1979) in his book “Introduction to Biotechnology” defines biotechnology as a section of the science of obtaining biosynthesis products. A. Sasson defined biotechnology as a technological process implemented using biological systems – living organisms and living cell components. By definition, the European Biotechnology Federation (1980), biotechnology is the combined use of biochemistry, microbiology and chemical technology for the technological (industrial) use of the beneficial properties of microorganisms and tissue cultures. In other words, biotechnology is a humandirected complex of methods for obtaining society-friendly target products using biological agents of microorganisms, viruses, animal and plant cells, as well as using extracellular substances and cell components. These definitions are mostly correct, but the range of sciences, the practical results of which are embodied in biotechnology is much broader. In 1983, at the congress of the socialist countries on biotechnology in Bratislava, the following definition was made: “biotechnology is a science that develops the scientific basis for large-scale implementation of the processes of obtaining various substances and means of environmental protection using biocatalysts”. At the moment, there is no consensus in understanding biotechnology. It is interpreted as a set of methods and techniques for obtaining products and phenomena that are useful to humans with the help of biological agents; special social activities of human transformation of the world and himself through the use of biological processes and agents; the science “about the methods of obtaining target products using biosynthesis, controlled by environmental parameters or genetic engineering manipulations, or a combination of these effects”. Based on the analysis of existing definitions, it can be concluded that the definition of biotechnology given in the late 1970s is basically correct. As we can see from the presented definitions, the term “biotechnology” has two meanings: on the one hand, it is the science of using biotechnological processes in production, on the other, it is a complex scientific and technical direction that studies these processes. Thus, in the mid-70s of the twentieth century, the term “biotechnology” appeared, which immediately filled in the pages of academic and popular publications. It should be noted that biotechnology science is served exclusively by English terminology, although the development of scientific research in the field of biotechnology is not a priority for the Anglo-American community. The analysis of English biotechnology terminology causes a growing interest of scientists, since it is a young term system, which is at the stage of formation due to the high level of innovation and dynamism of biotechnology. Therefore, the study of the general tendencies of the definition of the term “biotechnology” in the English and Russian languages and its individual features is interesting, in our opinion, from both theoretical and practical points of view. As noted above, the term unit biotechnology (biotechnology), despite belonging to the basic terms of innovative technical discourse, does not have an established definition in either English or Russian. Despite the fact that one of the basic requirements for the term is its uniqueness, examples of definitions of the term unit biotechnology (biotechnology), selected from dictionaries and glossaries, can cast doubt on this condition for the existence of special lexical units. Consider the following definitions: 1) Biotechnology – the use of a living organism to solve an engineering problem or perform an industrial task. 2) Biotechnology is the use of biological processes, organisms, or systems to manufacture products intended to improve the quality of human life. 3) Biotechnology – the manipulation (through genetic engineering) of living organisms or their components to produce useful usually commercial products (such as pest resistant crops, new bacterial strains, or novel pharmaceuticals); 4) Biotechnology – techniques that use living organisms or parts of organisms to produce a variety of products (from medicines to industrial enzymes) to improve plants or animals or to develop microorganisms to remove toxics from bodies of water, or act as pesticides; 5) Biotechnology – the use of bacteria and plant and animal cells for industrial or scientific purposes, for example to make drugs or chemicals; 6) Biotechnology – techniques that use living organisms or parts of organisms to produce a variety of products (from medicines to industrial enzymes) to improve plants or animals or to develop microorganisms to remove toxics from bodies of water, or act as pesticides; 7) Biotechnology is technology that utilizes biological systems, living organisms or parts of this to develop or create different products; 8) Biotechnology: the fusion of biology and technology, the application of biological techniques to product research and development. 9) Biotechnology, the use of biology to solve problems and make useful products. The most prominent area of biotechnology is the production of therapeutic proteins and other drugs through genetic engineering.

Conclusions

As we can see from a small number of examples, the term biotechnology is by no means unambiguous, and the reason lies not only in the difference in the wording and its prevalence, but also in the selection of the relevant features of the concept when creating the definition. In most of the definitions, the definition is based on the use of living organisms or their components for the production of products designed to improve the quality of life of people. Other definitions emphasize that biotechnology is a technology that combines biology and technology that uses biological systems, living organisms or their fragments to develop or create various products. In almost all definitions, the idea of the benefits of biotechnology is expressed, namely: biotechnology is used to obtain useful products for society with the help of biological agents of microorganisms, viruses, animal and plant cells; creating useful products (from drugs to industrial enzymes); to improve plants or animals; to solve engineering and industrial problems, etc. It should be noted that almost all definitions have a different nuclear seme or genus and species trait: science (science); technology; manipulation; techniques; use; area. Such differences in the definition of the key term of the biotechnology sphere confirm the proposition that the definitions of concepts in any science are temporary and, depending on the development of the latter, can be transformed. So, in the presented examples of the definition of one term “biotechnology”, we tried to demonstrate the diversity of definitional variations of the term in its static (vocabulary) manifestation at the initial stage of the formation of terminology, i.e. on the way to the formation of the term system. This fact indicates the dynamic structure of the term, the development of the denotation, the concept and signification. The terminology of biotechnology is not fully formed and needs to be standardized in order to provide the recipient with information about the concept reflected in the definition.

### Interp---Bioscience

#### Biotechnology is distinct from bioscience

Brown ’21 [Annie; 10/25/21; Founder of Lips, Director of Communications for CodePath; "Artificial Intelligence Is Transforming Biotechnology, Especially When It Comes To Innovations In Nitric Oxide," Forbes, <https://www.forbes.com/sites/anniebrown/2021/10/25/artificial-intelligence-is-transforming-biotechnology-especially-when-it-comes-to-innovations-in-nitric-oxide/?sh=5d40b66c7f00> //smarx, AZG]

Biotechnology is not to be confused with the closely related field of biosciences. While biosciences refer to all the sciences that study and understand life, biology, and biological organisms, biotechnology refers to the application of the knowledge of biosciences and other technologies to develop tech and commercial products. Biotechnology is the application of innovation to biosciences in a bid to solve real-world medical problems.

### Interp---Bioengineering

#### Biotechnology and bioengineering are distinct – common understanding is wrong

Brinson ’No Date [Phillip and Nelson; Heads of Biotech Health; "Biotech Vs. Bioengineering: What's The Difference?," BiotechHealth, <https://biotechhealth.com/biotechnology-and-bioengineering/> smarx, AZG]

While you might think that biotechnology and bioengineering are pretty much the same thing, they do have some important differences to know about. This is especially important if you want to start a career in either field because it will help you to choose the best one. What are examples of biotechnology and bioengineering? You can find examples of both of these around you. Just look at a glass of wine – technology used to produce wine was developed by biotechnologists. Similarly, if you need an ultrasound, this is an example of bioengineering. With that in mind, let’s explore both biotechnology and bioengineering in greater detail. We’ll start by looking at some important differences between them. Contents [show] The Main Differences Between Biotech And Bioengineering Biotechnology is focused on life science. Its aim is to create and develop products that can be useful in various industries, such as the food and medical industries. It makes use of biological systems to create useful products. Biotechnology concentrates on living organisms and how they can be applied to medicine, technology, agriculture, and business. Bioengineering, on the other hand, makes use of engineering principles to solve problems that arise in medicine as well as biology. It makes use of engineering methods and scientific concepts to find solutions. Although they are a bit different, the two are definitely connected! Biotechnology makes use of technology when studying and using biological systems. On the other hand, bioengineering relates to designing and transforming the technology in biotechnology. To see how this would work in real life, we can say that biotechnology creates the cells that will develop pharmaceutical drugs. Bioengineering, on the other hand, develops a process that will ensure those drugs can be produced faster. Now that we’ve analyzed the main definitions of both biotechnology and bioengineering, we can explore both of them in greater detail. Let’s start with biotechnology! The Four Main Types Of Biotechnology Biotechnology has four main types. These are: Medical biotechnology, which is focused on using living cells to create new technologies to improve human health. It also makes use of studying DNA to identify genetic disorders and find ways to treat them. Various developments in medical biotechnology include the development of antibiotics and vaccines. Agricultural biotechnology, which involves developing genetically-modified plants to increase crop yield. An example would be GM crops that are pest-resistant or can grow during droughts. This type of biotechnology also involves finding other ways to make crops healthier, such as by boosting their nutritional value. This can help to deal with the world’s hunger problem. Industrial biotechnology, which makes use of technology for industrial purposes to improve manufacturing processes. It basically makes use of microorganisms and enzymes to create products to make the processes smoother. Environmental biotechnology, which uses technology to improve the environment. This can take the form of finding innovative ways for waste treatment or the prevention of air, land, and water contaminants. THERE ARE MANY OTHER TYPES OF BIOTECHNOLOGY! The four previous types of biotech aren’t the only ones – with biotechnology growing and influencing many different fields and sectors, there are always new ones hitting the scene. Examples of other types of biotechnology include biotechnology in food production and biotechnology that focuses on marine resources. You can find out more about all the types of biotechnology by reading the article “Types of Biotechnology Explained: 4 Biotech Colors.” WHAT ARE THE APPLICATIONS OF BIOTECHNOLOGY? Biotechnology has applications in a variety of sectors, such as food processing and preservation, agriculture, bio energy, health and medicine, and waste management. The important thing to remember is that biotechnology mainly focuses on the natural sciences. Taking A Closer Look At Bioengineering Taking A Closer Look At Bioengineering Interestingly, bioengineering and its popularity can be traced back to electrical engineers of the 1950s. It came about as a way to find solutions to various needs, such as the need for replacement organs, as Britannica reports. Some examples of bioengineering include the engineering of bacteria to produce pharmaceutical drugs and the development of artificial knees and other joints. Even ultrasounds and other types of medical imaging techniques are examples of bioengineering, which just goes to show how it’s had such a huge impact on our lives. There are exciting developments in bioengineering currently underway, such as robotics, genetic engineering, and neural engineering. Bioengineers are usually employed by a variety of different institutions, such as pharmaceutical companies, medical research institutions, and regulatory agencies. WHAT ARE THE APPLICATIONS OF BIOENGINEERING? Bioengineering engineering is a field that mainly concerns itself with principles of engineering, such as mechanical, electrical, or chemical engineering, basic sciences such as physics, as well as biotechnology in the form of genetic engineering and tissue engineering. THE DIFFERENT TYPES OF BIOENGINEERING Bioengineering uses what biological theory there is to solve problems in the world. It either makes use of biological systems that are already present or it changes them to enhance or improve their effects. There are many different types, or branches, of bioengineering. Let’s take a look at them. Medical engineering. This has the focus of applying engineering principles to medical problems, such as finding ways to replace or heal damaged organs with the use of engineering techniques. Agricultural engineering. This puts engineering principles to work by using them to solve problems related to biological production and the environment. Bionics. This concerns the study of living systems so that all the knowledge gained from them can be used to design physical systems. An example of this is the use of prosthetic limbs that can be controlled with artificial intelligence. Biochemical engineering. This applies engineering principles to microscopic biological systems that create new products, such as producing protein from raw materials. Another example of biochemical engineering is the development of agricultural chemicals to treat and develop food for human consumption. Human-factors engineering. In human-factors engineering, principles of engineering, psychology, and physiology are applied to the human-machine relationship. In other words, those principles are applied to machines that are designed for our use. An example of human-factors engineering is the creation of the telephone and space suit. Environmental health engineering. This is when engineering principles are applied to the control of the environment, with the aim of increasing human beings’ health, safety, and comfort. An example includes life-support systems for space exploration. Genetic engineering. This is all about changing organisms, and it’s focused on manipulating DNA or other nucleic acid molecules. This has already led to various products that can help people, such as the development of human insulin to control diabetes. Biomimicry. This is a fascinating type of bioengineering, which is also known as biomimetics. It applies natural systems to solve complicated engineering problems. An example is how scientists have mimicked the design of termite mounds to create more energy-efficient buildings. This has been adopted in Zimbabwe, with what’s known as The Eastgate Building. This commercial block of offices is combined with a shopping mall, but it makes use of internal climate control by its design being similar to that of a termite mound. This makes use of natural processes to ensure that inside the building it’s warm during winter and cool during summer, as Environmental Science explains.

### Violation---Cognitive Enhancement

#### Cognitive enhancement falls under bioengineering

Kemp ’20, [Luke; 07/6/20; Centre for the Study of Existential Risk (CSER) and the Biosecurity Research Initiative at St Catharine’s College, University of Cambridge; "The Bioengineering Technologies to Look Out for in the Next Decade," The Wire Science, <https://science.thewire.in/the-sciences/bioengineering-technologies-horizon-scan-2020/> smarx, AZG]

The governance of cognitive enhancement

Cognitive enhancement is already a widely embraced idea throughout society – caffeine is the most widely consumed drug on Earth. Novel methods of cognitive enhancement such as nootropics, wakefulness enhancers, or the potential to directly modulate brain function through implants or biotechnology are emerging. Uptake of these is being driven by both a productivity-focused culture, commercial opportunities and increased understanding of neurochemistry. Although some cognitive enhancers require prescriptions, others only have to meet basic safety guidelines and are available to purchase online.

### AFF---AT: Bioengineering

#### The terms bioengineering and biotechnology are interchangeable

Campbell Soup Company ’17 [08/25/17; “National Bioengineered Food Disclosure Standard - USDA AMS Proposed Rule Questions Under Consideration,” Divisions of Dockets Management, Food and Drug Administration, <https://advance-lexis-com.proxy.lib.umich.edu/r/documentprovider/4588k/attachment/data?attachmentid=urn:contentItem:656P-05H1-J9YR-S067-00000-00&attachmenttype=PDF&attachmentname=Click%20to%20view%20PDF%20document&origination=BlobStore&sequencenumber=1&ishotdoc=false&docTitle=&pdmfid=1516831&#page=> //smarx, AZG]

FDA, in two Guidances for Industry4, has stated that its preferred term, "bioengineering" (which is the same term used in PL 114-216) is interchangeable with the terms "recombinant DNA technology," "modem biotechnology" and "genetic engineering" : In this guidance, we use the terms "bioengineering," "bioengineered," and "genetic engineering" to describe the use of modem biotechnology. Modem biotechnology means the application of in vitro nucleic acid techniques, including recombinant deoxyribonucleic acid (DNA) and direct injection of nucleic acid into cells or organelles, or fusion of cells beyond the taxonomic family, that overcome natural physiological reproductive or recombinant barriers and that are not techniques used in traditional breeding and selection (Ref 1). The term "modem biotechnology" may alternatively be described as "recombinant DNA (rDNA) technology," "genetic engineering," or "bioengineering." These terms are often used interchangeably by industry, federal agencies, international bodies, and other interested stakeholders and are used in this guidance to refer to foods derived from new plant varieties developed using modern biotechnology. 5

## General Definitions

#### Biotechnology is any tech application that uses biological systems, living organisms or derivatives to make or modify products or processes for specific use

Biology Today ‘21 [“Biotechnology: Principles and Processes,” Biology Today, December 28, 2021; https://advance.lexis.com/document/?pdmfid=1516831&crid=ae10a0fe-6992-4304-bc66-b02d89c6f764&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A64D9-BHG1-JBYT-H2MS-00000-00&pdcontentcomponentid=469928&pdteaserkey=sr2&pditab=allpods&ecomp=rzznk&earg=sr2&prid=8b190ba7-e72c-4470-b9a7-b68f451e3393#]

The term biotechnology is derived from a fusion of biology and technology. Biotechnology means any technological application that uses biological systems, living organisms or derivatives thereof, to make or modify products or processes for specific use. · The term biotechnology was coined in 1917 by a Hungarian Engineer, Karl Ereky to describe a process for large scale production of pigs. · Biotechnology involves two common factors: the use of biological agents and the generation of product for the well being of humans. Biotechnology Modern Biotechnology It developed during 1970 for the production of vaccines, medicines, industrial chemicals, genetically modified organisms and food products with the help of recombinant DNA technology.

#### **Biotechnology includes all forms of plant and animal breeding, traditional food fermentation and waste treatment**

Sandeep Rindhe, et al, ’20 [Assistant Professor, Department of Livestock Products Technology, College of Veterinary and Animal Sciences, MAFSU, Narpur, India, Manish Chatli, Professor cum Head and Rajesh Wagh, Assistant Professor, Department of Livestock Products Technology, College of Veterinary and Animal Sciences, GADVASU, Punjab, India; “Targeting selection and yield; The application of these techniques improve the quality, quantity and safety of food,” Fleischwirtschaft International, November 27, 2020; [https://advance.lexis.com/document/?pdmfid=1516831&crid=aae558e3-d410-4efc-a584-2d840ae92c70&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A61CP-32G1-DYG1-P4C9-00000-00&pdcontentcomponentid=280767&pdteaserkey=sr10&pditab=allpods&ecomp=rzznk&earg=sr10&prid=99d0ee5d-07d1-4c45-a24f-8543a393886b#](https://advance.lexis.com/document/?pdmfid=1516831&crid=aae558e3-d410-4efc-a584-2d840ae92c70&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A61CP-32G1-DYG1-P4C9-00000-00&pdcontentcomponentid=280767&pdteaserkey=sr10&pditab=allpods&ecomp=rzznk&earg=sr10&prid=99d0ee5d-07d1-4c45-a24f-8543a393886b)]

The Convention on Biological Diversity defines biotechnology as 'any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use' (CBD, 2000). It therefore includes all forms of plant and animal breeding, traditional food fermentation and waste treatment. The term biotechnology can be defined as "the application of science to biological organisms to give new and improved agricultural and industrial production". The application of biotechnology to farm animals is exciting; offering a mechanism whereby genetic material isolated from any animal, plant or bacterial source can be transferred to a recipient animal resulting in the altered activity of an existing gene within the animal or the production of a new gene product from the animal. The application of biological techniques to food crops, animals and microorganisms opens the possibilities to improve the quality, quantity, safety, ease of processing and production economics of food (IFST, 2004). Biotechnology in the food processing sector targets the selection and improvement of microorganisms with the objectives of improving process control, yields and efficiency as well as the quality, safety and consistency of bio-processed products.

#### **Biotechnology can include the manipulation of tissue, DNA, and desired effect of an organism’s innate functions**

PCU, ’18 [“Biotech 101: A Disruptive Technology Crash Course,” Plus Company Updates, July 2, 2018; [https://advance.lexis.com/document/?pdmfid=1516831&crid=29f299ec-9a14-4f9d-9900-164ffc49f20c&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5SPF-0VK1-J9XT-P408-00000-00&pdcontentcomponentid=424987&pdteaserkey=sr0&pditab=allpods&ecomp=rzznk&earg=sr0&prid=00b89da2-0ef2-4ab7-9eae-ae2916e089f8#](https://advance.lexis.com/document/?pdmfid=1516831&crid=29f299ec-9a14-4f9d-9900-164ffc49f20c&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5SPF-0VK1-J9XT-P408-00000-00&pdcontentcomponentid=424987&pdteaserkey=sr0&pditab=allpods&ecomp=rzznk&earg=sr0&prid=00b89da2-0ef2-4ab7-9eae-ae2916e089f8)]

As a part of this initiative, AmCham China hopes to provide insight on the fundamentals and applications of specific technologies through varied content. One technology driving the incredible motion of innovation forward is biotechnology. The Basics Biotechnology generally refers to “the use of an organism, or component of an organism, for a specific use,” (Khan Academy). More specifically, biotechnology can include the manipulation of tissue, DNA, and desired effect of an organism’s innate functions. Biotechnology is the crossroad of hardware, software, and the most complicated machines in the world: living organisms. The relationship between the three is symbiotic: each supports and relies on the other. The thriving economy of biotechnology lives at the crossroad of technology and medicine, and is currently being driven by massive amounts of money and research - by just March of 2018, US $2.8 billion was poured into biotech startups over the year-to-date. Applications of biotechnology are endless, and can reach us through several avenues. Beer-brewing technology involves biotechnological processes—fungi in the form of yeast are used in the fermentation of malted barley sugar. The same type of technology that makes craft beer has the power to edit DNA. DNA technology is a biotechnology that involves editing the genome, which acts like a genetic instruction manual. Applications of DNA in biotechnology are found in cloning, gel electrophoresis, and DNA sequencing. The human genome is composed of four base components, much like binary code (which is composed of two base components). The genome can be treated like software binary via this similarity, and edited to delete or replace incorrect DNA sequences. By just 2002, scientists at Watson Labs were already learning how to code and program DNA - the leap from one base pair (the 1s and 0s of binary) to two base pairs (ATCG, the building blocks of DNA) was apparently not too large.

#### **OECD broad definition of biotechnology**

OECD, ’06 [“OECD Biotechnology Statistics-2006,” Organization for Economic and Co-operation and Development, 2006; <https://www.oecd.org/science/inno/36760212.pdf>, Accessed via Google Scholar]

Definition of biotechnology  
The OECD has developed both a single definition of biotechnology and a list-based definition (see Box  
below) of different types of biotechnology. The single definition defines biotechnology as “the application of  
science and technology to living organisms, as well as parts, products and models thereof, to alter living or non-  
living materials for the production of knowledge, goods and services.”

#### **OECD list-based definition of biotechnology best – it is the only way of limiting respondent firms that are active in modern biotech**

OECD, ’06 [“OECD Biotechnology Statistics-2006,” Organization for Economic and Co-operation and Development, 2006; <https://www.oecd.org/science/inno/36760212.pdf>, Accessed via Google Scholar]

The OECD list-based definition, or close variants, were used in surveys in 15 countries, but different  
definitions of biotechnology were used in the other 11 countries: 7 studies limit biotechnology to ‘modern’ or  
third-generation biotechnologies that are similar to the OECD list-based definition in practice, 2 studies use  
mixed definitions that include second generation biotechnologies (Japan and South Africa), and 2 do not define  
biotechnology, but leave it to the survey respondent to decide if their firm is active in biotechnology. As the  
latter two studies cover Denmark and Sweden, a large majority of the respondents are likely to interpret  
biotechnology as modern biotechnology.  
OECD list-based definition of biotechnology techniques

DNA/RNA: Genomics, pharmacogenomics, gene probes, genetic engineering, DNA/RNA  
sequencing/synthesis/amplification, gene expression profiling, and use of antisense technology.  
Proteins and other molecules: Sequencing/synthesis/engineering of proteins and peptides (including  
large molecule hormones); improved delivery methods for large molecule drugs; proteomics, protein  
isolation and purification, signaling, identification of cell receptors.  
Cell and tissue culture and engineering: Cell/tissue culture, tissue engineering (including tissue  
scaffolds and biomedical engineering), cellular fusion, vaccine/immune stimulants, embryo manipulation.  
Process biotechnology techniques: Fermentation using bioreactors, bioprocessing, bioleaching,  
biopulping, biobleaching, biodesulphurisation, bioremediation, biofiltration and phytoremediation.  
Gene and RNA vectors: Gene therapy, viral vectors.  
Bioinformatics: Construction of databases on genomes, protein sequences; modelling complex biological  
processes, including systems biology.  
Nanobiotechnology:Applies the tools and processes of nano/microfabrication to build devices for studying  
biosystems and applications in drug delivery, diagnostics etc

# Cybersecurity

## 1NC---Cybersecurity---CIA Triad

#### Interpretation---Cybersecurity policy must expand protections for the confidentiality, integrity, AND availability of data on computer systems and networks.

#### INSERT ANY CIA TRIAD DEFINITION

#### Violation---The affirmative doesn’t address [confidentiality/integrity/availability] explicitly.

#### That’s a voter---

#### A---Limits---any other interp blows the lid off of topical affirmatives as there are infinite ways to engage in some way with cyber-related assets.

#### B---Ground---core negative ground is reliant on the mechanisms described in Kosseff---you should over-correct for the negative on a topic with no topic generics.

#### C---Topic Education---our evidence is most precise about mechanisms at the core of the topic---allowing other mechanisms causes a race to the bottom and skews debate away from controversies.

#### At best they’re extra-T---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

## 2NC---Cybersecurity---CIA Triad

#### Cybersecurity includes protecting networks, devices, and data by ensuring confidentiality, integrity, and availability.

CISA 19, United States federal agency under Department of Homeland Security oversight, November 14, 2019, “What is Cybersecurity?”, https://www.cisa.gov/uscert/ncas/tips/ST04-001 \\SYang

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

#### More ev.

Sudeep Jadey et al. 19, Assistant Professor in the Department of Information Science and Engineering in a reputed organization named "NIE Institute of Technology, Mysuru, Methods, Implementation, and Application of Cyber Security Intelligence and Analytics, https://www.igi-global.com/book/methods-implementation-application-cyber-security/286806, Introduction to Cyber Security (pages 1-24) \\SYang

Cybersecurity may be defined as the ability to protect and recuperate from cyberattacks. According to NIST (National Institute of Standards & Technology), it can be defined as the ability to defend cyberspace usage from cyberattacks. Cyberspace could be internet, computer systems, telecom networks, embedded controllers etc. The security of any organization completely relies on three key areas namely confidentiality, availability and integrity.

1.

Confidentiality: The word confidentiality looks alike privacy. The key idea is to prevent unauthorized users from accessing the sensitive information. Confidentiality makes sure that only authorized users are given permission to access sensitive information. Identity theft, credit card fraud, phishing, wiretapping are some examples of confidentiality attacks

2.

Availability: Availability refers to the genuine access of resources. The information should be made available to the authorized personal. Denial of service attack, Internet Control Message Protocol flood attacks are some examples of availability attacks.

3.

Integrity: Trustworthiness, Data consistency and accuracy are all ensured by integrity. The main goal is to prevent data modification who aren’t authorised to do so. Man in middle attacks, salami attacks and session hijacking are some examples of Integrity attacks. (Priyadarshini, I. 2019)

#### More ev.

Matt Bishop et al. 17, faculty at the Department of Computer Science at the University of CalIFORnia at Davis, May 4, 2017, “Cybersecurity Curricular Guidelines”, https://link.springer.com/chapter/10.1007/978-3-319-58553-6\_1 \\SYang

“Cybersecurity” is a widely used term that speaks to the security of systems and data but has many different definitions. Examples include “[p]revention 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” [9]; “defensive methods used to detect and thwart would-be intruders” [13]; and “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” [7]. Agresti [3] notes that four forces (rebranding, organizational imperative, cyberspace domain, and national defense priority) shape the definitions. Thus, any guidance aimed at cybersecurity must begin by defining that term.

## 1NC---Cybersecurity---Defensive

#### Interpretation: Cybersecurity means to protect---that precludes offensive operations.

MW 22, Merriam Webster is a American company that publishes reference books, Accessed July 4, 2022, “cybersecurity”, https://www.merriam-webster.com/dictionary/cybersecurity \\SYang

Definition of cybersecurity

: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

#### Violation---The affirmative engages in offensive operations.

#### That’s a voter---

#### A---Limits---any other interp blows the lid off of topical affirmatives as there are infinite ways to engage offensively.

#### B---Ground---core negative ground is reliant on the mechanism of defensive action---you should over-correct for the negative on a topic with no topic generics.

#### C---Topic Education---allowing non-defensive operations causes a race to the bottom away from core topical controversies like hardening systems and skews debate.

#### At best they’re extra-T---that’s a voter for limits, clash, and fairness---their model justifies infinite extra-topical planks.

## 2NC---Cybersecurity---Defensive

#### Cybersecurity exclusively means protecting electronic assets and information---that precludes the offensive actions of the aff.

Dr. James Stanger 19, Chief Technology Evangelist at CompTIA and former consultant for IBM, Symantec, the Scottish Qualifications Authority (SQA), the United Arab Emirates Cultural Division, the Open University (UK), the U.S. Department of State, Mesei University, the University of Phoenix, and the Business Professionals of America (BPA), June 17, 2019 “What Is the Difference Between IT Security and Cybersecurity?”, https://www.comptia.org/blog/what-is-the-difference-between-it-security-and-cybersecurity \\SYang

1. Physical security: Focuses on how you keep people and infrastructure safe. In this category, you focus on securing buildings, server rooms and wiring closets. You focus on proper lighting for buildings and parking lots, for example. It also involves understanding how to use camera guards, as well as actual guards and even guard dogs.

2. Information security: Focuses on keeping all data and derived information safe. This includes physical data (e.g., paper, computers) as well as electronic information. In this category, individuals focus on data backups, as well as monitoring techniques to make sure that no one has tampered with data or exfiltrated information. This category focuses less on the actual equipment and computing resources because it focuses on the data itself. And, yes, I’m distinguishing between data and information: data is raw and unprocessed. Information is derived from data after quite a bit of scrubbing, processing and handling.

3. Cybersecurity: Focuses on protecting electronic assets – including Internet, WAN and LAN resources – used to store and transmit that information. Cybersecurity tends to focus on how malicious actors use these resources to attack information. Those individuals interested in cybersecurity are the ones interested in making sure that hackers can’t use electronic means to gain improper access to data and information.

#### Cybersecurity only means protection.

Dan Craigen et al. 14, Director of Carleton University's Global Cybersecurity Resource, former science advisor for the Government of Canada and former President of ORA Canada, October 2014, “Defining cybersecurity”, https://www.timreview.ca/article/835, Technology Innovation Management Review \\SYang

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.

#### Protect means to keep safe from injury, damage, or loss---that’s not the aff.

Cambridge Dictionary 22, Accessed July 5, 2022, “protect”, https://dictionary.cambridge.org/us/dictionary/english/protect \\SYang

to keep someone or something safe from injury, damage, or loss:

## 1NC---Cybersecurity---Electronic Digital Media

#### Cybersecurity necessitates the use of electronic digital media

Nicholas Bartlett 21, law degree from University of Toledo, “HONING IN ON HARDWARE: DATA SECURITY CONCERNS OF LARGE COMPANIES”, Winter 2021, University of Toledo Law Review, Vol. 52, p. 545 /lg

I magine for a moment that you are interested in computers, and you purchase a couple of old used servers from a company. Once you get home and access the servers, you notice that one of them is completely full of sensitive consumer information. This includes names, addresses, contact information, etc. A few questions should circle your mind at that point. "What do I do now? How did this happen?" Well, in 2006, this actually occurred. Mark Morris, self-described used computer dealer, claimed to have found sensitive data on servers from Ernst & Young. Morris wanted to be paid to remove the data which should have been wiped before he came into possession of the servers, but Ernst & Young simply wanted the servers returned to them. This conflict unsurprisingly resulted in legal proceedings.

This event raises a significant issue: hardware security. Much of the news today revolves around data breaches that occur from hackers or people intruding networks remotely. The general public does not hear much about events like the scenario described above, where someone discovers a server that was not properly disposed of by the company. There are a few possibilities for why this is rarely known, but it is still an important aspect of data security that should be handled with competence. Failure to competently secure company data on hard drives may result in liability either from federal or state securities laws or common law fiduciary duties. The aftereffects of incompetence can be just as destructive as a remote security breach. Hefty fines can be issued if the information was required by law or industry standard to have been retained by the company. Further, the information may end up in the wrong hands. Morris was allegedly receiving offers to purchase the information on the purchased servers for up to $ 1.2 million. It [\*546] would not be at all shocking for a court to be harsher on a company who negligently handles their hardware when the entity has complete, direct control over the process as opposed to a data hack by an outsider.

While most of the focus in the cybersecurity context today revolves around protecting the intangible data, directors need to pay equal attention to the physical devices this data is stored on. The Securities Exchange Commission (SEC) should be issuing further guidance specifying this need. This guidance should look similar to state statutes that require companies to develop comprehensive data security practices and procedures.

While many legal scholars have recently focused on liability resulting from data breaches, this note focuses exclusively on hardware and what the SEC should be doing to guide corporations. Specifically, this note will provide a more nuanced look at how large companies should be treating their physical hardware, i.e., servers, hard drives, and the like.

This note will examine what cybersecurity is and the related issues facing companies today. It will then transition to an elaboration on fiduciary duties and their relation to cybersecurity incidents and hardware concerns. A discussion of current federal and state laws will follow, along with examples of guidance from other organizations. Finally, the conclusion will provide a recommendation of how hardware security should be emphasized and what may be missing from federal guidance from the SEC. Specifically, the SEC should issue further guidance and potentially adopt a statute that is designed to meet the concerns related to physical data breaches.

I. BACKGROUND

a. Cybersecurity and Potential Liability

A cyberattack is a willful breach of a company's computer systems and networks. Code is often used to disrupt the normal operations that can compromise sensitive data and result in consequences such as identity and information theft. Cyber threats are constantly changing and require an expenditure of resources to continually update data security departments within corporations. Cybersecurity can be defined as "the protection of investor and firm information from compromise through the use -- in whole or in part -- of electronic [\*547] digital media." The phrase "data has been compromised" refers to loss of confidentiality, integrity, or availability of that data. Specifically, a loss of confidentiality indicates disclosure of information, a loss of integrity means the destruction of information, and a loss of availability is the interruption of access to information.

The probability of cyber incidents occurring combined with their impact is referred to as Cyber Risk. Cyberattacks may be carried out in a variety of ways, such as by third parties or company insiders using complex techniques or through traditional social engineering. Attacks can come remotely in a more stereotypical sense similar to what is seen on television or they can come through more personal means by directly interacting with people and gaining information needed to conduct the cyber-attack. There can be many costs and negative consequences associated with a data breach:

#### Violation: the affirmative does not require or involve electronic digital media

#### Prefer our interpretation:

#### Neg ground – failing to specify the technologies used to achieve cybersecurity crushes the potential for disad links

#### Aff ground – our interpretation allows for protection of physical technological devices, which is usually disregarded

#### Education – Bartlett uses relevant cybersecurity issues as the basis for his definition

## 1NC---Cybersecurity---Cyberattacks

#### Cybersecurity means preventing, detecting, and responding to cyberattacks

Allison Shuren 20, co-chair of a practice at Arnold & Porter who advises on regulatory, compliance, enforcement, and legislative matters, “HHS Finalizes New Protections Under The Stark Law For Value-Based Arrangements And Makes Other Critical Revisions And Clarifications To The Regulations That Physicians And Designated Health Service Entities Must Understand”, 11/27/2020, Mondaq Business Briefing /lg

"Necessary and used predominantly" standard: To meet the Stark Law exception, the donated technology (both software and hardware) must be "necessary and used predominantly" for cybersecurity purposes. Definition of Cybersecurity: CMS finalizes the definition of cybersecurity to be: "the process of protecting information by preventing, detecting, and responding to cyberattacks."Definition of Technology: CMS finalizes the definition of technology to be: "any software or other types of information technology."Donors: In the proposed rule, CMS solicited comments on the types of donors who should be protected under this exception. In the Final Rule, CMS declines to finalize limits on the types of donors protected under this exception; instead, the Final Rule protects all donors. However, neither the eligibility of a physician for the technology or services, nor the amount or nature of the technology or services, should be determined in any manner that directly takes into account the volume or value of referrals or other business generated between the parties. CMS declined to include a list of selection criteria that, if met, would mean a donation would be deemed to meet this requirement.Recipients: CMS finalizes the proposed requirement that neither the physician nor the physician's practice can make the receipt of cybersecurity technology or services, or the amount or nature of the technology or services, a condition of doing business with the donor.Written requirement: CMS finalizes the requirement that an arrangement for the provision of cybersecurity technology and related services be documented in writing.This requirement is fulfilled if contemporaneous documents would permit a reasonable person to verify compliance with the exception at the time that a referral is made.No Monetary Cap: CMS declines to finalize a monetary cap in the Final Rule.

#### Violation: the affirmative is extra topical – the plan addresses more than cyberattacks

#### Extra topicality is a voter:

#### Fairness – allowing affirmatives to take untopical actions denies the neg an opportunity to negate the resolution

#### Topic education – debates should be confined to the topic of the resolution – we switch topics for a reason

#### Predictability – neg teams can’t imagine the multitude of affs that aren’t a core part of the topic

#### Prefer our interpretation:

#### Limits – any other interpretation allows for affs that address tangentially related concerns

#### Ground – the aff-skewed nature of the resolution means that neg teams need the chance to generate links to a core topic area

## Affirmative

### 2AC---C/I---Cybersecurity = 5 Mechs

#### C/I---Cybersecurity includes these 5 mechanisms---that’s the aff.

CompTIA 22, leading provider of vendor-neutral IT certifications in the world, Accessed July 4, 2022, “What Is Cybersecurity?”, https://www.comptia.org/content/articles/what-is-cybersecurity \\SYang

Cybersecurity can be categorized into five distinct types:

Critical infrastructure security

Application security

Network security

Cloud security

Internet of Things (IoT) security

### 2AC---C/I---NIST Framework

#### C/I---Cybersecurity is defined as according to the NIST framework---IPDRR (Identify, Protect, Detect, Respond, Recover)---it’s the most contextually accurate.

* Probably includes affs like OCOs (MOU= “Respond”) and affs that clarify article V responses---“Respond”
* Probably does not include affs that directly engage in offensive operations

Jeroen Van Der Ham 21, associate professor of Cyber Security Incident Response in the Design and Analysis of Communication Systems (DACS) group at the University of Twente, June 2021, “Toward a Better Understanding of Cybersecurity”, https://dl.acm.org/doi/fullHtml/10.1145/3442445 \\SYang

With over 40 years of practice, we now have a better understanding of the risks for cybersecurity. We have been able to learn from many different kinds of incidents and attacks. So the risk models that we can create now are grounded in both theory and practice.

Yet, many practical and academic reports today still use the CIA triad as the definition of cybersecurity, while many newer approaches exist. As an example, consider the NIST cybersecurity framework [3].

3.1 The NIST Cybersecurity Framework

The NIST cybersecurity framework is defined as a set of five different activities. These activities are continuous, and the level to which these are performed depend on the organisation and its context. They are as follows:

 Identify: identify the assets that must be secured and the context that they are in

 Protect: define and implement protective measures for the assets

 Detect: put sensors and processes in place to detect when protection has been breached

 Respond: define response processes for when an incident has been detected

 Recover: develop plans for resilience in the organisation, as well as recovery mechanisms

With the identify activity all assets of an organisation that must be secured are identified. Creating this overview of all assets facilitates taking a more generic approach to security when assets are to be protected. Another important part of the identify activity is to examine the context of the assets, to consider what the assets must be protected, but also how the protective measures may impact existing processes.

Protect in the framework is only one of the activities instead of the main focus. This process puts the protective measures more into perspective and makes them part of an overall solution.

The Detect, Respond, and Recover activities force one to consider that security is never absolute. Some risks are just too costly to protect against and instead should be addressed by detection, incident response, and recovery activities. It also forces one to consider that security is never perfect, so other measures should be put in place to mitigate negative consequences of other protective measures that may fail.

3.2 More Appropriate Cybersecurity

Addressing cybersecurity as a an overarching activity instead of a binary measure creates more appropriate responses on cybersecurity. Appropriate in the sense that the defence fits the context and the actual risks identified instead of aiming for an absolute defence for each individual asset. Approaching cybersecurity as a general activity creates a better overview and facilitates a more concerted effort with different protectional measures.

Finally, viewing cybersecurity as a continuous activity allows organisations to better move with developments. Having identified each of the assets and having already done risk-assessments makes it easier to re-evaluate these in light of upcoming changes.

### 2AC---C/I---Includes Satellites

#### Cybersecurity is the prevention of damage to, unauthorized use of, or exploitation of information systems --- includes protection and restoration of satellites

Christopher Hannan 16, lawyer who briefed and argued multiple issues on consolidated appeals in the United States Fifth Circuit Court of Appeals and graduated from the Loyola School of Law, J.D., magna cum laude with Law Excellence Awards in Civil Procedure I, Legal Research & Writing, Civil Law Property II, Maritime Personal Injury, Evidence, Law of the European Union I, Courts in a Federal System and Community Property, “Maritime Cybersecurity Inland and Offshore – Avoiding ‘Paid Spies and Secret Confidential Agents on the Water of the Devil’ and ‘Mere Dead Reckoning of the Error-Abounding Log’”, 12/14/2016, JDSUPRA, https://www.jdsupra.com/legalnews/maritime-cybersecurity-inland-and-51369/ /lg

The past eighteen to twenty-four months have seen a tectonic shift of focus (as well as a plethora of industry-generated white papers) by virtually every governmental regulatory entity, NGO, and industry group in the maritime world (up to and including the President of the United States) to the amorphous and dynamic issue of maritime “cybersecurity,” a term that covers a large waterfront of potential threats. The United States Coast Guard (USCG) has adopted the following broad definition of “cybersecurity” from the U.S. Department of Homeland Security. National Infrastructure Protection Plan, 2013:

Cybersecurity – The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

USCG Cyber Strategy: The U.S. Coast Guard’s Vision for Operating in the Cyber Domain (June 2015).

And with the recent September 2016 roll-out of what has been billed as the maritime industry’s first “cybersecurity” certification program by the American Bureau of Shipping (ABS) – the USCG’s foremost third-party delegated enforcement entity – vessel owners and operators would be well-advised to stay ahead of the ever-sharpening “cybersecurity” curve.

All of the competing (sometimes conflicting) and overlapping aspects of this ever-and-rapidly changing issue are far beyond the scope of this blog post. Given that the majority of the focus in this area has tended toward the traditional blue-water shipping industry (viz. vessels and ports/terminals), this post will focus on ways that the inescapable brave new world of maritime cybersecurity is affecting, and will continue to effect, inland and offshore vessel operators.

### 2AC---C/I---Includes Cybercrime

#### Cybersecurity includes network and information security, the fight against cybercrime, and cyber defense

Christian Calliess & Ansgar Baumgarten 20, Professor for Public and European Law at Freie Universität Berlin, holder of an Ad Personam Jean-Monnet-Chair, and previous Legal Adviser to the European Political Strategy Center (EPSC), advising and working under the authority of its President Jean-Claude Juncker & PhD candidate and scientific assistant for Dr. Calliess at Freie Universität Berlin, “Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective”, 2020, German Law Journal, Vol. 21, p. 1149 /lg

Alongside space, air, land, and sea, cyber is the fifth dimension. It opens a global virtual world, radically changing societies and shaking classical borders. But a digital world also comes with new types of micro threats on businesses and citizens, and macro threats on public policies and state security, which are asymmetrical, unpredictable, and unaffected by classical state responses. They occur at [\*1150] the level of tricksters and range up to state espionage and, potentially, offensive cyber-attacks against states. Cyber is as such a new global world, where there is no dividing line between external and internal security. There is an attacker in one country, aiming for a target in another, causing damage in yet a third. There are as well large-scale attacks targeting and affecting several Member States at once--with the actual attack being carried out in cyberspace, which does not even adhere to one spot, country, or continent, but is a dimension for itself. This raises the question of the adequacy, or inadequacy, of the classical regulatory tools to reply to these challenges.

In this new environment, the EU and its Member States need to anticipate and plan for hitherto unimaginable scenarios in which they would be put if under a severe cyber-attack. This is particularly true for the implementation of the European Commission's EU Digital Single Market agenda. With the financial industry at its very center, a digital single market for the free movement of persons, services, and capital is highly dependent on a reliable and robust IT infrastructure. Comparable to the field of "industry 4.0," innovation in the financial sector--for example, the idea of a "Digital City," a financial platform of Europe that coordinates a network of financial centers in the EU --and the success of new business models depend on trust in a safe digital environment.

Cybersecurity is a term that covers a wide range of activities. Broadly speaking, it can be divided into three different categories: Network and information security, fight against cybercrime, and cyber defense. With regard to network and information security, cybersecurity can be defined as the ability of network and information systems to resist action that compromises the availability, authenticity, integrity, or confidentiality of digital data or the services those systems provide. This Article will focus on cybersecurity in the financial sector in its dimension of network and information security. Still, it will also refer to the other two areas of cybersecurity where necessary and appropriate. The financial sector is understood as the entirety of payment systems, credit institutions, payment institutions, stock exchanges, trade repositories, central securities depositories, central counterparty clearing houses, securities settlement platforms, credit rating agencies, insurance companies, and asset management companies.

### 2AC---C/I---Broad + Predictable

#### Cybersecurity can be in the realm of research domains, sectors, or technologies and use cases --- specific to European law

Igor Nai-Fovino et al. 19, Scientific Project Manager with the Joint Research Centre in Ispra, Italy who was a Contractual Researcher with the University of Milano and received Ph.D. in computer security from the Università degli Studi di Milano, “A Proposal for a European Cybersecurity Taxonomy”, 2019, European Comission (executive body of the EU) /lg

2.3 General Considerations on the analysed sources

The sources presented in the previous section have been used to identify:

A common set of vocabularies and terms;

A set of specific sub-domains;

A set of applicable sectors.

Ad-hoc desktop research activities have been conducted to identify relationships among domains, synonyms and to discriminate between cybersecurity peculiarities and generic items. Table 7 summarises the contribution provided by all the identified sources to the definition of the taxonomy presented in section 3.

On the basis of the analysis conducted, it is possible to draw some general considerations:

The analysed standards provided a good source reference for the definition of terms, and for the identification of some domain areas linked to the risk-assessment domain. The same risk-assessment elements can be found in the resilience function areas defined by NIST and well as in the NIST CSRC categorisation. When instead coming to the identification of research domains, the analysed standards can be considered negligible as conceived to drive a technical standardisation process in very specific domains and not to classify knowledge and scientific activities

The NIS directive and the NIST CRSC share, with some variations, a common understanding of the sectors where cybersecurity must be considered paramount, hence by merging these two sectorial views it is possible to identify a relevant element of the taxonomy which will be presented in Section 3

The taxonomies of IEEE, IFIP, ECSO, ETSI and Cyberwatch.eu often overlap with the NIST CRSC resulting the better detailed and logically structured. The merging of these three sources could provide a good starting point for what concerns the technological and scientific domains.

NIST CRSC considers into its categorisation also law and regulation aspects; this is perfectly in line with the scope of the taxonomy subject of this study, however the subdomains listed are obviously related to the US regulation landscape, and cannot be considered as useful to map the EU law and regulation cybersecurity expertise. However, the NIS directive and the GDPR can be used there to close the gap

As it is possible to see the identified sources well complement each other allowing to cover almost all the cybersecurity spectrum. By using the identified concepts and leveraging on standards for what concerns definitions and vocabulary, a more general and EU oriented taxonomy of the cybersecurity and privacy domain is presented in Section 3.

3 Holistic Taxonomy for Cybersecurity Research Domains

The analysis of the reference sources described in the previous section highlights the complexity and heterogeneity of the cybersecurity discipline. In a similar situation, in order to ensure capturing every aspect of this domain, the taxonomy proposed in this document might risk to become super-specialised, with a multitude of nested domains. The goal of the taxonomy proposed in this report is that of supporting the mapping of the European cybersecurity competencies available. The goal of the taxonomy is not to support the mapping of cybersecurity products, services, or processes including operational activities. The analysis conducted so far however suggests adopting a different, more agile approach. The analysis of the scientific/technological working groups activities (e.g. IFIP, ETSI etc.) and of the “knowledge management entities” (e.g. ACM, IEEE etc.) gives a clear and precise indication of the areas of fundamental research within the cybersecurity domain.

On the other side, the analysis of policy documents and regulations allowed to magnify which sectorial domains are perceived as the most relevant for the wellbeing of the European Society (the assumption here is that regulations and policy packages answer to a precise European citizen and industry regulatory needs).

Finally, the analysis of the market studies, of the observatory initiatives and of the R&D programs (H2020), provides an indication of the field of technologies and use cases where the cybersecurity foundational research results are applied. Technologies and uses cases typically involve multiple sectors.

This reasoning reached the conclusion that a taxonomy trying to cluster a complex and multifaceted discipline as cybersecurity needs to be structured on multiple dimensions, capturing not only the core and traditional research domains, but also impacted sectors and applications.

Figure 5, depicts, in a graphical way, the proposed three-dimensional taxonomy, based on the following dimensions:

Research domains represent areas of knowledge related to different cybersecurity aspects. Given the multidisciplinary nature of cybersecurity, such domains are intended to cover different areas, including human, legal, ethical and technological aspects.

Sectors are proposed to highlight the need for considering different cybersecurity requirements and challenges (from a human, legal and ethical perspective) in scenarios, such as energy, transport or financial sector.

Technologies and Use Cases represent the technological enablers to enhance the development of the different sectors. They are related to cybersecurity domains covering technological aspects.

The three-dimensional taxonomy can be used as a reference to map cybersecurity competencies, for example, in Figure 5 an entity working on Cryptology in the Energy sector considering Embedded Systems is mapped.

Each dimension has been fine-tuned and detailed on the basis of the analysis presented in the previous section to:

a) ensure its alignment with the European Regulatory landscape;

b) ensure its comprehensiveness (merging together where needed sub-domains highlighted in different classifications and standards);

c) avoid redundancy of terms and definitions.

In what follows, definitions for each dimension of the proposed taxonomy are presented. More in details, Subsection 3.1 lists for each of cybersecurity domains the relevant sub-domains. Subsection 3.2 details the sectorial sub-domains, and Subsection 3.3 illustrates the list of technologies and use cases. The taxonomy is completed with the glossary of concepts and vocabulary included in Annex 1. The cybersecurity subdomains defined for each domain, sectors and technologies/use cases are by no means an exhaustive list, these elements will be complemented in the future based on the input from cybersecurity centre of excellences surveyed.

### 2AC---C/I---Military/Domestic/Econ

#### “Cybersecurity” means protecting military security, domestic peace and order, or economic stability from cyber threats

National Cybersecurity Bill (Thai) 15, “Memorandum of Principle and Rationale of [Draft] National Cybersecurity Act B.E”, draft was approved by the cabinet on 01/06/2015, translated by the Thai Netizen Network, [https://thainetizen.org/wp content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf](https://thainetizen.org/wp%20content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf) /lg

“Cybersecurity” means measures and operations that are conceived in order to maintain national Cybersecurity, enabling it to protect, prevent or tackle circumstances of cyber threats which may affect or pose risks to the service or application of computer network, internet, telecommunications network, or the regular service of satellites in ways that affect national security, which includes military security, domestic peace and order, and economic stability.

### 2AC---C/I---Includes Offensive Operations

#### C/I---Cybersecurity can be both offensive and defensive---their evidence doesn’t have intent to exclude.

Lily Teplow 21, Content Marketing Manager at Huntress, September 14, 2021, “Should We Be Playing Offense or Defense in Cybersecurity?”, https://www.huntress.com/blog/should-we-be-playing-offense-or-defense-in-cybersecurity \\SYang

Defensive cybersecurity is all about blocking. This could come in the form of both tools and actions. You have your defensive tools that are designed to prevent or mitigate the effects of a cyberattack—such as antivirus software, firewalls, etc. And then you have your defensive actions, which include things like patching software and fixing system vulnerabilities.

Offensive cybersecurity, on the other hand, is all about tackling and outmaneuvering. The focus here is on seeking out the hackers, and in some cases, attempting to disable or “hack back” to disrupt their operations. Offensive cybersecurity can also help identify vulnerabilities or weaknesses in your defense. It’s a slightly more proactive approach to security and can include practices like penetration testing and threat hunting.

No matter which side of the field you’re on, the goal of any cybersecurity strategy should always be preventing the hackers (a.k.a. the opponent) from winning. But that brings us back to our original question: should we be playing offense or defense in cybersecurity?

The answer is both.

The best teams know how to block and tackle. In cybersecurity, building the best possible defense means folding in some offensive strategies to gain intel on attackers and how they’re trying to penetrate your systems.

### 1AR---C/I---Includes Offensive Operations

#### The USfg says it includes military missions---that’s the aff.

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES 22, online training initiative and portal built as per the National Initiative for Cybersecurity Education framework operated and maintained by the Cybersecurity and Infrastructure Security Agency, June 30, 2022, “Glossary”, https://niccs.cisa.gov/cybersecurity-career-resources/glossary \\SYang

cybersecurity

Definition: 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.

Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

### 2AC---AT: Defensive Only

#### Precision DA---contemporary cybersecurity includes offensive techniques.

Bred Medairy 22, 2021 Federal 100 Award Winner, Top 50 Cyber Leader for 2021, 2020 Cyber Executive of the Year by the Northern Virginia Technology Council, and a Finalist for WashingtonExec’s 2020 Cybersecurity Industry Executive of the Year, accessed July 5, 2022, “The future of cybersecurity: the best defense is a good offense”, https://www.boozallen.com/s/insight/blog/future-of-cybersecurity.html \\SYang

In today’s unpredictable environment, filled with rapidly evolving threat actors and emerging technologies, the only way organizations can protect themselves is by unleashing offensive cyber techniques to uncover advanced adversaries on their networks. The most effective approach—Threat hunting—is essential to any organization that wants to stop and prevent attacks in its networks.

“In working with clients on hunt engagements, Booz Allen has found an average dwell time—that is, the time an advanced adversary lies undetected in a victim’s network—of 200-250 days before discovery. ”

Advanced adversaries live in the noise of networks and defeat reactive, rule-based cybersecurity defenses by constantly developing malicious tactics, techniques, and procedures (TTPs). These developments—such as polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and hijacking legitimate operating system functions—all evade traditional defenses.

### 2AC---AT: Excludes Property Rights

#### The property rights interp is too vague, unnecessarily broad, and impedes the success of cybersecurity operations

Derek E. Bambauer 15, Professor of Law at the University of Arizona, where he teaches Internet law and intellectual property (covers Internet censorship, cybersecurity, and intellectual property) + was a Research Fellow at the Berkman Center for Internet & Society at Harvard Law School, “Conundrum”, 04/11/2015 revision date (originally published 4/11/2011), Minnesota Law Review, Vol. 96, p. 584 /lg

Conceptualizing cybersecurity challenges policymakers and academics. 32 The current theoretical approaches to cybersecurity, though, have proved to be significantly flawed. They employ definitions that are vague and overbroad; they seek to force cybersecurity's issues into the straitjackets of existing doctrines poorly suited to cybersecurity's problems; and they produce concomitant policy recommendations that not only fail to mitigate, but actually worsen, the Internet's security challenges.

Conventional wisdom on cybersecurity identifies the problem as all-encompassing. 33 Scholars, government officials, and journalists tend to view cybersecurity as the "protection of all things Internet" 34 - an approach that impedes practical progress by failing to set priorities. Government efforts at capturing cybersecurity's scope have been particularly overbroad. [\*592] President Barack H. Obama's Cyberspace Policy Review offers a representative definition, where cybersecurity is:

strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. 35

Presidential policies have been strikingly consistent. President Barack Obama's approach to cybersecurity is almost identical to the Comprehensive National Cybersecurity Initiative (CNCI), the strategy employed by Obama's Republican predecessor, President George W. Bush. 36 Their cybersecurity definitions and programs are closely aligned; indeed, Richard Clarke and Robert Knake call Obama's plan "CNCI redux." 37 Both policies build on the recommendations and definitions (in particular, of critical infrastructure) of President William J. Clinton's Commission on Critical Infrastructure Protection. 38 Regardless of political affiliation, American Presidents have taken an expansive view of cybersecurity.

Proposed federal legislation is equally capacious in approach. The National Cyber Infrastructure Protection Act of 2010 defines "cyber security activities" as:

[\*593]

a class or collection of similar cyber security activities by a Federal agency that involves personally identifiable data that is -

(A) screened by a cyber security system outside of the Federal agency …

(B) transferred, for the purpose of cyber security, outside such Federal Agency; or

(C) transferred, for the purpose of cyber security, to an element of the intelligence community. 39

The Act conceives of cybersecurity not only broadly - it could include the Federal Trade Commission's anti-spam efforts, for example - but recursively. 40 The Protecting Cyberspace as a National Asset Act of 2010 defines "information security" as "protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide" integrity, confidentiality, and availability. 41 The Homeland Security Cyber and Physical Infrastructure Protection Act of 2011 proposes cybersecurity requirements that cover "an occurrence that jeopardizes the security of data or the physical security of a computer network owned or operated by a Federal agency or covered critical infrastructure," 42 where critical infrastructure includes private sector computer systems identified by the Department of Homeland Security. 43 In short, for government policymakers, there is little that cybersecurity does not cover.

Similarly, legal scholars define the concept expansively. Gus P. Coldebella and Brian M. White see cybersecurity as encompassing "criminality of all stripes, nation state and corporate espionage, and attacks," even while they decry term-creep in the concept. 44 Sean M. Condron, of the U.S. Army's Judge Advocate General's Legal Center and School, 45 defines [\*594] the problem as attacks on critical infrastructure by "terrorists, nation-states, terrorist sympathizers, and thrill seekers," 46 where critical infrastructure comprises networked computer systems "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 47 Susan Brenner, in her Article classifying cybersecurity risks based on the actor's intent, defines cyberthreats as those "using computer technology to engage in activity that undermines a society's ability to maintain internal or external order." 48 Milton L. Mueller decries the fact that "the term security now encompasses a host of problems, perhaps too many to fit properly under one word." 49 However, he then proposes a governance-based approach to cybersecurity without offering a coherent definition of the term, and includes spam, phishing, and surveillance as representative threats. 50

Even scholars who purportedly focus on narrower aspects of cybersecurity employ commodious definitions. Kelly Gable, who concentrates on cyberterrorism, defines it as "efforts by terrorists to use the Internet to hijack computer systems, bring down the international finance system, or commit analogous terrorist actions in cyberspace." 51 A 2001 report by Steven A. Hildreth of the Congressional Research Service describes cyberwarfare as "various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same." 52 Brenner defines cybercrime as "the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order." 53 Richard Clarke, former Special Advisor on Cybersecurity to President George W. Bush, and co-author Robert Knake even conceive of cybersecurity as encompassing [\*595] intellectual property theft. 54 These definitions of cybersecurity are vague, overbroad, and not helpful. Each attempt at framing the cybersecurity problem implicitly sets a standard for addressing the problem, for prioritizing it relative to competing concerns, and for measuring progress. Inaccurate cybersecurity definitions impede these efforts.

Conceptual failures - shortcomings in theoretical orientation - are largely to blame for what all commentators agree is an utter lack of success in improving cybersecurity. 55 Legal scholarship has thus far approached cybersecurity questions from within well-established, comfortable, yet poorly fitting models from criminal law, national security law, and military law. These doctrinal frameworks push scholars to concentrate upon the identity of actors behind a cyberthreat, and to determine their intent. 56 The problem is that the Internet's design makes attribution extremely difficult. 57 Tracing an attack to a given computer is challenging; deciphering who operated that computer during the attack is harder yet; and discerning motive can be nearly impossible. 58 The chief culprit, for most [\*596] scholars, is the lack of an authentication mechanism in the Internet's core TCP/IP protocols. 59 The Internet routes data in best-efforts fashion, regardless of who sent it. 60 Indeed, there is simply no way to verify a sender's identity under TCP/IP; functions such as authentication and error-checking are left to higher-level network layers and applications. 61 This default setting, which permits unattributed communication, is frequently exploited by malefactors - Internet traffic can be generated by botnets of suborned computers available for rent, or from computers specifically compromised for purposes of an attack. 62

Recent cybersecurity incidents illustrate the problem. The cyberassault on Estonia during that country's conflict with Russia in May 2007 originated in part from computers located in Brazil and Vietnam. 63 The July 2009 denial of service attack against South Korea and the U.S., widely attributed to North [\*597] Korea, 64 was launched from computers in Austria, Georgia, Germany, and even South Korea and America. 65 In both cases, initial judgments that a State (Russia or North Korea) was responsible dissolved into uncertainty in the face of mixed evidence. Attribution is thus an intolerably hard problem for conventional legal approaches. Worse, it is one that flows directly from the architecture of the Internet. 66

Unsurprisingly, the predominant answer to this perceived shortcoming is to retrofit attribution capabilities into the core of the Internet. Clarke and Knake want to move to new networks where "the user's authenticated identity could be embedded in each packet." 67 Jeffrey A. Hunker too believes that the "existing Internet architecture is fundamentally insecure." 68 He seeks to replace the Internet with a network that allows "different governments to have different rules," where governments "protect their citizens on the Internet the same way they protect them" in other media. 69 Former Director of National Intelligence Mike McConnell argues "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment … more manageable." 70 Former CIA Director Michael V. Hayden proposes creating a new, "hardened enterprise structure" for the Internet that [\*598] would embed identification capabilities into its architecture. 71 Stuart Biegel states that "code-based adjustments in Internet architecture … can go a long way toward countering cyberterrorism." 72 Greater attribution enables the traditional practice of deterrence, along with traditional distinctions among criminals, terrorists, soldiers, and spies. 73 By building strong attribution into networking protocols, lawyers (and their governments) can apply time-tested ways of thinking and reacting to threats online. However, trying to redesign the architecture of the Internet as a solution has at least three critical shortcomings: difficult implementation, unintended consequences, and loss of generativity.

### 2AC---AT: CIA Triad

#### Precision and Topic Education DA---the CIA definition sucks---it was relevant in the 80s---the field has shifted since then and continued use of the definition is archaic and impedes effective cybersecurity.

Jeroen Van Der Ham 21, associate professor of Cyber Security Incident Response in the Design and Analysis of Communication Systems (DACS) group at the University of Twente, June 2021, “Toward a Better Understanding of Cybersecurity”, https://dl.acm.org/doi/fullHtml/10.1145/3442445 \\SYang

1 INTRODUCTION

For many years a popular definition of cybersecurity has been the CIA triad: Confidentiality, Integrity, and Availability. In this column I argue that this definition can lead to a narrow view of cybersecurity. Instead, we should focus more on the activity and associated risks for cybersecurity. It is now time to let go of this ancient definition and seek better ways to define cybersecurity.

2 THE CIA TRIAD

The CIA triad, Confidentiality, Integrity and Availability, has been used as the practical definition of information security, and later cybersecurity, since the beginning of the field of cybersecurity. The tenet of the CIA triad is that cybersecurity of assets is defined by three different aspects:

 Confidentiality: information is only available to the intended consumers,

 Integrity: it is possible to prove that the information has not been changed,

 Availability: information should be available to the intended consumers.

The triad itself was introduced in the Anderson Report [1], which discussed security exposure, and repeated in Saltzer and Schroeder [5]. The CIA abbreviation was coined later by Steve Lipner around 1986 [2]. Since then, the term has been used widely in reports, standards, and other publications on cybersecurity.

2.1 Focus on the CIA Triad Aspects

The focus on the aspects defined in the CIA triad is problematic for several different reasons. The aspects are binary measures; at a given time they are either true or false. This sense of measurement gives a false sense of accomplishment, as the current status gives no guarantees about the future (or even the past).

The binary nature of these aspects is counterintuitive to risk assessment. Each aspect is taken as an absolute value that must be upheld, instead of performing a risk assessment that may impact the security of an asset.

The triad leads to a narrow focus on the security of individual assets. Confidentiality is a property of an individual asset, and usually not a property of a context, such as a computer network or office environment. This then leads to individual measures on objects instead of a general approach to cybersecurity.

The individual, binary measures and narrow focus in turn often lead to stop-gap solutions. Once a vulnerability threatens to break confidentiality, a measure is put in place to ensure confidentiality again. The actual risk associated with that vulnerability is then usually not taken into account. Due to the mitigation, confidentiality is now guaranteed again, so the problem appears to be solved. This is then often repeated many times for every new vulnerability.

Over the years, the CIA triad has been extended but has always retained a focus on aspects of assets. One of the first extensions has been to add “non-repudiation.” A later extension is the Parkerian hexad [4], with two other additional aspects, “possession” and “utility.” The fundamental problem of the focus on (binary) aspects of individual objects remains, however.

2.2 The Context has Evolved, the Approach to Security Has Only Minimally Adapted

In the advent of the cybersecurity field, risks associated with cybersecurity were poorly understood. When the CIA triad was proposed, computers were not connected to a (local) network, and the Internet did not even exist. Ware [6], Anderson, and Saltzer and Schroeder have done great theoretical work regarding computer security, since there were little to no practical attacks on computers.

The context in which we use computers has evolved significantly. From single, offline, room-filling computers, we now have multiple computers in our pockets that are constantly connected. Most processes in the physical world are now affected in some way or another by computers. The nature of adversaries have changed significantly.

### **2AC---C/I – Defend systems & info – AT: CIA triad**

#### Cybersecurity is a state whereby systems and information are defended against damage, unauthorized use, or exploitation --- Kosseff bases this definition on legal documents and policy

Jeff Kossef 16, Assistant Professor of Cybersecurity Law, United States Naval Academy. B.A., M.P.P., University of Michigan; J.D., Georgetown University Law Center, “The Cybersecurity Privilege”, Spring 2016, Ohio State Technology Law Journal, Vol. 12, p. 261 /lg

Cybersecurity is a relatively new concept for courts. Indeed, few U.S. courts have used the term, and none have articulated a common definition for cybersecurity. The Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS) offers a fairly comprehensive definition of cybersecurity: "[t]he 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." That definition, which is based on various documents and policies issued by Department of Homeland Security, National Institutes of Standards and Technology, and the White House, makes clear that cybersecurity includes the protection of both systems and information. This definition also correctly makes clear that cybersecurity is different from privacy, which NICCS defines as the "assurance that the confidentiality of, and access to, certain information about an entity is protected." Although cybersecurity can help to protect individuals' privacy, the terms are not interchangeable. Privacy involves assuring individuals that their personal data is protected, while cybersecurity more broadly encompasses the steps that a company takes to protect its systems and the information that is stored on those systems. If a company does not enact the necessary cybersecurity safeguards, then its consumers' and employees' privacy may be more likely to be at risk. Accordingly, companies are increasingly focusing on cybersecurity.

### 1AR---AT: CIA triad

#### We meet --- \_\_{area of aff found in card}\_\_\_ is specifically included within the CIA triad

Igor Nai-Fovino et al. 19, Scientific Project Manager with the Joint Research Centre in Ispra, Italy who was a Contractual Researcher with the University of Milano and received Ph.D. in computer security from the Università degli Studi di Milano, “A Proposal for a European Cybersecurity Taxonomy”, 2019, European Comission (executive body of the EU) /lg

Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network [SOURCE ISO/IEC TR 29181-5]. Information Security in the network context deals with data integrity, confidentiality, availability and non-repudiation while is sent across the network. A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. In this context cybersecurity deals with all the aspects of computation, coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.

Network security (principles, methods, protocols, algorithms and technologies);

Distributed systems security;

Managerial, procedural and technical aspects of network security;

Requirements for network security;

Protocols and frameworks for secure distributed computing;

Network layer attacks and mitigation techniques;

Network attack propagation analysis;

Distributed systems security analysis and simulation;

Distributed consensus techniques;

Fault tolerant models;

Secure distributed computations;

Network interoperability;

Secure system interconnection;

Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication);

Network steganography.

#### The CIA triad interp is too vague, unnecessarily broad, and impedes the success of cybersecurity operations

Derek E. Bambauer 15, Professor of Law at the University of Arizona, where he teaches Internet law and intellectual property (covers Internet censorship, cybersecurity, and intellectual property) + was a Research Fellow at the Berkman Center for Internet & Society at Harvard Law School, “Conundrum”, 04/11/2015 revision date (originally published 4/11/2011), Minnesota Law Review, Vol. 96, p. 584 /lg

Conceptualizing cybersecurity challenges policymakers and academics. 32 The current theoretical approaches to cybersecurity, though, have proved to be significantly flawed. They employ definitions that are vague and overbroad; they seek to force cybersecurity's issues into the straitjackets of existing doctrines poorly suited to cybersecurity's problems; and they produce concomitant policy recommendations that not only fail to mitigate, but actually worsen, the Internet's security challenges.

Conventional wisdom on cybersecurity identifies the problem as all-encompassing. 33 Scholars, government officials, and journalists tend to view cybersecurity as the "protection of all things Internet" 34 - an approach that impedes practical progress by failing to set priorities. Government efforts at capturing cybersecurity's scope have been particularly overbroad. [\*592] President Barack H. Obama's Cyberspace Policy Review offers a representative definition, where cybersecurity is:

strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. 35

Presidential policies have been strikingly consistent. President Barack Obama's approach to cybersecurity is almost identical to the Comprehensive National Cybersecurity Initiative (CNCI), the strategy employed by Obama's Republican predecessor, President George W. Bush. 36 Their cybersecurity definitions and programs are closely aligned; indeed, Richard Clarke and Robert Knake call Obama's plan "CNCI redux." 37 Both policies build on the recommendations and definitions (in particular, of critical infrastructure) of President William J. Clinton's Commission on Critical Infrastructure Protection. 38 Regardless of political affiliation, American Presidents have taken an expansive view of cybersecurity.

Proposed federal legislation is equally capacious in approach. The National Cyber Infrastructure Protection Act of 2010 defines "cyber security activities" as:

[\*593]

a class or collection of similar cyber security activities by a Federal agency that involves personally identifiable data that is -

(A) screened by a cyber security system outside of the Federal agency …

(B) transferred, for the purpose of cyber security, outside such Federal Agency; or

(C) transferred, for the purpose of cyber security, to an element of the intelligence community. 39

The Act conceives of cybersecurity not only broadly - it could include the Federal Trade Commission's anti-spam efforts, for example - but recursively. 40 The Protecting Cyberspace as a National Asset Act of 2010 defines "information security" as "protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide" integrity, confidentiality, and availability. 41 The Homeland Security Cyber and Physical Infrastructure Protection Act of 2011 proposes cybersecurity requirements that cover "an occurrence that jeopardizes the security of data or the physical security of a computer network owned or operated by a Federal agency or covered critical infrastructure," 42 where critical infrastructure includes private sector computer systems identified by the Department of Homeland Security. 43 In short, for government policymakers, there is little that cybersecurity does not cover.

Similarly, legal scholars define the concept expansively. Gus P. Coldebella and Brian M. White see cybersecurity as encompassing "criminality of all stripes, nation state and corporate espionage, and attacks," even while they decry term-creep in the concept. 44 Sean M. Condron, of the U.S. Army's Judge Advocate General's Legal Center and School, 45 defines [\*594] the problem as attacks on critical infrastructure by "terrorists, nation-states, terrorist sympathizers, and thrill seekers," 46 where critical infrastructure comprises networked computer systems "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 47 Susan Brenner, in her Article classifying cybersecurity risks based on the actor's intent, defines cyberthreats as those "using computer technology to engage in activity that undermines a society's ability to maintain internal or external order." 48 Milton L. Mueller decries the fact that "the term security now encompasses a host of problems, perhaps too many to fit properly under one word." 49 However, he then proposes a governance-based approach to cybersecurity without offering a coherent definition of the term, and includes spam, phishing, and surveillance as representative threats. 50

Even scholars who purportedly focus on narrower aspects of cybersecurity employ commodious definitions. Kelly Gable, who concentrates on cyberterrorism, defines it as "efforts by terrorists to use the Internet to hijack computer systems, bring down the international finance system, or commit analogous terrorist actions in cyberspace." 51 A 2001 report by Steven A. Hildreth of the Congressional Research Service describes cyberwarfare as "various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same." 52 Brenner defines cybercrime as "the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order." 53 Richard Clarke, former Special Advisor on Cybersecurity to President George W. Bush, and co-author Robert Knake even conceive of cybersecurity as encompassing [\*595] intellectual property theft. 54 These definitions of cybersecurity are vague, overbroad, and not helpful. Each attempt at framing the cybersecurity problem implicitly sets a standard for addressing the problem, for prioritizing it relative to competing concerns, and for measuring progress. Inaccurate cybersecurity definitions impede these efforts.

Conceptual failures - shortcomings in theoretical orientation - are largely to blame for what all commentators agree is an utter lack of success in improving cybersecurity. 55 Legal scholarship has thus far approached cybersecurity questions from within well-established, comfortable, yet poorly fitting models from criminal law, national security law, and military law. These doctrinal frameworks push scholars to concentrate upon the identity of actors behind a cyberthreat, and to determine their intent. 56 The problem is that the Internet's design makes attribution extremely difficult. 57 Tracing an attack to a given computer is challenging; deciphering who operated that computer during the attack is harder yet; and discerning motive can be nearly impossible. 58 The chief culprit, for most [\*596] scholars, is the lack of an authentication mechanism in the Internet's core TCP/IP protocols. 59 The Internet routes data in best-efforts fashion, regardless of who sent it. 60 Indeed, there is simply no way to verify a sender's identity under TCP/IP; functions such as authentication and error-checking are left to higher-level network layers and applications. 61 This default setting, which permits unattributed communication, is frequently exploited by malefactors - Internet traffic can be generated by botnets of suborned computers available for rent, or from computers specifically compromised for purposes of an attack. 62

Recent cybersecurity incidents illustrate the problem. The cyberassault on Estonia during that country's conflict with Russia in May 2007 originated in part from computers located in Brazil and Vietnam. 63 The July 2009 denial of service attack against South Korea and the U.S., widely attributed to North [\*597] Korea, 64 was launched from computers in Austria, Georgia, Germany, and even South Korea and America. 65 In both cases, initial judgments that a State (Russia or North Korea) was responsible dissolved into uncertainty in the face of mixed evidence. Attribution is thus an intolerably hard problem for conventional legal approaches. Worse, it is one that flows directly from the architecture of the Internet. 66

Unsurprisingly, the predominant answer to this perceived shortcoming is to retrofit attribution capabilities into the core of the Internet. Clarke and Knake want to move to new networks where "the user's authenticated identity could be embedded in each packet." 67 Jeffrey A. Hunker too believes that the "existing Internet architecture is fundamentally insecure." 68 He seeks to replace the Internet with a network that allows "different governments to have different rules," where governments "protect their citizens on the Internet the same way they protect them" in other media. 69 Former Director of National Intelligence Mike McConnell argues "we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment … more manageable." 70 Former CIA Director Michael V. Hayden proposes creating a new, "hardened enterprise structure" for the Internet that [\*598] would embed identification capabilities into its architecture. 71 Stuart Biegel states that "code-based adjustments in Internet architecture … can go a long way toward countering cyberterrorism." 72 Greater attribution enables the traditional practice of deterrence, along with traditional distinctions among criminals, terrorists, soldiers, and spies. 73 By building strong attribution into networking protocols, lawyers (and their governments) can apply time-tested ways of thinking and reacting to threats online. However, trying to redesign the architecture of the Internet as a solution has at least three critical shortcomings: difficult implementation, unintended consequences, and loss of generativity.

#### Cybersecurity only requires one tenet of the CIA triad

Christian Calliess & Ansgar Baumgarten 20, Professor for Public and European Law at Freie Universität Berlin, holder of an Ad Personam Jean-Monnet-Chair, and previous Legal Adviser to the European Political Strategy Center (EPSC), advising and working under the authority of its President Jean-Claude Juncker & PhD candidate and scientific assistant for Dr. Calliess at Freie Universität Berlin, “Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective”, 2020, German Law Journal, Vol. 21, p. 1149 /lg

Alongside space, air, land, and sea, cyber is the fifth dimension. It opens a global virtual world, radically changing societies and shaking classical borders. But a digital world also comes with new types of micro threats on businesses and citizens, and macro threats on public policies and state security, which are asymmetrical, unpredictable, and unaffected by classical state responses. They occur at [\*1150] the level of tricksters and range up to state espionage and, potentially, offensive cyber-attacks against states. Cyber is as such a new global world, where there is no dividing line between external and internal security. There is an attacker in one country, aiming for a target in another, causing damage in yet a third. There are as well large-scale attacks targeting and affecting several Member States at once--with the actual attack being carried out in cyberspace, which does not even adhere to one spot, country, or continent, but is a dimension for itself. This raises the question of the adequacy, or inadequacy, of the classical regulatory tools to reply to these challenges.

In this new environment, the EU and its Member States need to anticipate and plan for hitherto unimaginable scenarios in which they would be put if under a severe cyber-attack. This is particularly true for the implementation of the European Commission's EU Digital Single Market agenda. With the financial industry at its very center, a digital single market for the free movement of persons, services, and capital is highly dependent on a reliable and robust IT infrastructure. Comparable to the field of "industry 4.0," innovation in the financial sector--for example, the idea of a "Digital City," a financial platform of Europe that coordinates a network of financial centers in the EU --and the success of new business models depend on trust in a safe digital environment.

Cybersecurity is a term that covers a wide range of activities. Broadly speaking, it can be divided into three different categories: Network and information security, fight against cybercrime, and cyber defense. With regard to network and information security, cybersecurity can be defined as the ability of network and information systems to resist action that compromises the availability, authenticity, integrity, or confidentiality of digital data or the services those systems provide. This Article will focus on cybersecurity in the financial sector in its dimension of network and information security. Still, it will also refer to the other two areas of cybersecurity where necessary and appropriate. The financial sector is understood as the entirety of payment systems, credit institutions, payment institutions, stock exchanges, trade repositories, central securities depositories, central counterparty clearing houses, securities settlement platforms, credit rating agencies, insurance companies, and asset management companies.

#### Only one part of the CIA triad is necessary to constitute a cyberattack --- and, it’s not a triad at all --- the fourth category is authentication

William L. Painter 17, Specialist in Homeland Security and Appropriations, “Selected Homeland Security Issues in the 115th Congress”, 05/11/2017, Congressional Research Service, <https://crsreports.congress.gov/product/pdf/R/R44847> /lg

Defining Cybersecurity

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750) The United States government does not have a single definition describing cybersecurity. However, the Commission on Enhancing National Cybersecurity’s “Report on Securing and Growing the Digital Economy” offers the following:

The process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.277

The concepts of “confidentiality,” “integrity,” and “availability” are defined in U.S. Code as part of the “information security” triad. “Confidentiality” means that data is known only to authorized parties, “integrity” means that data is known to those parties in the manner they intend and not altered by another, and “availability” means that the data is available for access by those parties when they choose. These terms apply to the data stored, processed and transmitted by information technology (IT) systems, but also to the IT systems themselves. Growing in importance is a fourth term for information security—“authentication”—or the ability to confirm that parties using a system and accessing data are who they claim to be and have legitimate access to that data and system.

With the information security framework, cyberattacks can be categorized by what the attack compromises. For example, a data breach compromises confidentiality of information, malware that instructs a system to take an action the user did not authorize compromises integrity, and a denial of service attack compromises the availability of information.

### 2AC---AT: A lot

#### [x] DA---[x]. (highlight it for whatever definition they’re reading)

Dan Craigen et al. 14, Director of Carleton University's Global Cybersecurity Resource, former science advisor for the Government of Canada and former President of ORA Canada, October 2014, “Defining cybersecurity”, https://www.timreview.ca/article/835, Technology Innovation Management Review \\SYang

|  |  |  |
| --- | --- | --- |
|  | **Participant Working Definitions** | **Critique(s)** |
| 1 | “Cybersecurity is the protection of information/data, assets, services, and systems of value to reduce the probability of loss, damage/corruption, compromise, or misuse to a level commensurate with the value assigned.” | In the main, the feedback suggested that the inclusion of value introduced the human concepts related to security, but that the definition was too prescriptive and suffered the problem of a restrictive "listing" of what is being protected. |
| 2 | “Cybersecurity is a collection of interacting processes intended to protect cyberspace and cyberspace-enabled systems (collectively resources) from intentional actions designed to misalign actual resource property rights from the resource owner perceived property rights.” | This definition introduced the emerging cyber-physical environment and included the important concept of control over property rights. However, the definition’s focus on "human intentional actions" was viewed as being overly restrictive. |
| 3 | “Cybersecurity is a collection of interacting processes intended to make cyberspace safe and secure.” | Specifically intended to be broader than the seed definition, this definition introduced more problems than it solved because it was unnecessarily broad and introduced the contested notion of safety with security. |
| 4 | “Cybersecurity is a domain dedicated to the study and practice of the protection of systems or digital assets from any action taken to impose authorization on those systems or digital assets that do not align with the property rights of the resource facility as understood by its owner.” | In this definition, the concepts of property rights and control were introduced. However, there were concerns about the potential implications of "action taken" to mean limiting cybersecurity to human actors. Also there were concerns regarding the terms, which imposed limits on the scope of the definition such as "study" and "practice", thereby situating the issues largely within the academic domain. |
| 5 | “Cybersecurity is the state in which power over the execution of computers (sensu lato) and over information in the control of computers is where it should be.” | This definition reinforced the notions of control over information and systems. The main criticism was defining cybersecurity as a state. |

### 1AR---Cybersecurity---Reasonability

#### SPECIFICALLY in the field of cybersecurity our arguments about substance crowd-out are true.

Robert Dewar 14, Senior Researcher on the Cyber Defense Project at the CSS, 2014, "The "Triptych" of Cyber Security", https://www.academia.edu/9034642/The\_Triptych\_of\_Cyber\_Security?email\_work\_card=thumbnail, 6th International Conference on Cyber Conflict, accessed 7-7-2022 \\SYang

In the ﬁeld of cyber security, ill-deﬁned concepts and inconsistently applied terminology are further complicating an already complex issue. This causes difﬁculties for policy-makers, strategists and academics. Using national cyber security strategies to support current literature, this paper undertakes three tasks with the goal of classifying and deﬁning terms to begin the development of a lexicon of cyber security terminology. The ﬁrst task is to offer for consideration a deﬁnition of “active cyber defence” (ACD). This deﬁnition is based upon a number of characteristics identiﬁed in current academic and policy literature. ACD is deﬁned here as the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network. Once deﬁned, ACD is contextualised alongside two further approaches to cyber defence and security. These are fortiﬁed and resilient cyber defence, predicated upon defensive perimeters and ensuring continuity of services respectively. This contextualisation is postulated in order to provide more clarity to non-active cyber defence measures than is offered by the commonly used term “passive cyber defence”. Finally, it is shown that these three approaches to cyber defence and security are neither mutually exclusive nor applied independently of one another. Rather they operate in a complementary triptych of policy approaches to achieving cyber security.

## 1NC---Info Warfare Not Cybersecurity

#### The DOD defines “cybersecurity” and “information warfare” as distinct activities

Catherine A. Theohary 18, Information Operations and National Security Specialist at Congressional Research Service, “Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues,” Congressional Research Service (CRS) <https://crsreports.congress.gov/product/pdf/RL/RL31787> //chico

IO = Information Operations

IW = Information warfare

Cyberspace presents a force multiplier for IW activities. Social media and botnets can amplify a message or narrative, using all three elements of information to foment discord and confusion in a target audience.19 Much of today’s IW is conducted in cyberspace, leading many to associate IO with cybersecurity. Within DOD, however, IO and cyberspace operations are distinct doctrinal activities. Cyberspace operations can be used to achieve strategic information warfare goals; an offensive cyberattack, for example, may be used to create psychological effects in a target population. A foreign country may use cyberattacks to influence decisionmaking and change behaviors, for example the Democratic People’s Republic of Korea (DPRK)-attributed cyberattacks on Sony in late 2014. Cyber operations may be conducted for other purposes, such as to disable or deny access to an adversary’s lines of communication, or to degrade components of critical infrastructure that may be used for nefarious purposes.20

IO may be overt, such as a government’s production and dissemination of materials intended to convey democratic values. In this case, the government sponsorship of such activity is known. Covert operations are those in which government sponsorship is denied if exposed. The anonymity afforded by cyberspace can present an ideal battle space to conduct covert information operations. In addition, IO may take place outside of cyberspace.

Although several official documents now refer to “information warfare” in other countries, the United States has no formal government definition of IW. The DOD definition of information operations refers only to military operations and does not emphasize the use of cyberspace to achieve nonmilitary strategic objectives. Similarly, there is no commonly accepted definition of “cyberwarfare”; rather, the military refers to offensive and defensive cyberspace operations, with cyberspace as a warfighting domain or operating environment.

Cyberspace operations differ from information operations, which are specifically concerned with the use of information-related capabilities, such as military information support operations or military deception. Cyber-enabled information operations can be characterized as IO conducted in cyberspace. Just as IO carries its own doctrine and associated organizational structures, so do cyberspace operations, which are generally considered the purview of the United States Cyber Command.

#### Violation: The AFF is in the area of information operations NOT cybersecurity

#### Voting issue for limits and ground---any other interp justifies an infinite number tiny mechanisms that modify the information ecosystem and allows AFFs to spike out of core NEG generics.

## 2NC

### 2NC---OV

#### Our interpretation is that topical AFFs in the area of cybersecurity exclude information operations---info ops are distinct under the DOD and carries its own doctrine and organizational structures. That’s Theohary.

#### Prefer it:

#### 1---Limits---

#### 2---Ground---

### 2NC---AT: W/M

#### Information Warfare is not “cyberwar”

Catherine A. Theohary 18, Information Operations and National Security Specialist at Congressional Research Service, “Information Warfare: Issues for Congress,” Congressional Research Service (CRS) <https://crsreports.congress.gov/product/pdf/R/R45142> //chico

IW = Information Warfare

Information warfare is hardly a new endeavor. In the Battle of Thermopylae in 480 BC, Persian ruler Xerxes used intimidation tactics to break the will of Greek city-states. Alexander the Great used cultural assimilation to subdue dissent and maintain conquered lands. Military scholars trace the modern use of information as a tool in guerilla warfare to fifth-century BC Chinese military strategist Sun Tzu’s book The Art of War and its emphasis on accurate intelligence for decision superiority over a mightier foe. These ancient strategists helped to lay the foundation for information warfare strategy in modern times. Taking place below the level of armed conflict, information warfare (IW) is the range of military and government operations to protect and exploit the information environment. Although information is recognized as an element of national power, IW is a relatively poorly understood concept in the United States, with several other terms being used to describe the same or similar sets of activity. IW is a strategy for using information to pursue a competitive advantage, including offensive and defensive efforts. A form of political warfare, IW is a means through which nations achieve strategic objectives and advance foreign policy goals. Defensive efforts include information assurance/information security, while offensive efforts include information operations. Similar terms sometimes used to characterize information warfare include active

measures, hybrid warfare, and gray zone warfare.

IW is sometimes referred to as a “disinformation campaign,” yet disinformation is only one of the tactics used in information operations (IO). The types of information used in IO include propaganda, misinformation, and disinformation.

As cyberspace presents an easy, cost-effective method to communicate a message to large swaths of populations, much of present day information warfare takes place on the internet, leading some to conflate “cyberwarfare” with information warfare. While IO in the United States tends to be seen as a purely military activity, other countries and terrorist organizations have robust information warfare strategies and use a whole-of-government or whole-of-society approach to information operations.

### Cybersecurity – Excludes Info Sharing

#### Information sharing often weakens cybersecurity

Eli Dourado & Andrea O’Sullivan 15, Senior Research Fellow at the Mercatus Center at George Mason University and advisor to the State Department on international telecommunication matters who has served on several U.S. delegations to UN treaty and policy conferences & feature writer at the Mercatus Center at George Mason University, “’Information Sharing’: No Panacea for American Cybersecurity Challenges”, 06/22/2015, Mercatus Center at George Mason University, <https://www.mercatus.org/publications/technology-and-innovation/%E2%80%9Cinformation-sharing%E2%80%9D-no-panacea-american-cybersecurity> /lg

Information sharing initiatives are not novel. A 1998 presidential order authorized the formation of public-private partnerships to share threat information within critical infrastructure industries. Dozens of such Information Sharing and Analysis Centers (ISACs) have coordinated cyberthreat information flows among public and private entities since that time. Additionally, at least 20 federal offices already carry out missions that prioritize information sharing and public-private cybersecurity coordination. The National Cybersecurity and Communications Center (NCCIC), a DHS cyberthreat coordination center, houses the US Computer Emergency Response Team (US-CERT), which has served as the primary cyberthreat collection, assistance, and notification center since it was founded in 2003. President Obama created the CTIIC in February 2015 to advance information sharing goals along with the NCCIC, the Federal Bureau of Intelligence’s National Cyber Investigative Task Force, DOD’s US Cyber Command, and “other relevant United States Government entities”—which could amount to several dozen offices. Such overlapping roles and unclear lines of communication results in waste, inefficiency, and poorer security outcomes.

Despite the ample resources devoted to this task, the federal government has struggled to effectively collect and share incident information internally and with the private sector. ISACs can cease to operate if members do not actually share valuable information. A DHS Inspector General Report finds that the NCCIC faces large challenges in effectively sharing information among the appropriate parties. As of October 2014, the NCCIC had not even developed a common incident management system to coordinate information sharing—five years after being formed to do so. US-CERT has yet to develop performance metrics to gauge and improve effectiveness, despite serving as the main federal cybersecurity consultant for over a decade. Additionally, private sector threat analysis efforts often outpace US-CERT in breach notification. Indeed, DHS has at times been unable to even adequately share threat information within its own offices. In March 2013, DHS’s own US-CERT issued a warning about Windows XP vulnerabilities to government and private sector partners. But by November of that year, DHS’ Inspector General reported that several DHS computers were still running a vulnerable version of Windows XP, even after other DHS representatives ensured they had stopped running that version.

The Congressional Research Service notes “greater information sharing may, in some instances, effectively weaken cybersecurity by creating an overwhelming amount of information, eliminating the capacity to pay attention to truly important alerts.” The federal government sought to overcome this challenge by developing technological tools to surveil network activity, called the “EINSTEIN” projects, yet these projects often run over cost and perform worse than anticipated. Indeed, the EINSTEIN projects failed to identify the recent OPM hack. However ambitious their design, these programs have so far proven too technologically crude to handle the complex central identification and communication efforts intended to protect federal systems. There may never be enough EINSTEINs in the world for DHS, DOD, and DOJ to adequately coordinate and respond to the massive amounts of private data that would be collected under CISA.

#### Cybersecurity solely refers to technical features

Rand Waltzman 17, Senior Information Scientist for the RAND Corporation, Testimony from Senate Armed Services Subcommittee on Cybersecurity Hearing; "Cyber-Enabled Information Operations."; Congressional Documents and Publications //chico

The General Threat

Traditionally, "information operations and warfare, also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent." n4 This definition is applicable in military as well as civilian contexts. Traditional techniques (e.g. print media, radio, movies, and television) have been extended to the cyber domain through the creation of the Internet and social media.

These technologies have resulted in a qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation. The ability to influence is now effectively "democratized," since any individual or group can communicate and influence large numbers of others online. Second, this landscape is now significantly more quantifiable. Data can be used to measure the response of individuals as well as crowds to influence efforts. Finally, influence is also far more concealable. Users may be influenced by information provided to them by anonymous strangers, or even by the design of an interface. In general, the Internet and social media provide new ways of constructing realities for actors, audiences, and media. It fundamentally challenges the traditional news media's function as gatekeepers and agenda-setters. n5

Interaction within the information environment is rapidly evolving, and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defenses.

The information environment can be broadly characterized along both technical and psychosocial dimensions. Information environment security today (often referred to as cybersecurity) is primarily concerned with purely technical features--defenses against denial-of-service attacks, botnets, massive Intellectual Property thefts, and other attacks that typically take advantage of security vulnerabilities. This view is too narrow, however. For example, little attention has been paid to defending against incidents like the April 2013 Associated Press Twitter n6 hack in which a group hijacked the news agency's account to put out a message reading "Two explosions in the White House and Barack Obama is injured." This message, with the weight of the Associated Press behind it, caused a drop and recovery of roughly $136 billion in equity market value over a period of about five minutes. This attack exploited both technical (hijacking the account) and psychosocial (understanding market reaction) features of the information environment.

## Affirmative

#### They’re not mutually exclusive

Laura B. West 21, Judge Advocate in the U.S. Army and currently serves as the Deputy Chief of National Security Law at U.S. Cyber Command, “ARTICLE: BEYOND FIGHTING WORDS: RECONCEPTUALIZING INFORMATION WARFARE AND ITS LEGAL BARRIERS,” National Security Law Journal, 8, 162. //chico

This article's focus on a data-centric solution to information warfare by no means suggests neglecting network-centric efforts. On the contrary, cybersecurity and data security need to be viewed as mutually reinforcing mechanisms to solving the information warfare problem. Discussing the needed reform and issues revolving around cybersecurity is, however, outside the scope of this article.

#### Cybesecurity goes beyond technical vulnerabilities---includes disinfo

Scott J. Shackelford 13 Assistant Professor of Business Law and Ethics, Indiana University, Kelley School of Business. INTEROPERABILITY IN AN INTERCONNECTED WORLD: ARTICLE: TOWARD CYBERPEACE: MANAGING CYBERATTACKS THROUGH POLYCENTRIC GOVERNANCE, 62 Am. U.L. Rev. 1273 //chico

E. The Cyberthreat in Internet Governance

On February 2, 2012, FBI Director Robert Mueller told a U.S. House Committee, "the cyberthreat will equal or surpass the threat from counter terrorism in the foreseeable future." 120 The elements comprising the cyberthreat are complex. No system is secure in an absolute sense. It is possible to covertly raid and damage even the most protected computer networks for those with the will, resources, and patience to commit such acts - cybersecurity is a continuum in which all users are at some degree of risk. Technical vulnerabilities, though, are only part of the story of the cyberthreat. Other confounding variables include the fact that the applicable international law is often ambiguous or non-binding, while regulators must keep pace with advancing technology that is continually changing the threat matrix. 121 Developments in cybersecurity and data monitoring are also allowing for increased national regulation and censorship of the Internet. 122 This trend toward Internet sovereignty discussed in Part II is pitted against a history of a more hands-off approach to Internet governance and complicates efforts to address cybersecurity challenges. 123 To meet the diverse elements of the cyberthreat, some commentators have moved from a one-size-fits-all approach to a tiered model, parsing out cyberattacks based on the attacker's motive and means into the categories of cyberwar, cybercrime, cyberespionage, and cyberterrorism. 124 These categories help define policy and legal responses to cyber-related incidents, but problems of overlap, attribution, and other challenges curtail their utility. 125 The following subsections briefly unpack the cyberthreat and underscore the extent to which these collective action problems thwart attempts at management.

1. Cyberwar

Definitions vary, but cyberwarfare generally refers to an attack by one hostile nation against the computers or networks of another in order to cause disruption or damage, as compared to a criminal or terrorist attack, which involves a private actor. 126 Such attacks are known as "informationalized warfare" in China. 127 From a U.S. military perspective, cyberwar falls under "information operations," 128 which includes computer network defense and exploitation involving the offensive and defensive use of IT to protect critical national infrastructure and eliminate cyberthreats to Department of Defense (DoD) computers or networks. 129 The specific doctrine of cyberwar is a classified and evolving topic in U.S. defense circles, but the prevailing military doctrine calls for "U.S. dominance" across all "domains of warfare," including cyberspace. 130 This entails the U.S. military having "freedom of access to and use of" cyberspace while denying that freedom to adversaries. 131 Both the UK Ministry of Defense and the U.S. Joint Forces Command are working to preserve access to cyberspace. 132 Still, a genuine cyberwar has yet to take place, even though cyberweapons are being developed worldwide without transparent discussions about the circumstances in which they may be used. Thus, "cyberwarfare" has become a catchall term that does not explain cyberattacks in general. Similarly, the term "cyberattack," used throughout this Article, is commonly invoked by the media, but should not be confused with an "armed attack," which activates the law of armed conflict. 133 Indeed, a traditional war framework is inappropriate for managing most cyber-related incidents. This makes defining the line between cyberwar, cyberespionage, cybercrime, and cyberterrorism all the more important.

## 1NC---Cybersecurity – Strengthen Systems

#### ‘Cybersecurity’ is defined as strengthening systems

Newton and Hogan ’15 [Elaine; Michael; December 2015; Newton, PhD in Engineering and Public Policy at Carnegie Mellon University; Hogan, Distinguished Graduate of the Infantry Officer Candidate School, electronics engineer at NIST; “Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity,” National Institute of Standards and Technology, U.S. Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf> //smarx, AZG]

Cybersecurity is defined as 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.

#### Violation – The AFF aligns capabilities, that’s not strengthening systems

#### Voting issue for

#### 1 – Limits – endless mechanisms explode the topic

#### 2 – Ground – Miniscule AFF’s that align ‘capabilities’ skirt already weak neg ground based off tradeoff and enforcement

## 2NC – OV

#### Topical AFF’s must strengthen cyberspace systems. They violate by [xyz]

#### They justify AFF’s that could reduce the amount of resources we spent on EDT or cooperated to change military authorization and solve miniscule ambiguity problems with some random NATO article – the possibilities are endless. We ensure stable, big AFF’s that actually link to DA’s like PGM’s and Space Asset AFF’s, that’s best for

#### 1 – Limits – Endless mechanisms explode the NEG research burden. Confining the topic into one stable mechanism makes debate playable on an already miserable topic without any real uniqueness – AFF teams can leverage the strategic concept and Ukraine situation to get out of most situations

#### 2 – Ground – The AFF’s described above prove that they WILL skirt every DA link – strengthening systems means you must spend time and money, so we get tradeoff and enforcement DA’s

### 2NC – Cybersecurity – Strengthen Systems

#### Cybersecurity is strengthening the security and resilience of cyberspace

Wallace ’No Date [Matthew; Certification in Cybersecurity: Technology, Application, and Policy from Massachusetts Institute of Technology Professional Education, Professional Member Association of Computing Machinery; “Glossary of Terms,” Internet Salmagundi, <https://internet-salmagundi.com/glossary-of-terms-tag-terms/> smarx, AZG]

CyberSecurity is strengthening the security and resilience of cyberspace:

CyberSecurity at the federal level includes: Combating Cyber Crime, Securing Federal Networks, Protecting Critical Infrastructure, Cyber Incident Response, Cyber Safety, Cybersecurity Governance, Cybersecurity Insurance, Cybersecurity Jobs, Cybersecurity Training & Exercises, Information Sharing, Stakeholder Engagement and Cyber Infrastructure Resilience.

—U.S. Dept. of Homeland Security – CyberSecurity overview, “Cybersecurity“

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

—U.S. Dept. of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA), “Cybersecurity, Overview“

Internet Security deals specifically with networks and so is a subset of Cybersecurity.

Three elements are key to any definition of security: 1) Confidentiality, 2) Integrity, and 3) Availability.

### Violation – Interoperability

#### Interoperability is for exchanging info, NOT strengthening systems – they are at best effects T

Oxford Learner’s Dictionaries ’No Date [“Interoperability noun,” <https://www.oxfordlearnersdictionaries.com/us/definition/english/interoperability> //smarx, AZG]

​interoperability (between/with something) the ability of computer systems or programs to exchange information

#### Interoperability refers to how things can be used together

Cambridge Dictionary ’No Date [“Interoperability,” <https://dictionary.cambridge.org/us/dictionary/english/interoperability> //smarx, AZG]

the degree to which two products, programs, etc. can be used together, or the quality of being able to be used together:

### **Violation – Cohesion – Strengthen Systems**

#### Extensive findings prove that cohesion is about synergy, NOT strengthening systems

Bazin ’17 [Aaron; 09/27/17; Graduate Certificate in Blockchain Strategy from the University of Oxford, PsyD from the University of Rockies; and Dominika Kunertova, PhD in Political Science from Université de Montréal with specialization in Security Studies, Senior Researcher at the Center for Security Studies in fields like security cooperation; "An Alliance Divided? Five Factors That Could Fracture NATO," Army University Press, [https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/An-Alliance-Divided-Five-Factors-That-Could Fracture-NATO/](https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/An-Alliance-Divided-Five-Factors-That-Could%20Fracture-NATO/) smarx, AZG]

In making sense of Alliance cohesion in the future, this study first refined the understanding of cohesion itself. The findings indicate that NATO’s cohesion means synergy and the ability of NATO nations to think and act together. That is, to develop shared interests, values, and common standards and rules, and to respond to problems as a united group. Relying on mutual trust, cohesion is “doing what is best for the community” and looking beyond self-interests. Building on the analogy of ties between family members, the participants stated that cohesion is an expression of staying together despite differences, of “something bigger than ourselves.” One participant believed that “without cohesion, the Alliance would implode.”

#### NATO’s cohesion means unity

Mierzwa ’21 [Danuta; 09/30/21; General Tadeusz Kościuszko Military University of Land Forces; and Marek Tomaszycki, General Tadeusz Kościuszko Military University of Land Forces; "Imperial policy of the Russian Federation versus cohesion and coherence of NATO’s new strategic concept," SpringerLink, <https://link.springer.com/article/10.1057/s41311-021-00332-1> //smarx, AZG]

NATO’s cohesion means a level of political and ideological unity as well as solidarity between the members of the Pact. It mainly refers to the principles on which the Alliance is based. This is particularly true of the Member States’ commitment to collective defence, threats and challenges facing the Alliance.

### Violation – OCO’s

#### The AFF is NOT strengthening systems – they are at most effects topical

1AC Lewis ’15 [read yellow] [James; October; Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies; "THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO’S COLLECTIVE DEFENCE,” Tallin Paper No. 8, A NATO CCDCOE Publication on Strategic Cyber Security, https://www.ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf]

The central question for NATO’s cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend. Put another way, can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal? Offensive capabilities, unlike NATO’s current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction. The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term.

The US has always been overly secretive about its offensive cyber capabilities, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations.

Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that cyber attack is a “weapon” with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO’s defensive actions are not at all obvious, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO’s defensive activities, and NATO’s credibility in defence requires some public discussion on the use of offensive cyber operations.

There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the ability to deter cyber attack work best when embedded in a larger military force structure. Adding offensive cyber capabilities to NATO’s force structure and response doctrine will increase its deterrent capabilities – by how much is unclear, but what is clear is that a failure to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.5

Beyond deterrence, two other factors point to the need for additional consideration of NATO’s public posture on offensive cyber operations. The first is that cyber techniques are essential for the kinds of combat operations that NATO forces may carry out in the future. No modern air force would enter into combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support. The same is true for special forces operations. Offensive cyber capabilities will shape the battlefields of the future.

Second, NATO’s potential opponents will use cyber techniques in new ways, in what some have called “hybrid warfare”.6 These include countries traditionally of concern to NATO, but cyber threats could also come from new actors, such as Iran or North Korea, and proxy or non-state actors such as the Syrian Electronic Army. These nations and groups, using cyber techniques, now have new ways to strike NATO countries.

Military doctrine is changing as opponents seek to circumvent US military power and use a blend of political action and “influence operations”, special forces, proxies and irregular units, unconventional tactics and cyber techniques to apply force to gain their ends. Cyber techniques for political action and “influence operations” are not intended to destroy or disrupt, but rather to put coercive political pressure on targets. This new style of warfare will challenge planning for mutual defence. For these reasons, the need for more than defensive or technical cyber capabilities will increase.7

#### OCO’s are for disrupting OTHER countries’ networks, NOT strengthening our own – here’s definitive evidence

Hanson ’18 [Fergus; 2018; Professional Fulbright Scholar based at Georgetown University working on the uptake of new technologies by the US Government, Fellow at Cambridge University’s Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies; and Tom Uren, Senior Fellow at ASPI, formerly of the Department of Defence and CSIRO; “Organization, Command and Approvals,” Australian Strategic Policy Institute, <https://www.jstor.org/stable/pdf/resrep23053.8.pdf> //smarx, AZG]

For the purposes of this policy brief, we use a draft definition that’s being developed as part of the Department of the Prime Minister and Cabinet’s Cyber Lexicon project. It defines offensive cyber operations as ‘activities in cyberspace that manipulate, deny, disrupt, degrade or destroy targeted computers, information systems, or networks’.7 Given the range of countries with varying capabilities and using examples from open sources, offensive cyber operations could range from the subtle to the destructive: removing computer accounts or changing passwords; altering databases either subtly or destructively; defacing web pages; encrypting or deleting data; or even attacks that affect critical infrastructure, such as electricity networks. Even though it may use the same tools and techniques, cyber espionage, by contrast, is explicitly designed to gather intelligence without having an effect—ideally without detection. The Global Commission on the Stability of Cyberspace has commissioned ASPI’s International Cyber Policy Centre to do further work on defining offensive cyber capabilities.

#### Even offensive cyber capabilities are about manipulating adversarial networks – NOT strengthening our own

Egloff ’21 [Florian J.; 10/26/21; DPhil in Cyber Security from the University of Oxford and Masters in International Relations from Geneva Graduate Institute; and James Shires,

Offensive cyber capabilities (OCCs) are the combination of people, technologies, and organizational attributes that jointly enable offensive cyber operations: the adversarial manipulation of digital services or networks. Most works on OCCs focus on their (de-)escalatory potential in terms of diplomatic tension, instability, or power. This article argues for a re-orientation toward the normatively prior question of their relative violence. It asks: how are OCCs integrated into violent state capacities and what are the consequences? The article proposes three logics of integration by which OCCs are included in violent state actions, in both repressive and interstate situations. These logics—substitution, support, and complement—weigh the benefits of using OCCs against an adversary instead of, as part of, and in addition to other means of violence, respectively. The article argues that the violence of OCCs depends on two things: first, whether one adopts a narrowly physical or a more expansive definition of violence and, second, which logic of integration governs their use. On a narrow definition of violence, substitutive and supportive uses of OCCs are less likely to be violent than conventional alternatives, and complementary uses of OCCs are not violent at all. On a wider definition, both substitutive and supportive uses of OCCs can lead to more violence than conventional alternatives, while complementary uses of OCCs are highly likely to increase violence overall. Acknowledging the different logics of integration for OCCs, and understanding their violent effects, has important analytical and policy benefits for global security studies.

### AT: CIA Triad = Arbitrary

#### Confidentiality, integrity, and availability are NOT arbitrary

#### [A] – Integrity is protecting the accuracy and completeness

Newton and Hogan ’15 [Elaine; Michael; December 2015; Newton, PhD in Engineering and Public Policy at Carnegie Mellon University; Hogan, Distinguished Graduate of the Infantry Officer Candidate School, electronics engineer at NIST; “Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity,” National Institute of Standards and Technology, U.S. Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf> //smarx, AZG]

Integrity, property of protecting the accuracy and completeness of assets;

#### [B] – Confidentiality is ensuring info is not made available

Newton and Hogan ’15 [Elaine; Michael; December 2015; Newton, PhD in Engineering and Public Policy at Carnegie Mellon University; Hogan, Distinguished Graduate of the Infantry Officer Candidate School, electronics engineer at NIST; “Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity,” National Institute of Standards and Technology, U.S. Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf> //smarx, AZG]

Confidentiality, property that information is not made available or disclosed to unauthorized individuals, entities, or processes;

#### **[C] – Availability is the property of being accessible and usable**

Newton and Hogan ’15 [Elaine; Michael; December 2015; Newton, PhD in Engineering and Public Policy at Carnegie Mellon University; Hogan, Distinguished Graduate of the Infantry Officer Candidate School, electronics engineer at NIST; “Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity,” National Institute of Standards and Technology, U.S. Department of Commerce, <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf> //smarx, AZG]

Availability, property of being accessible and usable upon demand by an authorized entity.

### AT: Precision

#### 1 – Debatability outweighs on a topic without a single DA – Ukraine and Stratcon should logically thump everything

#### 2 – We are precise:

#### A – Newton has a PhD and Hogan is a distinguished graduate and electronics engineer

#### B – Newton and Hogan have an intent to define

#### 3 – Their [x] evidence isn’t precise because [explain]

## Affirmative

### W/M – Interoperability – CI Strengthen Systems

#### W/M – Interoperability strengthens interconnection and cohesive work

#### **CE Noticias Financieras ’21** [07/27/21; “They publish regulations that strengthen interoperability in the Specialized National Justice System,” <https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=504c4553-9aa3-4d37-bac2-7e4b3ddcea32&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A637N-V4N1-DY1R-B1MG-00000-00&pdcontentcomponentid=443607&pdteaserkey=sr3&pditab=allpods&ecomp=rz2yk&earg=sr3&prid=dded7a6f-0446-49af-b709-4146c010cbd0> //smarx, AZG]

On Monday, the regulation that strengthens interoperability in the Specialized National Justice System (SNEJ) for the Protection and Punishment of Violence against Women and Members of the Family Group was published. The law includes a number of ombudsman's recommendations and will allow for more articulated work on the problem.

Supreme Decree 145-2021-PCM, which regulates Law No. 30926, seeks a harmonious and cohesive functioning of the existing processes and digital platforms of the SNEJ, composed of the Judiciary, the Public Ministry (MP), the National Police of Peru (PNP), the Ministry of Justice and Human Rights, and the Ministry of Women and Vulnerable Populations (MIMP).

The Ombudsman's Office highlighted the actions of the regulation that aims to establish measures to strengthen interconnection and cohesive work through digital platforms. These actions are considered fundamental in the care and prevention of gender violence, through an articulated reaction and with the speed that is required.

### W/M – Cohesion – Strengthen Systems

#### Cohesion can strengthen coordination

Potter ’19 [Pitman B.; 12/22/19; professor of law at the University of B.C. and a distinguished fellow at APF Canada; and Stewart Beck, President and CEO of the Asia Pacific Foundation of Canada; "Stewart Beck and Pitman Potter: Canada’s future China strategy must consider national interests, global challenges," Vancouver Sun, <https://vancouversun.com/opinion/op-ed/stewart-beck-and-pitman-potter-canadas-future-china-strategy-must-consider-national-interests-global-challenges> //smarx, AZG]

The West cannot turn back the clock. For good or ill China has arrived and we need to be on the front foot as opposed to simply reacting to decisions taken in Beijing or Washington. Implemented together, the principles of autonomy, national interests, and integrated cohesion can strengthen Canada's capacity to proactively co-ordinate and effectively manage relations with China. China can no longer be viewed in isolation from challenging global dynamics. Neither should Canada's China policies.

### W/M – OCOs – Strengthen Systems

#### W/M – OCO’s are defined to project power in or through cyberspace

NIST ’No Date [National Institute of Standards and Technology; “offensive cyber operations (OCO),” Information Technology Laboratory, Computer Security Resource Center, <https://csrc.nist.gov/glossary/term/offensive_cyberspace_operations> //smarx, AZG]

Definition(s): Cyberspace operations intended to project power by the application of force in or through cyberspace.

### 2AC – Cybersecurity – Protection

#### Cybersecurity is the protection of digital systems – here’s qualified and definitive evidence

Treacy ’18 [Mike; 03/30/18; Treacy, 20 years of cybsercurity expertise, CEO of Salt Cybersecurity; "E.M.M.A. International Consulting Group Inc. Welcomes Mike Treacy As Their Cybersecurity Practice Lead," E.M.M.A. International Consulting Group, Inc., a global leader in FDA compliance consulting, <https://www.benzinga.com/pressreleases/18/03/p11445925/e-m-m-a-international-consulting-group-inc-welcomes-mike-treacy-as-the> //smarx, AZG]

"We are extremely pleased to have a seasoned Cybersecurity subject matter expert like Mike join our team," said Dr. Carmine Jabri, CEO of E.M.M.A. International. "Mike brings 20 years of leading-edge cybersecurity expertise to our team. He has spent years working as an expert to advance the state of the art in information systems' security. He understands the concerns and needs of large and small businesses alike after having worked for small tech start-ups and Monster.com."

Cybersecurity can be defined as the protection of digital systems against theft and damage to hardware and software. As medical device innovation grows, as well as the use of digital systems to track health progress, E.M.M.A. International sees the importance of providing cybersecurity services to its clients.

### 1AR – Cybersecurity – Protection

#### ‘Cybersecurity’ means protection an info system from a threat

Johnson ’20 [09/04/20; Johnson, Committee on Science, Space, and Technology; “Grid Security Research and Development Act,” House of Representatives Congressional Session, Authenticated U.S. Government Information, <http://libproxy.law.umich.edu:2048/login?url=https://heinonline.org/HOL/P?h=hein.congrecreports/crptxadhi0001&i=1> //smarx, AZG]

CYBERSECURITY.-The term 'cybersecurity' means protecting an informa- tion system or information that is stored on, processed by, or transiting an in- formation system from a cybersecurity threat or security vulnerability.

#### More definitive evidence proves that cybersecurity includes info-protection

Nawaz ’19 [Saba; 10/07/19; Nawaz, M.A. in Mass Communication and Media Studies; “Cyber-security and its objectives,” The Express Tribune, <https://global-factiva-com.proxy.lib.umich.edu/ha/default.aspx#./!?&_suid=165705185115204300742750491586> //smarx, AZG]

Cyber security is one of the most fundamental security paradigms in today's modern warfare era. Countries should protect their own information assets, because in today's warfare everyone's rivalry tries and seeks to target their information system. This is an advanced strategy of states to overthrow their adversary by creating new cyber threats such as APTs. APTs are known as advanced persistent threats, which are highly complex threats and are very difficult to counter. Cybersecurity is a part of information security and can be defined as the protection of information assets by addressing threats to information processes, stored and transported by an internetworked information system. Cybersecurity usually refers to an entity initiating threats due to the existence of global cyberspace (i.e. internet). Cyber security requires stakeholders in the cyberspace area to be active in security, beyond the protection of their own assets.

# T-Maritime

# Neg

## 1NC

#### Interp: NATO Maritime Security is limited to conventional military operations and cyberspace

North Atlantic Treaty Organization, 22 (7/14/22; “NATO’s maritime activities” NATO <https://www.nato.int/cps/en/natohq/topics_70759.htm>; Accessed 7/16/22) //LVL

The 2011 Alliance Maritime Strategy derives four maritime roles for the Alliance to contribute to: deterrence and collective defence, crisis management, cooperative security and maritime security. Since 2014, the Alliance’s adaptation to the changed security environment has been pursued along two essential tracks: strengthening the Alliance’s deterrence and defence posture and enhancing NATO’s contribution to projecting stability. Reinforcement of the Alliance Maritime Posture is an integral and cross-cutting part of the implementation of these two tracks and was reconfirmed in the 2022 Strategic Concept. The Alliance Maritime Strategy describes NATO’s four strategic roles or what it does in the maritime domain. The Alliance Maritime Posture describes NATO’s functions or how it uses the maritime domain and the Alliance’s naval forces. NATO is strengthening its deterrence and defence posture in all domains. The maritime domain encompasses oceans and seas, on, above and below the surface, in all directions. It is a continuum and it is fully connected to other domains and areas. The Alliance’s naval forces include those maritime forces, sensors and other capabilities under national or NATO command that contribute to Alliance security. The Alliance Maritime Posture comprises the Alliance’s naval forces, their presence within the maritime domain and the operational and cooperative activities that they conduct in the performance of three functions, which contribute to Alliance security: Strategic function: the presence of maritime forces creates strategic and deterrent effects, including for assurance and messaging, and demonstrates NATO’s intent to operate without constraint and as required. The flexibility of maritime forces provides nearly instant availability of inherently tailorable force packages yielding a range of attractive, measured and viable political and military options. Security function: maritime security has become a mainstay of NATO’s maritime activities. Allies have developed sophisticated skills, tactics, techniques and procedures associated with maritime security. The maintenance of a safe and secure maritime environment can be undertaken through a range of maritime security operations and/or activities. Maritime forces can provide a ready and flexible mechanism and significant versatility for a broad range and scale of missions and tasks. Warfighting function: during peacetime and in a crisis, maritime forces are primarily deterrent in nature. They can contribute to conventional operations, nuclear deterrence and ballistic missile defence, to advance Alliance security interests. Allies’ maritime forces provide deterrence and defence in their contiguous seas, extending the defence of their national territory and can project power at distance. Maritime forces can rapidly transition from low-intensity to high-intensity missions and tasks. Surface, sub-surface and above-surface capabilities and forces work together to exercise sea denial or control, support reinforcement, protect assets, project power and support joint forces and joint effects. Maritime and joint exercises are key to maintaining and developing warfighting competencies and improving Allies’ combined maritime skills and readiness for all operations. Some areas and competencies being incorporated into future exercises include high-end warfighting capacities, such as the protection of sea lines of communication and rapid reinforcement, carrier strike, amphibious forces, anti-submarine warfare, land attack, deep-precision strike, and integrated air and missile defence; countering hybrid threats in the maritime domain; and countering threats in cyber space.

#### Violation – the aff expands maritime domain awareness to Artificial intelligence and biotechnology – that’s not under current NATO maritime domain awareness guidelines/activities

#### Voter for

#### Limits – they justify affs creating entirely new NATO guidelines and security objectives

#### Ground – avoids core neg generics that are based on existing NATO objectives

## 2NC

#### Maritime security cooperation is an extension of conventional forces

CJCS, 18 (6/8/22; “Joint Maritime Operations”; JCS <https://irp.fas.org/doddir/dod/jp3_32.pdf>) //LVL

Security cooperation tasks may include the use of coastal riverine, construction, EOD, mobile diving, intelligence, logistics, medical, and training resources. Maritime forces may also employ security cooperation MAGTFs to enhance civil-military operations or conduct security force assistance activities to build partner capability or capacity. The USCG’s Atlantic Area Command and Pacific Area Command have OPCON of the Coast Guard’s deployable specialized forces to provide specialized capabilities in incident response, maritime law enforcement, port security, and antiterrorism/counterterrorism and can be brought together for surge operations which can deploy in advance of a potential conflict to conduct prevention activities or, after a conflict has ensued, to compliment conventional forces and contribute to establishing and sustaining stability.

# Aff

## 2AC

#### W/M – Maritime domain awareness includes disruptive tech like AI

Sakhuja ’18 [Vijay; 06/11/18; MPhil and PhD degrees from the Jawaharlal Nehru University, Senior Fellow Gujarat National Law University, "Artificial Intelligence and Maritime Domain Awareness," Society for the Study of Peace and Conflict, <https://sspconline.org/index.php/opinion/artificial-intelligence-maritime-domain-awareness-vijay-sakhuja-110618> //smarx, AZG]

There are several disruptive technologies that find application in the maritime domain beyond warfighting. Among these Artificial Intelligence (AI), its cutting edge application in machine learning (ML), internet of things (IOT), big data, and blockchain can profoundly change the management of the maritime domain, including search and rescue, humanitarian assistance and disaster relief, combating illegal, unregulated and unreported (IUU) fishing, counter piracy, counter trafficking, environment protection and illegal migration, to name a few.

A robust AI based maritime domain awareness (MDA) can potentially contribute to transparency across the seas and oceans by integrating multi-source data, analytics and advanced Cloud services making data accessible much more easily. It is possible to track vessels, determine the type of cargo and even the business behavior of shipping companies, including freight forwarders.

An ideal AI-based MDA architecture could be built around numerous diversified technical devices and systems such as radar (ships, aircraft, shore), vessel monitoring systems (VMS), satellite supported systems (AIS and LRIT), UAVs, drones, imagery, open source intelligence (OSINT), etc. to generate data. Thereafter, advanced algorithms fuse data from different sources including data from vessel profile library developed from stored knowledge and provide automated threat evaluation or early warning on anomalous activities at sea, understand and quantify risks, and provide timely alerts of possible threats or suspicious ships before reaching their destinations. In essence, this helps to minimize information gap, thus limiting the number of vessels that require investigation.

The fishing industry, which has in recent times been under suspicion for engaging in IUU activities, can be monitored and tracked. AI enabled drones can recognize the identification number of the fishing vessel, count people on board, determine if it is inside a protected area and verify its permit. Google is already using the image-recognition technology in conjunction with AI to locate vessels engaged in IUU activity.

As far as search and rescue at sea is concerned, navies and coast guards are often pressed into operations to rescue fishermen during cyclones and hurricanes. It will be possible in the future for ships to launch autonomous vehicles to respond to emergencies to help locate and rescue victims that have been left stranded, immobile or are sinking.

Another interesting application of AI enabled drones is their use in safety of beach goers against sharks. For instance, in Australia, shark detection system powered by artificial intelligence will be able to deliver “live-video feed to a drone operator who then uses the shark-spotting software to identify sharks in real time and with more accuracy than the human eye.”

The maritime domain is in the cusp of a major transformation and disruptive technologies will be advanced to overtake the skill, ability and judgment of humans. The trends indicate that that day is not far when artificial intelligence would overtake human intelligence and smart tools will enable technology-driven management of information and intelligence and provide a comprehensive and credible real-time MDA.

So long as these transformations do not challenge the natural human values of empathy and compassion, they are welcome and must be harnessed to address and respond to illegal activities that challenge good order at sea. In this context, Google’s decision to abandon Project Maven is a welcome decision and is a trigger for exploiting disruptive technologies to deliver public goods and services at the seas.

#### CI: Maritime domain awareness is anything associated with security – that includes machine learning

Saildrone ’20 [10/20/20; "Machine Learning Will Automate Maritime Domain Awareness," <https://www.saildrone.com/news/ai-ml-maritime-domain-awareness-mda> //smarx, AZG]

Saildrone uncrewed surface vehicles (USVs) have conducted extensive data collection missions around the world, continuously collecting meteorological and oceanographic variables above and below the sea surface and building an unprecedented at-sea image library of some four million images. This image library is the foundation of Saildrone’s machine learning software, unlocking new maritime domain awareness (MDA) capabilities at sea, a challenging environment where every pixel is moving across every frame.

MDA is the effective understanding of anything associated with the safety and security of the global maritime domain—illegal fishing, drug enforcement, and limiting intrusion into protected marine sanctuaries. The United States Coast Guard was tasked with exploring the feasibility, costs, and benefits of improving maritime domain awareness using a low-cost autonomous system like the saildrone. Throughout the month of October, Saildrone is demonstrating how its platform could be used to conduct MDA missions offshore and in remote areas of the ocean.

Saildrone USVs are equipped with a specially built 360° camera system integrated with a GPU. Computer vision is based on deep neural networks; the patterns within the collected data set are represented by numbers, which in turn are mathematically mapped to define a model that a computer can be trained to recognize. Saildrone achieved this over several years, leveraging Amazon Web Services (AWS)’s industrial-strength large-scale cloud-based compute infrastructure.

The Saildrone MDA solution combines the cameras, automated identification system (AIS) receivers, and optional radar or infrared cameras for night-time capabilities. The cameras capture images on a very high frequency and the crucial ML software fuses the data from all sensors, recognizes and identifies targets of interest, and automatically alerts the end-user in real time.

Each vehicle can operate for up to 12 months at sea. They use wind power for forward propulsion and are virtually silent while operating, sailing autonomously from waypoint to waypoint. Alternately, saildrones can be tasked to sail in a “racetrack” formation or hold station. The key to machine learning is continuous training of the model; the more saildrones that are deployed and the longer they are deployed, the better the Saildrone model becomes.

During the October demonstration, a fleet of Saildrone USVs will illustrate a variety of use cases and real-world examples to show the system’s effectiveness for improving maritime domain awareness in remote areas of the Pacific Ocean.

## 1AR

#### International Maritime Organization defines Maritime domain awareness as anything relating to maritime security

International Maritime Organization, 18 (11/14/22; “Enhancing maritime domain awareness in West Indian Ocean and Gulf of Aden”; International Maritime Organization <https://www.imo.org/en/MediaCentre/Pages/WhatsNew-1203.aspx>) //LVL

Maritime domain awareness is the effective understanding of anything associated with the maritime domain that could impact security, safety, the economy or the marine environment.

## Neg Misc

### Interp – Businesses

#### Cybersecurity is action with companies and businesses

Vegas ’22 [Marta; 02/18/2022; Vegas, Postgraduate in journalism from the Complutense University of Madrid, Sustainability Leader for Telefónica Hispam; CE Noticias Financieras English, <https://advance-lexis-com.proxy.lib.umich.edu/document/?pdmfid=1516831&crid=b750326f-ba4a-49df-b2c5-2015b6b51d48&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A64TM-0W91-JCG7-83HX-00000-00&pdcontentcomponentid=443607&pdteaserkey=sr10&pditab=allpods&ecomp=rzznk&earg=sr10&prid=64c8643a-cdf9-4cf7-ac6e-b85a216a7f29> //smarx, AZG]

In an increasingly digital world in which we spend much of our time, it is essential to achieve greater and greater security. The term cybersecurity is generally associated with companies and businesses, as it has an important implication in terms of losses, costs and the number of threats they receive.