# MSDI Topicality



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

NFHS Caselist:

Artificial Intelligence: Restrict development and/or use of Lethal Autonomous Weapons (LAWs)

Biotechnology: Ban the use of germline genetic engineering in humans

Biotechnology: Substantially increase funding for vaccine research

Cyber: Ban offensive cyber operations

## Topic Specific Terms

### Artificial Intelligence

#### Artificial Intelligence

Cambridge Dictionary “Artificial Intelligence” <https://dictionary.cambridge.org/us/dictionary/english/artificial-intelligence> Accessed 10 June 2022 (jshock)

the [study](https://dictionary.cambridge.org/us/dictionary/english/study) of how to [produce](https://dictionary.cambridge.org/us/dictionary/english/produce) [machines](https://dictionary.cambridge.org/us/dictionary/english/atm) that have some of the [qualities](https://dictionary.cambridge.org/us/dictionary/english/quality) that the [human](https://dictionary.cambridge.org/us/dictionary/english/human) [mind](https://dictionary.cambridge.org/us/dictionary/english/mind) has, such as the [ability](https://dictionary.cambridge.org/us/dictionary/english/ability) to [understand](https://dictionary.cambridge.org/us/dictionary/english/understand) [language](https://dictionary.cambridge.org/us/dictionary/english/language), [recognize](https://dictionary.cambridge.org/us/dictionary/english/recognize) [pictures](https://dictionary.cambridge.org/us/dictionary/english/picture), [solve](https://dictionary.cambridge.org/us/dictionary/english/solve) [problems](https://dictionary.cambridge.org/us/dictionary/english/problem), and [learn](https://dictionary.cambridge.org/us/dictionary/english/learn)

#### Artificial Intelligence

Ed Burns “What is Artificial Intelligence (AI)?” <https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence> Tech Target Accessed 23 June 2022 (jshock)

Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Specific applications of AI include [expert systems](https://www.techtarget.com/searchenterpriseai/definition/expert-system), natural language processing, speech recognition and [machine vision](https://www.techtarget.com/searchenterpriseai/definition/machine-vision-computer-vision).

[Artificial neural networks](https://www.techtarget.com/searchenterpriseai/definition/neural-network) and deep learning artificial intelligence technologies are quickly evolving, primarily because AI processes large amounts of data much faster and makes predictions more accurately than humanly possible.

#### AI excludes machine learning

William Stanton, 2-24-2016, https://www.alphr.com/artificial-intelligence/1002792/what-is-ai-ten-things-you-need-to-know-about-the-future-of/, "What is AI? Ten things you need to know about the future of artificial intelligence," Alphr (ermo/sms, Acc:6-27-2022)

To truly understand what AI is, though, you need to appreciate the jargon that’s thrown around out there right now. For instance, you need to know that artificial intelligence is not the same as machine learning, despite the fact it’s regularly used as a synonym for it. The chief difference to remember is that machine learning is simply a process by which a computer can learn a skill, whereas artificial intelligence refers to a computer that can “think” for itself without being programmed to do so.

#### AI excludes robots – it supplements humans, not replaces us

Nirmal Narayanan, 2-19-2019, https://www.ibtimes.co.in/will-artificial-intelligence-take-away-jobs-humans-792246, "Will Artificial Intelligence take away jobs from humans?," IBTimes India (ermo/sms, Acc:6-27-2022)

As panic surrounding job loss due to artificial intelligence reaches new levels, experts have clarified that AI will not take away jobs from humans. Experts revealed that artificial intelligence is actually supplementing human intelligence all across the spectrum, and it will actually make the life of humans easy.

In a recent post written on Science Focus, Dr Peter Bentley, a British author and computer scientist based at University College London revealed that artificial intelligence is not the same as factory automation or robots. Bentley believes that AI is very similar to the internet, and it is basically an enabling technology which creates new jobs in various industries.

#### AI does not mean artificial consciousness

Brian Green, August 24, 2018 Director of Technology Ethics, Markkula Center for Applied Ethics, Faculty (adj.), School of Engineering, Santa Clara University https://www.academia.edu/40920739/Ethical\_Reflections\_on\_Artificial\_Intelligence, "Ethical Reflections on Artificial Intelligence," Scientia et Fides (ermo/sms, Acc:6-27-2022)

Artificial intelligence is not the same as artificial consciousness (artificial consciousness has sometimes been called “Artificial General Intelligence (AGI),” “Strong AI,” or “Full AI”). Some thinkers vehemently believe that artificial consciousness is possible (e.g., Chrisley 2008; Kurzweil 2012; Koene 2013; most contributors to Chella & Manzotti 2013), while others just as vehemently believe that it is impossible (e.g., Searle 1980; Schlagel 1999; and from a Catholic perspective: Labrecque 2017). I am agnostic on the subject, but I am sure of this: AI developers will certainly try to make an AI that simulates interaction with a human as closely as possible (see, for example, Google’s recent release of Duplex (Leviathan & Matias 2018)). In other words, the artificial construct, if very well done, will seem conscious. But will it be conscious, or will it only be a simulation? To me, there is no reason to believe that a close mimicry of consciousness is the same as consciousness any more than a close mimicry of anything (fill in the blank: forged money, forged artwork, actors imitating famous people, simulated gemstones, etc.) actually becomes the real thing. But the possibility of an exception remains, after all, some artificial gemstones, such as rubies and sapphire, really are molecularly identical to natural rubies and sapphires (both are the mineral corundum: aluminum oxide). Will consciousness be exactly duplicable, like corundum? I doubt it, but I cannot be certain.

### Lethal Autonomous Weapons:

#### Lethal Autonomous Weapons

Congressional Research Service 2020 “Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems” <https://sgp.fas.org/crs/natsec/IF11150.pdf> CRS (jshock)

Lethal autonomous weapon systems (LAWS) are a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system.

#### Autonomous Weapon Systems

UQ School of Law October 2020 “Autonomous Weapon Systems” <https://law.uq.edu.au/research/future-war/autonomous-weapon-systems#terms> The University of Queensland (jshock)

Likewise, different countries have adopted a range of differing criteria for designating a weapon system as ‘autonomous’. Some, notably the [United States](https://fas.org/irp/doddir/dod/d3000_09.pdf), use broad definitions which focus on the role of the human operator:

‘A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.’

#### Autonomous Capability can be defined with the highest level of autonomy and evolution

UQ School of Law October 2020 “Autonomous Weapon Systems” <https://law.uq.edu.au/research/future-war/autonomous-weapon-systems#terms> The University of Queensland (jshock)

Other countries use more restrictive definitions based on some threshold level of autonomous capability. China, in a [2018 position paper](https://unog.ch/80256EDD006B8954/(httpAssets)/E42AE83BDB3525D0C125826C0040B262/$file/CCW_GGE.1_2018_WP.7.pdf), proposed a set of criteria including lethality, a high level of autonomy (‘absence of human intervention and control during the entire process of executing a task’), ‘impossibility for termination’, ‘indiscriminate effect’ and ‘evolution, meaning that through interaction with the environment the device can learn autonomously, expand its functions and capabilities in a way exceeding human expectations’. No existing weapons fit that definition, nor are any likely to in the foreseeable future. The United Kingdom also [originally proposed](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644084/20110505-JDN_2-11_UAS_archived-U.pdf) very stringent criteria, although there are more [recent signs](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf) that their position may be [softening](http://www.article36.org/wp-content/uploads/2018/07/Shifting-definitions-UK-and-autonomous-weapons-July-2018.pdf).

### Biotechnology

#### Biotechnology

Merriam Webster “biotechnology” <https://www.merriam-webster.com/dictionary/biotechnology> Merriam Webster Dictionary Accessed 23 June 2022 (jshock)

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)

#### Biotechnology

Encyclopedia of Agriculture and Food Systems 2014 “Food Microbiology” <https://www.sciencedirect.com/science/article/pii/B9780444525123000590> Science Direct (jshock)

Biotechnology is defined as the use of live organisms or biological systems in industrial processes and waste treatment plants (Borem et al., 2003).

#### Biotechnology used to improve our lives and health of the planet

BIO “What is Biotechnology?” <https://www.bio.org/what-biotechnology> Biotechnology Innovation Organization Accessed 23 June 2022 (jshock)

At its simplest, biotechnology is technology based on biology - biotechnology harnesses cellular and biomolecular processes to develop technologies and products that help improve our lives and the health of our planet. We have used the biological processes of microorganisms for more than 6,000 years to make useful food products, such as bread and cheese, and to preserve dairy products.

Modern biotechnology provides breakthrough products and technologies to combat debilitating and rare diseases, reduce our environmental footprint, feed the hungry, use less and cleaner energy, and have safer, cleaner and more efficient industrial manufacturing processes.

#### Biotechnology exlucde food & drink development

West Virginia Code, Current through legislation effective April 26, 2022, Chapter 11 - TAXATION Article 13Q - ECONOMIC OPPORTUNITY TAX CREDIT Section 11-13Q-10a - Credit allowed for specified high technology manufacturers, 4-26-2022, https://casetext.com/statute/west-virginia-code/chapter-11-taxation/article-13q-economic-opportunity-tax-credit/section-11-13q-10a-credit-allowed-for-specified-high-technology-manufacturers, "Section 11-13Q-10a," No Publication (ermo/sms, Acc:6-27-2022)

(D) Biotechnology

(i) "Biotechnology" means scientific invention, processes and methods, or industrial invention, processes and methods, based on the science of biology, microbiology, molecular biology, cellular biology, biochemistry, or biophysics, or any combination thereof. Biotechnology includes, but is not limited to, recombinant DNA techniques, genetics and genetic engineering, cell fusion techniques, and bioprocesses, using living organisms, or parts of organisms.

(ii) Biotechnology does not include farming, agriculture, or animal or apiary husbandry, or the production of any crop or agricultural product by traditional growing processes or by hydroponic growing processes, or fish farming, or the raising or growing or production of fish or any aquatic animal or product.

(iii) Biotechnology does not include zymurgy, wine making, brewing, preparation of yeast used in food production or preparation, or any food or drink preparation or production.

#### Biotech means genetic manipulation – it excludes biofuels

U.S.-China ESRC Economic and Security Review Commission, 2-13-2019, https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf, “China’s Biotechnology Development: The Role of US and Other Foreign Engagement" No Publication (ermo/sms, Acc:6-27-2022)

Our definition of biotechnology does not include use of non-biological processes for production from biomass (i.e., matter derived from living organisms, such as plant mass), to include the manufacture of biodiesel by chemical conversion of biomass. Most relevant to our scope are uses of organisms genetically engineered to produce a material of interest (for example, to be able to ferment specific types of biomass for fuel or to produce industrial enzymes). Use of naturally-occurring organisms for fermentation-based production may be relevant to an indirect or lesser degree; for instance, biofuels can be produced by fermentation with unmodified microorganisms. For this study of biotechnology, we are mainly interested in advances in the life sciences, usually involving genetic manipulation.

### Germline Genetic Engineering

#### Genetic Engineering

Merriam Webster “Genetic Engineering” <https://www.merriam-webster.com/dictionary/genetic%20engineering> Merriam Webster Dictionary Accessed 10 June 2022 (jshock)

the group of applied techniques of genetics and biotechnology used to cut up and join together genetic material and especially DNA from one or more species of organism and to introduce the result into an organism in order to change one or more of its characteristics

#### Germline DNA

NCI Dictionary “Germline DNA” <https://www.cancer.gov/publications/dictionaries/genetics-dictionary/def/germline-dna> National Cancer Institute Accessed 10 June 2022 (jshock)

Germline DNA refers to tissue derived from reproductive cells (egg or sperm) that become incorporated into the DNA of every cell in the body of the offspring. A germline mutation may be passed from parent to offspring. Also called constitutional DNA.

#### Germline Engineering

IGI Global “What is Germline Engineering” <https://www.igi-global.com/dictionary/ethical-aspects-genetic-engineering-biotechnology/37900> International General Insurance Co Accessed 10 June 2022 (jshock)

The genetic modification of individuals whose alterations will be passed on to their progeny. It involves altering genes in eggs, sperm, or early embryos, by insertion (e.g. of artificial chromosomes), gene deletion or gene transposition.

### Cybersecurity

#### Cybersecurity means protection

CISA 2019 “Security Tip (ST04-001” https://www.cisa.gov/uscert/ncas/tips/ST04-001 Cybersecurity & Infrastructure Security Agency (jshock)

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.

#### Cybersecurity – 5 Types

COMPtia “What is Cybersecurity?” <https://www.comptia.org/content/articles/what-is-cybersecurity> CompTIA Accessed 23 June 2022 (jshock)

CompTIA’s Chief Technology Evangelist, James Stanger says it best when he [defines cybersecurity](https://www.comptia.org/blog/what-is-the-difference-between-it-security-and-cybersecurity) as “focusing on protecting electronic assets – including internet, [WAN](https://www.comptia.org/content/guides/what-is-a-wide-area-network) and [LAN](https://www.comptia.org/content/guides/what-is-a-local-area-network) resources – used to store and transmit that information.”

Cybersecurity can be categorized into five distinct types:

* Critical infrastructure security
* Application security
* Network security
* Cloud security
* Internet of Things (IoT) security

#### Cybersecurity excludes information security – it is about the infrastructure

Bay, Morten, 2016, Ph.D. Candidate in Information Studies at UCLA https://frenchjournalformediaresearch.com/lodel-1.0/main/index.php?id=988, "What is cybersecurity? In search of an encompassing definition for the post-Snowden era " French Journal For Media Research – n° 6/2016 – ISSN 2264-4733 (ermo/sms, Acc:6-27-2022)

57 Topical difference

Upon further analysis into the actual meaning of the terms, differences also start to appear. Von Solms & van Niekerk (2013) shows that, although there are many similarities, there are also plenty of examples where a breach of cybersecurity is not the same as a breach of information security:

If cybersecurity is synonymous with information security it would be reasonable to assume that cybersecurity incidents could also be described in terms of the characteristics used to define information security. Thus, a cybersecurity incident would, for example, also lead to a breach in the confidentiality, integrity or availability of information. (p.99)

58The authors then go on to present a number of scenarios that

…deal with a specific aspect of cybersecurity where the interests of a person, society or nation, including their non-information based assets, need to be protected from risks stemming from interaction with cyberspace. This serves to highlight the difference between information security and cybersecurity (p.100).

59Generally, von Solms & van Niekerk conclude that the main difference in the natures of information security and cybersecurity is that information security is focused on the protection of the actual information itself, where as cybersecurity is concerned with the information infrastructure, and what is reachable through the infrastructure (which is not exclusively information):

Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cybersecurity, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace. (p. 101)

60With the number of devices connected to networks and the Internet growing, not least because of the emergence of the so-called ‘Internet of Things’, it is clear that information is not the only vulnerable assets in need of protection online (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Tan & Wang, 2010)

#### Plan is cyber resilience not cybersecurity

Imagine IT, 7-29-2021, https://imagineiti.com/understanding-cyber-resilience/, "Understanding cyber resilience. And how it relates to security," Imagine IT (ermo/sms, Acc:6-27-2022)

Cyber resilience vs. cyber security

The difference between cyber security and cyber-resilience comes down to the expected outcomes of each.

Cyber security: Is a component of cyber resilience and consists of technology processes and measures to protect networks, systems, and sensitive data from cyber attacks. Effective cyber-security reduces the chances of cyber attacks and protects your organization from external and internal assaults.

Cyber resilience: It reflects the fact that SMB technology systems will always have flaws and weaknesses that are exploitable. It has a much bigger scope and includes cyber security and business resilience. Cyber resilience focuses on instances when your company is disrupted by things like power outages, weather emergencies, and human error. This concept helps SMBs prepare, prevent, respond, and successfully recover to pre-event business levels and processes.

Why cyber resilience?

Because traditional cybersecurity measures for SMBs are just not enough.

The truth is, harmful cyber events negatively impact SMBs every day. These events may be external or internal and may be intentional or unintentional, caused by humans, nature, or a combination of both.

It isn’t a matter of if they will get in; it is when!

Today, it’s as critical for SMBs to be able to respond and recover from security breaches as it is to be able to prevent them. Cyber resilience aims to give your organization a plan that will consider actions and outcomes before, during, and after an event.

What are the benefits:

It improves your cyber-security posture

Reduces financial losses

Maintains the trust of customers

Protects your organization’s reputation

Maintains the trust of vendors

Improves your cultural and internal processes

Maintains the trust of employees

How does cyber resilience work?

It is a strategy that is considered a preventive measure to counteract human error and security weaknesses in hardware and software. The overall purpose is to protect the organization while understanding that there will likely be insecure parts, no matter how robust security controls are.

The main components of your cyber reliance strategy should include:

Threat protection: As security solutions advance, so does the ability of the cyber-attackers to breach your system. What were once state-of-the-art solutions are now the bare minimum requirements to protect your SMB.

Recoverability: After a security incident, whether internal or external, your organization must have the ability to return to normal operations quickly.

Adaptability: Your organization must evolve and adapt to new tactics that cyber-criminals deploy. Investing in continuous security monitoring so your people can recognize security issues in real-time and take immediate action is critical.

Resilience: Your organization’s ability to effectively operate after a security breach.

The six elements of a successful cyber resilience strategy

Identify

Includes the use of attack surface management, continuous monitoring to identify irregularities and breaches before they cause any significant damage

Protect

A good cyber resilience strategy protects your system, your applications, and your data. You need to ensure that only authorized users can access your system.

Detect:

You need the ability to detect when someone is trying to act maliciously against your systems and can come externally or internally.

Respond

You also need to Developing an incident response plan, identifying roles and responsibilities to ensure you can operate normally even after a cyber-attack.

Recover

Ability to quickly store digital and technology platforms and adapt and recover mission-critical systems to avoid disruption

Anticipate

You want to rely on automation, machine learning, and adaptive cyber-threat detection to address future threats

A digital transformation mindset

Cyber resilience goes hand in hand with digital transformation. Both require a similar way of thinking. Cyber resilience recognizes that the outdated notion of SMBs having impenetrable defenses be abandoned. Cyber resilience assumes that attackers will be successful, so measures must be in place to prevent, respond, and recover from these attacks.

For those measures to be successful, cybersecurity needs to be everybody’s responsibility, and cyber best practices need to be inserted into all aspects of the organization.

As the pandemic has changed all aspects of your business, it has accelerated the need for digital transformation in SMBs. As digital transformation has accelerated, so too have efforts to boost cybersecurity. Businesses realize that cyber-resilience is critical if they are to survive the effects of COVID.

Digital transformation requires a greater dependency on IT. Because SMBs are more dependent on IT, they need strong cyber resiliency. Without it, a business can’t be confident of its ability to continue operations when faced with increased cyber threats that accompany increased dependence on IT.

Do you put cyber-security first?

Is cyber-security front and center of your strategies, or are you just paying it lip service? Do you have a security-first culture, and does your leadership put cyber resilience in the same “box” as operational performance?

Like measuring your business’s ROI and profitability, cyber-security and cyber resilience must be a strategic priority that you track and measure.

Closing thoughts:

Cyber resilience is an organization-wide strategy that actively monitors threats, risks, and weak points. It is a collaborative strategy that extends to everyone your company connects with.

Organizations should keep in mind that cybersecurity is not the same as cyber resilience. When cybersecurity fails, you must have a plan in place to assess the problem and have the ability to recover quickly back to pre-cyber-event status.

### Offensive Cyber Operations

#### Offensive Cyber Operations

Dennis Miralis “Offensive Cyberattacks and Operations” <https://ngm.com.au/australia-offensive-cyber-capabilities/> NGM Defense Lawyers and Advisors Accessed 23 June 2022 (jshock)

The Department of the Prime Minister and Cabinet’s Cyber Lexicon project defines offensive cyber operations as ‘activities in cyberspace that manipulate, deny, disrupt, degrade or destroy targeted computers, information systems, or networks’.

Offensive cyber operations could encompass a range of [cybercrimes](https://ngm.com.au/cybercrime-lawyers/) including:

* Removing computer accounts or changing passwords;
* Altering databases either subtly or destructively;
* Defacing web pages;
* Encrypting or deleting data;
* Attacks that affect critical infrastructure, such as electricity networks.

By contrast, cyber espionage is designed to gather intelligence without being detected.

#### Offensive Cyber Operations work through Cyber Space

Edwin Djabatey July 2019 “U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I” <https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/> Just Security (jshock)

According to U.S. Military doctrine, “[offensive cyberspace operations](https://fas.org/irp/doddir/army/fm3-38.pdf)” are operations “intended to project power by the application of force in or through cyberspace.” They will seemingly be deployed according to the U.S. Department of Defense’s much vaunted 2018 Cyber strategy. That strategy is anchored around the concepts of “[defending forward](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF),” which [describes](https://www.lawfareblog.com/pentagons-new-cyber-strategy-defend-forward) the conduct of operations inside adversary networks to “stop threats before they reach their targets,” and “[persistent engagement](https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010),” which denotes the continuous [confrontation](https://www.lawfareblog.com/response-persistent-engagement-and-agreed-competition) of adversaries throughout cyberspace in order to gain operational advantages while denying such advantages to those adversaries. Examples of these concepts in practice include [Operation Synthetic Theology](https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?noredirect=on&utm_term=.347706662ddb), an operation to disrupt Russian efforts to interfere in the 2018 midterm elections, and more [recently reported](https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?login=email&auth=login-email) incursions into the Russian power grid and [Iranian missile systems](https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?utm_term=.f8cc588d0fb4).

### Security Cooperation

#### Security Cooperation

DSCU “Introduction to Security Cooperation” <https://www.dscu.edu/documents/publications/greenbook/01_Chapter.pdf?id=1> Defense Security Cooperation University Accessed 10 June 2022 (jshock)

While all of the programs previously mentioned are authorized under 22 U.S.C (Title 22), and are under the general control of the Department of State (DoS), the Department of Defense (DoD) administers many of them. Title 10 U.S. Code Section 301 defines security cooperation programs and activities of DoD as any program or interaction of U.S.C. with the security establishment of a foreign country to build capabilities, provide access or build relationships. As such, many of the previously described FAA and AECA-authorized security assistance programs administered by the 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 DSCU website or use the SC Programs Viewer on the Security Assistance Network Web (SANweb)

#### Security Cooperation uses DOD to promote US Interests

Joint Publication 3-20 May 2017 “Security Cooperation” <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf> Joint Doctrine Publication (jshock)

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

#### Security Cooperation Organization

Joint Publication 3-20 May 2017 “Security Cooperation” <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf> Joint Doctrine Publication (jshock)

A Department of Defense element that is part of the United States diplomatic mission located in a foreign country to carry out security assistance and cooperation management functions under the supervision and coordination authority of the senior defense official/defense attaché. Also called SCO. (Approved for incorporation into the DOD Dictionary.)

#### Security Cooperation is limited to military purposes – basing, self-defense, and DoD

Kevin Scott, 2017, Vice Admiral, US Navy, Director – Joint Force Development, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf, "," No Publication (ermo/sms, Acc:6-27-2022)

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

#### SC includes everything, such as disaster and emergency

Kevin Scott, 2017, Vice Admiral, US Navy, Director – Joint Force Development, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf, "," No Publication (ermo/sms, Acc:6-27-2022)

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

#### SC is limited to DOD roles

Kevin Scott, 2017, Vice Admiral, US Navy, Director – Joint Force Development, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf, "," No Publication (ermo/sms, Acc:6-27-2022)

SC activities are conducted with DOD funds, forces, and authorities, and with DOS SA funds and authorities, administered by DOD.

#### SC is broad – basically anything we do with other militaries

Kevin Scott, 2017, Vice Admiral, US Navy, Director – Joint Force Development, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf, "," No Publication (ermo/sms, Acc:6-27-2022)

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

a. SC can be conducted across the range of military operations and during all phases of an operation or campaign. DOD policy supports SC activities that enable building security relationships, building partner capacity, and gaining/maintaining access.

### North Atlantic Treaty Organization

#### North Atlantic Treaty Organization

Dictionary.com “NATO” [https://www.dictionary.com/browse/nato Dictionary.com](https://www.dictionary.com/browse/nato%20Dictionary.com) Accessed 23 June 2022 (jshock)

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.

#### NATO Security Alliance

US Mission “About NATO” <https://nato.usmission.gov/about-nato/> U.S Mission to the North Atlantic Treaty Organization Accessed 23 June 2022 (jshock)

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.

[Article 5 of the Washington Treaty](http://www.nato.int/cps/en/natolive/official_texts_17120.htm)  — that an attack against one Ally is an attack against all — is at the core of the Alliance, a promise of collective defense. Article 4 of the treaty ensures consultations among Allies on security matters of common interest, which have expanded from a narrowly defined Soviet threat to the critical mission in Afghanistan, as well as peacekeeping in Kosovo and new threats to security such as cyber attacks, and global threats such as terrorism and piracy that affect the Alliance and its global network of partners.

#### NATO’s Collective Military Power

NATO “The Power of NATO’s Military” <https://shape.nato.int/page11283634/knowing-nato/episodes/the-power-of-natos-military> Supreme Headquarters Allied Powers Europe Accessed 23 June 2022 (jshock

Since 1949, NATO has increased its collective military power. Today it has the capability to count on nearly 3.5-million personnel, troops and civilian combined. Each member state agrees to contribute with different strategic weight and influence.

Allied Command Operations (ACO) led by Supreme Allied Commander Europe (SACEUR), is responsible for executing all NATO operations and missions, Deputy SACEUR coordinates troop contributions. When an operation or mission ends, multinational forces return to their respective countries.

When the North Atlantic Council (NAC) decides to carry out an operation, mission or exercise, NATO's military authorities propose a draft concept of operations (called CONOPS) that presents the minimum request of forces they are demanding in terms of equipment, work force and resources. This process is called force generation.

### A2: Cybersecurity = Defensive

#### We Meet – we result in defense by denial

#### Counter Interp - Defensive Cybersecurity is only half of cybersecurity – offensive is cybersecurity too

Lily Teplow, 21, (Lily Teplow, Creative writer. Marketing maven. Content Marketing Manager at Huntress., 9-14-2021, Should We Be Playing Offense or Defense in Cybersecurity?, https://www.huntress.com/blog/should-we-be-playing-offense-or-defense-in-cybersecurity, 6-28-2022) SCade

Cybersecurity professionals tend to focus more on the defensive side of security. That’s the nature of the job after all—when adversaries attack, we defend. But defense is only half of the equation. Hackers are always evolving their tradecraft. They’re finding new ways to break into networks and systems, and they’re getting very good at defense evasion. With all the new tactics, techniques and procedures attackers are using, the traditional approach of defense-only cybersecurity isn’t enough. Many businesses are realizing the need to develop both offensive and defensive strategies. But what’s best to focus on, playing offense or playing defense?

#### Limits – still constrained to NATO cyber actions – they should be prepared to debate OCOs good AND OCOs bad

#### Predictability – two sections of OCOs does not destroy their ability to debate

#### Education – They still access all their education claims since we still have debates over OCO good/bad

#### Not effects T – result in immediate change in cyber policy

#### Reasonability – if you think that we are reasonably related to the topic you should vote aff, anything else encourages a race to the bottom and a definitional debate that is bad for education

## Common Terms

### Increase—generic dictionary

#### To make greater.

**Random House, 2011** (Dictionary.com Unabridged Based on the Random House Dictionary, © Random House, Inc. 2011)

–verb (used with object) 1. **to make greater**, as **in number, size, strength, or quality**; augment; add to

#### To become greater.

**Collins, 2009** (Collins English Dictionary - Complete & Unabridged 10th Edition)

World English Dictionary increase — vb 1. **to make or become greater in size, degree, frequency**, etc; grow or expand

**Requires preexistence**

**Increase requires pre-existence.**

**Brown, 2003** (US Federal Judge for the United States District Court for the District of Oregon, Elena mark and paul Gustafson v. Valley Insurance Company and Valley Property and Casualty, July 17, lexis)

FCRA does not define the term "increase." The plain and ordinary meaning of the verb "to increase" is to make something greater or larger. 4 Merriam-Webster's [\*\*22] Collegiate Dictionary 589 (10th ed. 1998). The "something" that is increased in the statute is the "charge for any insurance." The plain and common meaning of the noun "charge" is "the price demanded for something." Id. at 192. Thus, the statute plainly means an insurer takes adverse action if the insurer makes greater (i.e., larger) the price demanded for insurance. An insurer cannot "make greater" something that did not exist previously. The statutory definition of adverse action, therefore, clearly anticipates an insurer must have made an initial charge or demand for payment before the insurer can increase that charge. In other words, an insurer cannot increase the charge for insurance unless the insurer previously set and demanded payment of the premium for that insured's insurance [\*\*23] coverage at a lower price.

**Previously existing.**

**American Heritage, 2010** (The American Heritage Dictionary of the English Language, 4th edition, google)

Augment; usually applies to what is already developed or well under way

**“Increase” requires evidence of the preexisting condition to determine a net increase**

**Ripple 87** (Circuit Judge, Emmlee K. Cameron, Plaintiff-Appellant, v. Frances Slocum Bank & Trust Company, State Automobile Insurance Association, and Glassley Agency of Whitley, Indiana, Defendants-Appellees, 824 F.2d 570; 1987 U.S. App. LEXIS 9816, 9/24, lexis)

Also related to the waiver issue is appellees' defense relying on a provision of the insurance policy that suspends coverage where the risk is increased by any means within the knowledge or control of the insured. However, the term "increase" connotes change. To show change, appellees would have been required to present evidence of the condition of the building at the time the policy was issued. See 5 J. Appleman & J. Appleman, Insurance Law and Practice, § 2941 at 4-5 (1970). Because no such evidence was presented, this court cannot determine, on this record, whether the risk has, in fact, been increased. Indeed, the answer to this question may depend on Mr. Glassley's knowledge of the condition of the building at the time the policy was issued, see 17 J. Appleman & J. Appleman, Insurance Law and Practice, § 9602 at 515-16 (1981), since the fundamental issue is whether the appellees contemplated insuring the risk which incurred the loss.

**Doesn’t require preexistence**

**One can increase from zero**

**Words and Phrases 7** (Cumulative Supplementary Pamphlet, 2007 vol. 20a, 07, 76)

Increase: Salary change of from zero to $12,000 and $1,200 annually for mayor and councilmen respectively was an “increase” in salary and not merely the fixing of salary. King v. Herron, 243 S.E.2d36, 241 Ga. 5.

**Increase doesn’t require pre-existence**

**Reinhardt, 2005** (U.S. Judge for the United States Court of Appeals for the ninth circuit, Reynolds and Rausch v. Hartford Financial Services Group, inc, lexis)

Specifically, we must decide whether charging a higher price for initial insurance than the insured would otherwise have been charged because of information in a consumer credit report constitutes an "increase in any charge" within the meaning of FCRA. First, we examine the definitions of "increase" and "charge." Hartford Fire contends that, limited to their ordinary definitions, these words apply only when a consumer has previously been charged for insurance and that charge has thereafter been increased by the insurer. The phrase, "has previously been charged," as used by Hartford, refers not only to a rate that the consumer has previously paid for insurance but also to a rate that the consumer has previously been quoted, even if that rate was increased [\*\*23] before the consumer made any payment. Reynolds disagrees, asserting that, under [\*1091] the ordinary definition of the term, an increase **in a charge also** occurs whenever **an insurer charges** a higher **rate** than it would otherwise **have charged because of any factor**--such as adverse credit information, age, or driving record 8 --regardless of **whether the customer was** previously **charged** some **other** rate. According to Reynolds, he was charged an increased rate because of his credit rating when he was compelled to pay a rate higher than the premium rate because he failed to obtain a high insurance score. Thus, he argues, the definitions of "increase" and "charge" encompass the insurance companies' practice. Reynolds is correct. “Increase" means to make something greater. See, e.g., OXFORD ENGLISH DICTIONARY (2d ed. 1989) ("The action, process, or fact of becoming or making greater; augmentation, growth, enlargement, extension."); WEBSTER'S NEW WORLD DICTIONARY OF AMERICAN ENGLISH (3d college ed. 1988) (defining "increase" as "growth, enlargement, etc[.]"). "Charge" means the price demanded for goods or services. See, e.g., OXFORD ENGLISH DICTIONARY (2d ed. 1989) ("The price required or demanded for service rendered, or (less usually) for goods supplied."); WEBSTER'S NEW WORLD DICTIONARY OF AMERICAN ENGLISH (3d college ed. 1988) ("The cost or price of an article, service, etc."). Nothing in the definition of these words implies that the term "increase in any charge for" should be limited to cases in which a company raises the rate that an individual has previously been charged.

### Substantially – Without Material Qualification

#### Substantial means without material qualifications

Black’s Law Dictionary 91 - p. 1024 ///BDN

Substantially - means essentially; without material qualification.

**Substantially means ‘without material qualification.’**

**AGO, 1984** (Office of the Attorney General of Florida Number: AGO 84-63, myfloridalegal.com/ago.nsf/Opinions/9CF0AA7178DC692C8525657700610790(

No definition or construction of the term "substantially" is contained within s 166.041(3)(c), F.S., as that term is used in the phrase "which substantially change permitted use categories." However, words in common use in a statute are to be construed in their plain and ordinary sense. See, State v. Tunnicliffe, 124 So. 279 (Fla.1929); Gasson v. Gay, 49 So.2d 567 (Fla.1950); Pedersen v. Green, 105 So.2d 1 (Fla.1958); State v. Egan, 287 So.2d 1, 4 (Fla.1973). "Substantially" is defined as: "Essentially; without material qualification; in the main; in substance; materially; in a substantial manner." Black's Law Dictionary 1281 (5th ed. 1979). " 'Substantially' is variously defined as meaning in a substantial manner; in substance; in the main; essentially; solidly; actually; really; truly; competently." 83 C.J.S. Substantially p. 765.

### Substantially - Numbers

**20% is below the threshold for substantial**

**Words & Phrases**: Permanent Edition, **2002**, vol 40B, p.326

Bkrtcy.N.D.Ill. 2000. Where debtor-jewelry retailers historically obtained 15-20% of the inventory in their two divisions through consignments, thew were not, as a matter of law, "substantially" ear gaged in selling the goods of others, within meaning of Illinois Uniform Commercial Code (UCC) provision setting forth means by which transaction may be treated as a true consignment and consignor's interest in consigned goods may be protected against the interests of consignee's creditors S.H.A. 810 ILCS 5/2-326(3)(b).- In re Wean Holdings, Inc., 248 B.R. 336.-Sales 8.

**Substantially is greater than 50%.**

**Words and Phrases 2000** (Permanent Edition, Cumulative Annual Pamphlet, Volume 40, p. 561)

Ind.App. 1996. Within ruling that person who completes substantial portion of construction of his own home is exempt from building code requirements, **"**substantial" is to be understood as meaning "of **ample or** considerable amount, quantity, or size," and it would be inconsistent with ordinary meaning of the term to construe "substantial portion" as referring to only half of the whole. West's A.I.C. 46-7-8-3(d).-Robinson v. Monroe County, 683 N.E.2d 196.-Health & E 32.

**65% is below the substantially threshold**

**Words & Phrases**: Permanent Edition, **2002,** vol 40B, p.327

Ill. 1951. Employing unit which succeeded to 65% of assets of predecessor employing unit did not succeed to "substantially" all of employing enterprises of predecessor employing unit and therefore was not entitled to experience rating of predecessor employing unit for Unemployment vond Compensation Act purposes. S.H.A. ch. 48, 218(g) (1).— Winakor v. Annunzio, 99 N.E.2d , 191, 409 111. 236.—Tax 347.1.

**substantially is at least 90% (substantially all)**

**Words and Phrases, 2005 (v. 40B, p. 329)**

N.H. 1949. **The word “substantially**” as used in provision of Unemployment Compensation Act that experience rating of an employer may be transferred to an employing unit which acquires the organization, trade, or business, or “substantially” all of the assets thereof, is an elastic term which does not include a definite, fixed amount of percentage, and the transfer does not have to be 100 per cent but cannot be less than 90 per cent in the ordinary situation. R.L. c 218, § 6, subd. F, as added by Laws 1945, c.138, § 16.

**“Substantially" means 80 to 90%—government definitions prove.**

**Curtin, 2003** (John T. Curtin, Judge, United States District Court for the Western District of New York, Gateway Equipment Corp. -vs- United States of America, United States District Court for the Western District of New York, lexis)

**The government** cites Webster's Ninth New College Dictionary for the definitions of "limit" and "impairment" as suggesting "meanings equivalent to restriction and reduction, respectively." Item 30, p. 3, n.1. **It posits that the word "substantially" suggests "an order of magnitude equivalent to 80% or 90%**." Id. It concludes that "using those definitions, 'substantially limited' and 'substantially impaired' means that there must be an 80%-90% restriction and/ or reduction of use by virtue of the design of the CB-4000." Id.

## Topicality Theory Help

### Limits Good

#### Turns their offense—limits are vital to creativity and innovation

David **Intrator** (President of The Creative Organization) October 21, **2010** “Thinking Inside the Box,” http://www.trainingmag.com/article/thinking-inside-box

One of the most pernicious myths about creativity, one that seriously inhibits creative thinking and innovation, is the belief that one needs to “think outside the box.”  As someone who has worked for decades as a professional creative, nothing could be further from the truth. This a is view shared by the vast majority of creatives, expressed famously by the modernist designer Charles Eames when he wrote, “Design depends largely upon constraints.”  The myth of thinking outside the box stems from a fundamental misconception of what creativity is, and what it’s not.  In the popular imagination, creativity is something weird and wacky. The creative process is magical, or divinely inspired.  But, in fact, creativity is not about divine inspiration or magic. It’s about problem-solving, and by definition a problem is a constraint, a limit, a box. One of the best illustrations of this is the work of photographers. They create by excluding the great mass what’s before them, choosing a small frame in which to work. Within that tiny frame, literally a box, they uncover relationships and establish priorities. What makes creative problem-solving uniquely challenging is that you, as the creator, are the one defining the problem. You’re the one choosing the frame. And you alone determine what’s an effective solution. This can be quite demanding, both intellectually and emotionally. Intellectually, you are required to **establish limits**, set priorities, and cull patterns and relationships from a great deal of material, much of it fragmentary. More often than not, this is the material you generated during brainstorming sessions. At the end of these sessions, you’re usually left with a big mess of ideas, half-ideas, vague notions, and the like. Now, chances are you’ve had a great time making your mess. You might have gone off-site, enjoyed a “brainstorming camp,” played a number of warm-up games. You feel artistic and empowered. But to be truly creative, you have to clean up your mess, organizing those fragments into something real, something useful, something that actually works. That’s the hard part. It takes a lot of energy, time, and willpower to make sense of the mess you’ve just generated. It also can be emotionally difficult. You’ll need to throw out many ideas you originally thought were great, ideas you’ve become attached to, because they simply don’t fit into the rules you’re creating as you build your box.

### Procedural Fairness

#### Reasonable semblances of procedural fairness are absolutely achievable for all players in the debate-game model to incentivize prep and clash

**Rodriguez, 2006**- media theory professor at the City University of Hong Kong with a PhD from NYU (Hector Rodriguez, December 2006, “The Playful and the Serious: An approximation to Huizinga's Homo Ludens,” published in Game Studies, vol. 6 issue 1, fg)

There is a core feature of playing that offers a huge potential for serious game designers. According to Huizinga, the consciousness of play as a separate and self-contained sphere is often reinforced by the pervasive tendency to enclose the players within a spatiotemporal frame, the so-called "magic circle", which isolates their game from the more serious tasks of daily living. The separation often consists in a literal physical precinct: a chessboard, ring, arena, field, stadium, stage, altar, etc. There are also sharp temporal boundaries, a clear beginning and an end, which clearly mark the game off as a temporary interruption of ordinary life. The game unfolds within a temporarily closed world. Moreover, the existence of the magic circle is closely related to the existence of artificial rules or conventions that hold only within this enclosure.[4] Higher cultural forms also unfold within a magic circle. The temple or sacred area, for instance, provides a self-contained enclosure for the performance of religious ceremonies in accordance with strictly codified regulations. Many other cultural practices, such as initiation rites, require the demarcation of a special place characterized by temporary norms of behaviour that hold only for the duration of the ceremony. The boundaries of the playing field mark off the arena wherein the special rules of the game hold absolutely. These rules often generate ideal conditions. Playful competition often requires, for instance, that all players be given an equal chance at the outset. Two chess players always receive the same amount of pieces in the beginning of the game, to avoid favouring one player at the expense of another. While perfect equality may be difficult to achieve in practice, competitive games establish artificial conditions designed to neutralize potential sources of unfairness from the outset. Thus questions of ethics lie at the heart of many forms of play. Huizinga himself asserts that gaming often has an ethical import, and so tends to acquire at least a touch of seriousness. To play is in many instances to test the player's strength, intelligence, effort, persistence, manual dexterity, spatial reasoning and so forth. The idea of fair play also suggests an element of moral evaluation at the heart of many games. Huizinga clearly recognizes the presence of this ethical element, which strongly implies that the demarcation of play from obligation is not absolute. The institution of the magic circle is a core element in the ideal of an ordered life ruled by agreed-upon conventions, which lies at the heart of human society.

### Depth over Breadth

#### Studies prove—depth is better than breadth.

**Arrington 09** (Rebecca, UVA Today, “Study Finds That Students Benefit From Depth, Rather Than Breadth, in High School Science Courses” March 4)

**A recent study reports that** high school students who study **fewer** science **topics**, but study them **in** greater **depth, have an advantage** in college science classes **over** their peers who study **more topics** and spend less time on each. Robert Tai, associate professor at the University of Virginia's Curry School of Education, worked with Marc S. Schwartz of the University of Texas at Arlington and Philip M. Sadler and Gerhard Sonnert of the Harvard-Smithsonian Center for Astrophysics to conduct the study and produce the report. "Depth Versus Breadth: How Content Coverage in High School Courses Relates to Later Success in College Science Coursework" relates the amount of content covered on a particular topic in high school classes with students' performance in college-level science classes. The study will appear in the July 2009 print edition of Science Education and is currently available as an online pre-print from the journal. "As a former high school teacher, I always worried about whether it was better to teach less in greater depth or more with no real depth. This study offers evidence that teaching fewer topics in greater depth is a better way to prepare students for success in college science," Tai said. "These results are based on the performance of thousands of college science students from across the United States." The 8,310 students in the study were enrolled in introductory biology, chemistry or physics in randomly selected four-year colleges and universities. Those who spent one month or more studying one major topic in-depth in high school earned higher grades in college science than their peers who studied more topics in the same period of time. The study revealed that **students** in courses that focused on **mastering a particular topic were impacted twice as much as those** in courses **that touched on every major topic**.

### Limits – Iterative testing

#### A well-defined resolution is critical to allow the neg to refute the aff in an in-depth fashion---this process of negation produces iterative testing and improvement, where we learn to improve our arguments based on our opponents’ arguments. This process does not proscribe particular styles or forms of argument, but does require a common point of disagreement around which arguments can be organized.

**Poscher 16** – Director at the Institute for Staatswissenschaft and Philosophy of Law at the University of Freiburg (Ralf, “Why We Argue About the Law: An Agonistic Account of Legal Disagreement”, Metaphilosophy of Law, Tomasz Gizbert-Studnicki/Adam Dyrda/Pawel Banas (eds.), Hart Publishing, forthcoming)

Hegel’s dialectical thinking powerfully exploits the idea of negation. It is a central feature of spirit and consciousness that they have the power to negate. The spirit “is this power only by looking the negative in the face and tarrying with it. This […] is the magical power that converts it into being.”102 The tarrying with the negative is part of what Hegel calls the “labour of the negative”103. In a loose reference to this Hegelian notion Gerald Postema points to yet another feature of disagreements as a necessary ingredient of the process of practical reasoning. Only if our reasoning is exposed to contrary arguments can we test its merits. We must go through the “labor of the negative” to have trust in our deliberative processes.104 This also holds where we seem to be in agreement. Agreement without exposure to disagreement can be deceptive in various ways. The first phenomenon Postema draws attention to is the group polarization effect. When a group of like‐minded people deliberates an issue, informational and reputational cascades produce more extreme views in the process of their deliberations.105 The polarization and biases that are well documented for such groups106 can be countered at least in some settings by the inclusion of dissenting voices. In these scenarios, disagreement can be a cure for dysfunctional deliberative polarization and biases.107 A second deliberative dysfunction mitigated by disagreement is superficial agreement, which can even be manipulatively used in the sense of a “presumptuous ‘We’”108. Disagreement can help to police such distortions of deliberative processes by challenging superficial agreements. Disagreements may thus signal that a deliberative process is not contaminated with dysfunctional agreements stemming from polarization or superficiality. Protecting our discourse against such contaminations is valuable even if we do not come to terms. Each of the opposing positions will profit from the catharsis it received “by looking the negative in the face and tarrying with it”. These advantages of disagreement in collective deliberations are mirrored on the individual level. Even if the probability of reaching a consensus with our opponents is very low from the beginning, as might be the case in deeply entrenched conflicts, entering into an exchange of arguments can still serve to test and improve our position. We have to do the “labor of the negative” for ourselves. Even if we cannot come up with a line of argument that coheres well with everybody else’s beliefs, attitudes and dispositions, we can still come up with a line of argument that achieves this goal for our own personal beliefs, attitudes and dispositions. To provide ourselves with the most coherent system of our own beliefs, attitudes and dispositions is – at least in important issues – an aspect of personal integrity – to borrow one of Dworkin’s favorite expressions for a less aspirational idea. In hard cases we must – in some way – lay out the argument for ourselves to figure out what we believe to be the right answer. We might not know what we believe ourselves in questions of abortion, the death penalty, torture, and stem cell research, until we have developed a line of argument against the background of our subjective beliefs, attitudes and dispositions. In these cases it might be rational to discuss the issue with someone unlikely to share some of our more fundamental convictions or who opposes the view towards which we lean. This might even be the most helpful way of corroborating a view, because we know that our adversary is much more motivated to find a potential flaw in our argument than someone with whom we know we are in agreement. It might be more helpful to discuss a liberal position with Scalia than with Breyer if we want to make sure that we have not overlooked some counter‐argument to our case. It would be too narrow an understanding of our practice of legal disagreement and argumentation if we restricted its purpose to persuading an adversary in the case at hand and inferred from this narrow understanding the irrationality of argumentation in hard cases, in which we know beforehand that we will not be able to persuade. Rational argumentation is a much more complex practice in a more complex social framework. Argumentation with an adversary can have purposes beyond persuading him: to test one’s own convictions, to engage our opponent in inferential commitments and to persuade third parties are only some of these; to rally our troops or express our convictions might be others. To make our peace with Kant we could say that “there must be a hope of coming to terms” with someone though not necessarily with our opponent, but maybe only a third party or even just ourselves and not necessarily only on the issue at hand, but maybe through inferential commitments in a different arena. f) The Advantage Over Non‐Argumentative Alternatives It goes without saying that in real world legal disagreements, all of the reasons listed above usually play in concert and will typically hold true to different degrees relative to different participants in the debate: There will be some participants for whom our hope of coming to terms might still be justified and others for whom only some of the other reasons hold and some for whom it is a mixture of all of the reasons in shifting degrees as our disagreements evolve. It is also apparent that, with the exception of the first reason, the rationality of our disagreements is of a secondary nature. The rational does not lie in the discovery of a single right answer to the topic of debate, since in hard cases there are no single right answers. Instead, our disagreements are instrumental to rationales which lie beyond the topic at hand, like the exploration of our communalities or of our inferential commitments. Since these reasons are of this secondary nature, they must stand up to alternative ways of settling irreconcilable disagreements that have other secondary reasons in their favor – like swiftness of decision making or using fewer resources. Why does our legal practice require lengthy arguments and discursive efforts even in appellate or supreme court cases of irreconcilable legal disagreements? The closure has to come by some non‐argumentative mean and courts have always relied on them. For the medieval courts of the Germanic tradition it is bequeathed that judges had to fight it out literally if they disagreed on a question of law – though the king allowed them to pick surrogate fighters.109 It is understandable that the process of civilization has led us to non‐violent non‐ argumentative means to determine the law. But what was wrong with District Judge Currin of Umatilla County in Oregon, who – in his late days – decided inconclusive traffic violations by publicly flipping a coin?110 If we are counting heads at the end of our lengthy argumentative proceedings anyway, why not decide hard cases by gut voting at the outset and spare everybody the cost of developing elaborate arguments on questions, where there is not fact of the matter to be discovered? One reason lies in the mixed nature of our reasons in actual legal disagreements. The different second order reasons can be held apart analytically, but not in real life cases. The hope of coming to terms will often play a role at least for some time relative to some participants in the debate. A second reason is that the objectives listed above could not be achieved by a non‐argumentative procedure. Flipping a coin, throwing dice or taking a gut vote would not help us to explore our communalities or our inferential commitments nor help to scrutinize the positions in play. A third reason is the overall rational aspiration of the law that Dworkin relates to in his integrity account111. In a justificatory sense112 the law aspires to give a coherent account of itself – even if it is not the only right one – required by equal respect under conditions of normative disagreement.113 Combining legal argumentation with the non‐argumentative decision‐ making procedure of counting reasoned opinions serves the coherence aspiration of the law in at least two ways: First, the labor of the negative reduces the chances that constructions of the law that have major flaws or inconsistencies built into the arguments supporting them will prevail. Second, since every position must be a reasoned one within the given framework of the law, it must be one that somehow fits into the overall structure of the law along coherent lines. It thus protects against incoherent “checkerboard” treatments114 of hard cases. It is the combination of reasoned disagreement and the non‐rational decision‐making mechanism of counting reasoned opinions that provides for both in hard cases: a decision and one – of multiple possible – coherent constructions of the law. Pure non‐rational procedures – like flipping a coin – would only provide for the decision part. Pure argumentative procedures – which are not geared towards a decision procedure – would undercut the incentive structure of our agonistic disagreements.115 In the face of unresolvable disagreements endless debates would seem an idle enterprise. That the debates are about winning or losing helps to keep the participants engaged. That the decision depends on counting reasoned opinions guarantees that the engagement focuses on rational argumentation. No plain non‐argumentative procedure would achieve this result. If the judges were to flip a coin at the end of the trial in hard cases, there would be little incentive to engage in an exchange of arguments. It is specifically the count of reasoned opinions which provides for rational scrutiny in our legal disagreements and thus contributes to the rationales discussed above. 2. THE SEMANTICS OF AGONISTIC DISAGREEMENTS The agonistic account does not presuppose a fact of the matter, it is not accompanied by an ontological commitment, and the question of how the fact of the matter could be known to us is not even raised. Thus the agonistic account of legal disagreement is not confronted with the metaphysical or epistemological questions that plague one‐right‐answer theories in particular. However, it must still come up with a semantics that explains in what sense we disagree about the same issue and are not just talking at cross purposes. In a series of articles David Plunkett and Tim Sundell have reconstructed legal disagreements in semantic terms as metalinguistic negotiations on the usage of a term that at the center of a hard case like “cruel and unusual punishment” in a death‐penalty case.116 Even though the different sides in the debate define the term differently, they are not talking past each other, since they are engaged in a metalinguistic negotiation on the use of the same term. The metalinguistic negotiation on the use of the term serves as a semantic anchor for a disagreement on the substantive issues connected with the term because of its functional role in the law. The “cruel and unusual punishment”‐clause thus serves to argue about the permissibility of the death penalty. This account, however only provides a very superficial semantic commonality. But the commonality between the participants of a legal disagreement go deeper than a discussion whether the term “bank” should in future only to be used for financial institutions, which fulfills every criteria for semantic negotiations that Plunkett and Sundell propose. Unlike in mere semantic negotiations, like the on the disambiguation of the term “bank”, there is also some kind of identity of the substantive issues at stake in legal disagreements. A promising route to capture this aspect of legal disagreements might be offered by recent semantic approaches that try to accommodate the externalist challenges of realist semantics,117 which inspire one‐right‐answer theorists like Moore or David Brink. Neo‐ descriptivist and two‐valued semantics provide for the theoretical or interpretive element of realist semantics without having to commit to the ontological positions of traditional externalism. In a sense they offer externalist semantics with no ontological strings attached. The less controversial aspect of the externalist picture of meaning developed in neo‐ descriptivist and two‐valued semantics can be found in the deferential structure that our meaning‐providing intentions often encompass.118 In the case of natural kinds, speakers defer to the expertise of chemists when they employ natural kind terms like gold or water. If a speaker orders someone to buy $ 10,000 worth of gold as a safe investment, he might not know the exact atomic structure of the chemical element 79. In cases of doubt, though, he would insist that he meant to buy only stuff that chemical experts – or the markets for that matter – qualify as gold. The deferential element in the speaker’s intentions provides for the specific externalist element of the semantics. In the case of the law, the meaning‐providing intentions connected to the provisions of the law can be understood to defer in a similar manner to the best overall theory or interpretation of the legal materials. Against the background of such a semantic framework the conceptual unity of a linguistic practice is not ratified by the existence of a single best answer, but by the unity of the interpretive effort that extends to legal materials and legal practices that have sufficient overlap119 – be it only in a historical perspective120. The fulcrum of disagreement that Dworkin sees in the existence of a single right answer121 does not lie in its existence, but in the communality of the effort – if only on the basis of an overlapping common ground of legal materials, accepted practices, experiences and dispositions. As two athletes are engaged in the same contest when they follow the same rules, share the same concept of winning and losing and act in the same context, but follow very different styles of e.g. wrestling, boxing, swimming etc. They are in the same contest, even if there is no single best style in which to wrestle, box or swim. Each, however, is engaged in developing the best style to win against their opponent, just as two lawyers try to develop the best argument to convince a bench of judges.122 Within such a semantic framework even people with radically opposing views about the application of an expression can still share a concept, in that they are engaged in the same process of theorizing over roughly the same legal materials and practices. Semantic frameworks along these lines allow for adamant disagreements without abandoning the idea that people are talking about the same concept. An agonistic account of legal disagreement can build on such a semantic framework, which can explain in what sense lawyers, judges and scholars engaged in agonistic disagreements are not talking past each other. They are engaged in developing the best interpretation of roughly the same legal materials, albeit against the background of diverging beliefs, attitudes and dispositions that lead them to divergent conclusions in hard cases. Despite the divergent conclusions, semantic unity is provided by the largely overlapping legal materials that form the basis for their disagreement. Such a semantic collapses only when we lack a sufficient overlap in the materials. To use an example of Michael Moore’s: If we wanted to debate whether a certain work of art was “just”, we share neither paradigms nor a tradition of applying the concept of justice to art such as to engage in an intelligible controversy.

### Reasonability

#### You’re not reasonable --- that’s the limits debate.

#### Reasonability is arbitrary and lacks a brightline---it mandates judge intervention, which outweighs because it eliminates the point of debate.

#### The combination of all reasonable interps, or reasonable affirmatives, is unmanageably large, which is a new link to limits.

#### Limits turns substance crowd-out---we can’t engage the substance of the AFF if they’re not T

## Violations

### Cybersecurity Defensive

#### Cybersecurity means protection

CISA 2019 “Security Tip (ST04-001” https://www.cisa.gov/uscert/ncas/tips/ST04-001 Cybersecurity & Infrastructure Security Agency (jshock)

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.

#### Violation – cybersecurity means defensive not offensive – ramping up offensive cyber operations isn’t T

#### Predictability – core of the topic is whether NATO should defend against cyber – OCOs good is neg ground. Their interp opens the door to affs that negotiate norms.

#### Ground – their model doesn’t distinguish between aff and neg ground – they would allow affs to say both “Ban OCOs” and “Increase OCOs”

#### Education – our model creates the best forms of education – establishes roles for aff/neg that make it more of a 50/50 win rate with clear forms of education on both sides

#### Effects T – at best they engage in deterrence by denial which may eventually decrease cyber attacks – but the brightline is whether they make NATO systems more resilient

#### 2NC - Case List

#### Cybersecurity – 5 Types

COMPtia “What is Cybersecurity?” <https://www.comptia.org/content/articles/what-is-cybersecurity> CompTIA Accessed 23 June 2022 (jshock)

CompTIA’s Chief Technology Evangelist, James Stanger says it best when he [defines cybersecurity](https://www.comptia.org/blog/what-is-the-difference-between-it-security-and-cybersecurity) as “focusing on protecting electronic assets – including internet, [WAN](https://www.comptia.org/content/guides/what-is-a-wide-area-network) and [LAN](https://www.comptia.org/content/guides/what-is-a-local-area-network) resources – used to store and transmit that information.”

Cybersecurity can be categorized into five distinct types:

* Critical infrastructure security
* Application security
* Network security
* Cloud security
* Internet of Things (IoT) security

### Security Cooperation – Extra T

#### A. Security Cooperation is limited to military purposes – basing, self-defense, and DoD

Kevin Scott, 2017, Vice Admiral, US Navy, Director – Joint Force Development, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_20\_20172305.pdf, "," No Publication (ermo/sms, Acc:6-27-2022)

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

#### B. Violation – the plan uses US agencies beyond the DoD and is not limited to defending a specific security interest

#### C. Extra Topicality is bad

A. De-justifies the Resolution – more is needed to solve, reject the resolution as insufficient.

B. Ground – the topic is written to provide negative ground isolated from the affirmative – extra T allows the affirmative to co-opt counterplan ground, even solvency arguments radically disrupt the balance of ground and predictable prep

C. Limits – justifies any topical plan plus anything – extra topical parts allow the affirmative to destroy negative ground

#### D. Extra Topicality is a voter for fairness, education, and competitive equity stated above.

### Biotech – Extra T

#### A. Biotech means genetic manipulation – it excludes biofuels

U.S.-China ESRC Economic and Security Review Commission, 2-13-2019, https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf, “China’s Biotechnology Development: The Role of US and Other Foreign Engagement" No Publication (ermo/sms, Acc:6-27-2022)

Our definition of biotechnology does not include use of non-biological processes for production from biomass (i.e., matter derived from living organisms, such as plant mass), to include the manufacture of biodiesel by chemical conversion of biomass. Most relevant to our scope are uses of organisms genetically engineered to produce a material of interest (for example, to be able to ferment specific types of biomass for fuel or to produce industrial enzymes). Use of naturally-occurring organisms for fermentation-based production may be relevant to an indirect or lesser degree; for instance, biofuels can be produced by fermentation with unmodified microorganisms. For this study of biotechnology, we are mainly interested in advances in the life sciences, usually involving genetic manipulation.

#### B. Violation – the plan expands traditional biology – it is not limited to genetic manipulation

#### C. Extra Topicality is bad

A. De-justifies the Resolution – more is needed to solve, reject the resolution as insufficient.

B. Ground – the topic is written to provide negative ground isolated from the affirmative – extra T allows the affirmative to co-opt counterplan ground, even solvency arguments radically disrupt the balance of ground and predictable prep

C. Limits – justifies any topical plan plus anything – extra topical parts allow the affirmative to destroy negative ground

#### D. Extra Topicality is a voter for fairness, education, and competitive equity stated above.

### Cyber Resilience – Extra T

#### Plan is cyber resilience not cybersecurity

Imagine IT, 7-29-2021, https://imagineiti.com/understanding-cyber-resilience/, "Understanding cyber resilience. And how it relates to security," Imagine IT (ermo/sms, Acc:6-27-2022)

Cyber resilience vs. cyber security

The difference between cyber security and cyber-resilience comes down to the expected outcomes of each.

Cyber security: Is a component of cyber resilience and consists of technology processes and measures to protect networks, systems, and sensitive data from cyber attacks. Effective cyber-security reduces the chances of cyber attacks and protects your organization from external and internal assaults.

Cyber resilience: It reflects the fact that SMB technology systems will always have flaws and weaknesses that are exploitable. It has a much bigger scope and includes cyber security and business resilience. Cyber resilience focuses on instances when your company is disrupted by things like power outages, weather emergencies, and human error. This concept helps SMBs prepare, prevent, respond, and successfully recover to pre-event business levels and processes.

Why cyber resilience?

Because traditional cybersecurity measures for SMBs are just not enough.

The truth is, harmful cyber events negatively impact SMBs every day. These events may be external or internal and may be intentional or unintentional, caused by humans, nature, or a combination of both.

It isn’t a matter of if they will get in; it is when!

Today, it’s as critical for SMBs to be able to respond and recover from security breaches as it is to be able to prevent them. Cyber resilience aims to give your organization a plan that will consider actions and outcomes before, during, and after an event.

What are the benefits:

It improves your cyber-security posture

Reduces financial losses

Maintains the trust of customers

Protects your organization’s reputation

Maintains the trust of vendors

Improves your cultural and internal processes

Maintains the trust of employees

How does cyber resilience work?

It is a strategy that is considered a preventive measure to counteract human error and security weaknesses in hardware and software. The overall purpose is to protect the organization while understanding that there will likely be insecure parts, no matter how robust security controls are.

The main components of your cyber reliance strategy should include:

Threat protection: As security solutions advance, so does the ability of the cyber-attackers to breach your system. What were once state-of-the-art solutions are now the bare minimum requirements to protect your SMB.

Recoverability: After a security incident, whether internal or external, your organization must have the ability to return to normal operations quickly.

Adaptability: Your organization must evolve and adapt to new tactics that cyber-criminals deploy. Investing in continuous security monitoring so your people can recognize security issues in real-time and take immediate action is critical.

Resilience: Your organization’s ability to effectively operate after a security breach.

The six elements of a successful cyber resilience strategy

Identify

Includes the use of attack surface management, continuous monitoring to identify irregularities and breaches before they cause any significant damage

Protect

A good cyber resilience strategy protects your system, your applications, and your data. You need to ensure that only authorized users can access your system.

Detect:

You need the ability to detect when someone is trying to act maliciously against your systems and can come externally or internally.

Respond

You also need to Developing an incident response plan, identifying roles and responsibilities to ensure you can operate normally even after a cyber-attack.

Recover

Ability to quickly store digital and technology platforms and adapt and recover mission-critical systems to avoid disruption

Anticipate

You want to rely on automation, machine learning, and adaptive cyber-threat detection to address future threats

A digital transformation mindset

Cyber resilience goes hand in hand with digital transformation. Both require a similar way of thinking. Cyber resilience recognizes that the outdated notion of SMBs having impenetrable defenses be abandoned. Cyber resilience assumes that attackers will be successful, so measures must be in place to prevent, respond, and recover from these attacks.

For those measures to be successful, cybersecurity needs to be everybody’s responsibility, and cyber best practices need to be inserted into all aspects of the organization.

As the pandemic has changed all aspects of your business, it has accelerated the need for digital transformation in SMBs. As digital transformation has accelerated, so too have efforts to boost cybersecurity. Businesses realize that cyber-resilience is critical if they are to survive the effects of COVID.

Digital transformation requires a greater dependency on IT. Because SMBs are more dependent on IT, they need strong cyber resiliency. Without it, a business can’t be confident of its ability to continue operations when faced with increased cyber threats that accompany increased dependence on IT.

Do you put cyber-security first?

Is cyber-security front and center of your strategies, or are you just paying it lip service? Do you have a security-first culture, and does your leadership put cyber resilience in the same “box” as operational performance?

Like measuring your business’s ROI and profitability, cyber-security and cyber resilience must be a strategic priority that you track and measure.

Closing thoughts:

Cyber resilience is an organization-wide strategy that actively monitors threats, risks, and weak points. It is a collaborative strategy that extends to everyone your company connects with.

Organizations should keep in mind that cybersecurity is not the same as cyber resilience. When cybersecurity fails, you must have a plan in place to assess the problem and have the ability to recover quickly back to pre-cyber-event status.

#### B. Violation – the plan increases cyber resilience – it seeks to respond to and recover from cyber attacks, not merely to prevent them

#### C. Extra Topicality is bad

A. De-justifies the Resolution – more is needed to solve, reject the resolution as insufficient.

B. Ground – the topic is written to provide negative ground isolated from the affirmative – extra T allows the affirmative to co-opt counterplan ground, even solvency arguments radically disrupt the balance of ground and predictable prep

C. Limits – justifies any topical plan plus anything – extra topical parts allow the affirmative to destroy negative ground

#### D. Extra Topicality is a voter for fairness, education, and competitive equity stated above.

### AI – Robots

#### A. AI excludes robots – it supplements humans, not replaces us

Nirmal Narayanan, 2-19-2019, https://www.ibtimes.co.in/will-artificial-intelligence-take-away-jobs-humans-792246, "Will Artificial Intelligence take away jobs from humans?," IBTimes India (ermo/sms, Acc:6-27-2022)

As panic surrounding job loss due to artificial intelligence reaches new levels, experts have clarified that AI will not take away jobs from humans. Experts revealed that artificial intelligence is actually supplementing human intelligence all across the spectrum, and it will actually make the life of humans easy.

In a recent post written on Science Focus, Dr Peter Bentley, a British author and computer scientist based at University College London revealed that artificial intelligence is not the same as factory automation or robots. Bentley believes that AI is very similar to the internet, and it is basically an enabling technology which creates new jobs in various industries.

#### B The plan increase security cooperation in the field of robotic technology

#### C. Standards.

#### 1. Limits- Robots do thousands of tasks without developing the capacity to learn – the plan’s precedent makes any mechanical or industrial process topical.

#### 2. Core NEG ground- the NEG should be able to get links related to autonomous machine learning policy, but those links don’t apply to old school robotics.

#### D. Topicality is a voting issue for fairness, education, and iterative testing.

### Substantially 80%

#### A. “Substantially" means 80 to 90%—government definitions prove.

**Curtin, 2003** (John T. Curtin, Judge, United States District Court for the Western District of New York, Gateway Equipment Corp. -vs- United States of America, United States District Court for the Western District of New York, lexis)

**The government** cites Webster's Ninth New College Dictionary for the definitions of "limit" and "impairment" as suggesting "meanings equivalent to restriction and reduction, respectively." Item 30, p. 3, n.1. **It posits that the word "substantially" suggests "an order of magnitude equivalent to 80% or 90%**." Id. It concludes that "using those definitions, 'substantially limited' and 'substantially impaired' means that there must be an 80%-90% restriction and/ or reduction of use by virtue of the design of the CB-4000." Id.

#### B. The plan names a subset under bio/cyber/AI – far less than the whole category

#### C. Standards.

#### 1. Limits- Allowing minor aff means cases can be about any desk or program in NATO – some have under 100 people assigned. The number of small tweaks is infinite.

#### 2. Core NEG ground- the NEG should be get DA links from NATO dramatically increasing its security cooperation, not limited to links specific to the aff’s content.

#### D. Topicality is a voting issue for fairness, education, and iterative testing.

### Increase (previously existing 1NC)

#### A. Increase requires making something previously existing greater.

**Buckley et al., 2006** (Jeremiah, attorney, Amicus Curiae Brief, Safeco Ins. Co. of America et al v. Charles Burr et al., google)

First, the court said that the ordinary meaning of the word “increase” is “to make something greater,” which it believed should not “be limited to cases in which a company raises the rate that an individual has previously been charged.” 435 F.3d at 1091. Yet the definition offered by the Ninth Circuit compels the opposite conclusion. **Because “increase” means “to make something greater,” there must necessarily have been an existing premium**, to which Edo’s actual premium may be compared, **to determine whether an “increase” occurred**. Congress could have provided that “ad-verse action” in the insurance context means charging an amount greater than the optimal premium, but instead chose to define adverse action in terms of an “increase.” That def-initional choice must be respected, not ignored. See Colautti v. Franklin, 439 U.S. 379, 392-93 n.10 (1979) (“[a] defin-ition which declares what a term ‘means’ . . . excludes any meaning that is not stated”). Next, the Ninth Circuit reasoned that because the Insurance Prong includes the words “existing or applied for,” Congress intended that an “increase in any charge” for insurance must “apply to all insurance transactions – from an initial policy of insurance to a renewal of a long-held policy.” 435 F.3d at 1091. This interpretation reads the words “exist-ing or applied for” in isolation. Other types of adverse action described in the Insurance Prong apply only to situations where a consumer had an existing policy of insurance, such as a “cancellation,” “reduction,” or “change” in insurance. Each of these forms of adverse action presupposes an already-existing policy, and **under usual canons of statutory construction the term “increase**” also **should be construed to apply to increases of an already-existing policy**. See Hibbs v. Winn, 542 U.S. 88, 101 (2004) (“a phrase gathers meaning from the words around it”) (citation omitted).

#### B. Violation: the AFF creates a NEW form of security cooperation – it doesn’t exist now

#### C. Standards.

#### 1. Limits- previously existing forms of assistance create a stable, finite literature base, which increases argument depth and clash. New forms of security cooperation could include new enemies, new NATO members, new non-geopolitical threats, or new solutions to any known problem.

#### 2. Core NEG ground- the NEG should be able to reform current programs, to test the word “increase” in the resolution. These CPs are key to topic education and specific NEG strategy.

#### D. Topicality is a voting issue for fairness, education, and iterative testing.