# AFF T-cybersec (draft)

### 2ac – oco’s=cybersec

#### W/M: OCO’s defend forward which is defensive.

Garromone ’19 Jim Garromone, journalist for the US Federal Government’s Depart of Defense. “Esper Describes DOD,” *U.S. Department of Defense*, <https://www.defense.gov/News/News-Stories/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/> Accessed 27 June 22

''Training to operate in a degraded environment is now regularly built into our exercises, and our service members are quickly becoming aware of our cyber vulnerabilities,'' the secretary said. But winning in cyberspace requires an offensive strategy, Esper told the summit audience. ''We need to do more than just play goal line defense,'' he said. ''As such, the department's 2018 Cyber Strategy articulates a proactive and assertive approach to defend forward of our own virtual boundaries. ''Just as we do on land, at sea, and in the air, we must posture our forces in cyberspace where we can most effectively accomplish our mission,'' he continued. ''Defending forward allows us to disrupt threats at the initial source before they reach our networks and systems. To do this, we must be in a position to continuously compete with the ongoing campaigns being waged against the United States. Not only does this protects us day-to-day, but enacting this strategy builds the readiness of our cyber warriors so they have the tools, skills and experience needed to succeed in conflict.''

#### C/I: Cybersecurity can be offensive or defensive—there’s no relevant brightline

**Stephen M.W 21**, technology, business, and compliance journalist for TechGenix “The Dangers of Offensive Cybersecurity,” *TechGenix*, 04/14/2021, <https://techgenix.com/dangers-of-offensive-cybersecurity/>.

Governments and corporations have realized that a passive, defensive approach to cybersecurity has limited success. Instead, there is growing recognition of the need for persistent engagement that infiltrates and degrades an attacker’s systems and infrastructure. Also known as hacking back, offensive cybersecurity operations refer to the proactive attack on hackers to cripple or disrupt their operations and deter future attacks. Offensive cybersecurity has the advantage of stopping or preempting cyberattacks before they impair target systems or penetrate cyber-defenses. The operations can also introduce uncertainty in an attacker in addition to influencing their behavior.

#### Prefer our definition---

#### Limits---it excludes actions that tangentially affect cyber security, requiring a direct framework for cyber security operations: OFFENSIVE or DEFENSIVE.

#### Ground---overarching NATO governance guarantees large change, ensuring link uniqueness

#### Their ground arg is terrible – require them to name specific das and counterplan that offensive rather than defensive cyber security spikes out of.

#### Predictability – Their interp isn’t exclusive all cybersecurity operations can technically be considered defensive🡪 “defending forward” see our we meet arg above

#### Functional limits check – NATO Withdrawal CP & NATO turns ensure neg always has ground. The neg ran multiple turns specific to our aff and DAs with direct links - solves any abuse.

#### Reasonability over competing interps --- solves race to the bottom and arbitrary limits.

### 1AR

**W/M Ext: OCO’s are active defense.**

**Niknamian n/d** Dr. Sorush Niknamian is a professional in Terrorism Affairs and an ACP Chapter member in United States Army and Air Force. Active Member of IMRTC-USA (International Management Research and Technology Consortium Research) as Advisor, Referee and Professor at IMRTC-USA (International Management Research and Technology Consortium Panel). He is a Service Member of Modern Military Association of America. “Active Defense” file:///C:/Users/kweis/Downloads/ACTIVE\_DEFENSE%20(1).pdf

Additionally, "active defense measures" are often another term used to define and refer to offensive cyber operations (OCOs) or computer network attacks (CNAs). Some have defined active defenses as including of deception or honeypots, which seek to confuse attackers with traps and advanced forensics. Examples of such honeypot technologies include Illusive Networks, TrapX, Cymmetria, Attivo, and others. Other types of active defenses might include automated incident response, which attempts to tie together different response strategies in order to increase work for attackers and decrease work for defenders. The Department of Defense defines active defense as: "The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[12] This definition does not specify whether it refers to physical actions, or cyber-related actions. Recently, the Department of Homeland Security and financial institutions have identified Active Defense as a top priority for security industrial infrastructure systems. As part of a broader push for greater resiliency, the National Institute of Standards and Technology 800-160 Volume 2 framework has gone further, providing guidance on standardization for active defense.

…This capability can be required to guarantee one's freedom of action in the cyber domain. Cyber-attacks can be launched to repel an attack (active defense) or to support the operational action. The distinction between active cyber defense and offensive cyber operations (OCO) is that the later requires legislative exceptions or executive prerogative to undertake. Hence, offensive cyber capabilities may be developed in collaboration with industry, or facilitated by private sector but operations are led by nation states. There are some exceptions, notably in self-defense or with judicial authority (civil warrants) or assisting law enforcement.

#### C/I Ext : cybersecurity is offensive and defensive.

#### DeSimone 22, John DeSimone is president of cybersecurity, intelligence, and services at Raytheon Intelligence and Space which is an American aerospace and defense company directly contracted by the US DoD, “An Offensive Mindset Is Crucial for Effective Cyber Defense” *Help Net Security*, 05/11/2022, <https://www.helpnetsecurity.com/2022/05/11/offensive-mindset-cyber-defense/>

As ransomware attacks continue to increase and cybercriminals are becoming more sophisticated, the federal government has implemented a more proactive approach when it comes to cybersecurity. As evidenced by its stated strategy to adopt a [zero trust architecture](https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/), the federal government is taking measures to reduce the risk of cyberattacks against its digital infrastructure, and setting specific security goals for agencies to quickly detect, isolate and respond to threats. This approach is also exemplified by the extension of its [Industrial Control Systems Cybersecurity Initiative](https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/), which is aimed at facilitating the deployment of technologies and systems that provide cyber-related threat visibility, indicators, detections and warnings to the water infrastructure.

An offensive mindset is key to ensuring the best cyber defense. To ensure success, there are three main components for organizations to consider when developing a defensive strategy based on an offensive cyber model: re-envisioning recruitment, thinking like a hacker, and promoting offensive training in tangent with defensive training.

### Standards---Not Much Lit

#### Security coop receives little attention

Nathan L. Fenell 11, Operations/Administration Management Professional and Military Veteran with over 20 years of experience in the United States Marine Corps, “Security Cooperation Poorly Defined,” University of San Francisco, 12/12/11, <https://repository.usfca.edu/cgi/viewcontent.cgi?article=1020&context=thes>

The literature review will establish the premise that security cooperation as an academic area of study receives little attention.17 The paucity of literature on the subject contributes to the current misunderstanding of the definition as well as its improper strategic utilization. Authors who participate in scholarly conversation on the topic fall into one of two categories, doctrinal use or modern misconception.18 The contradictory nature of the literature further supports my hypothesis that the definition of security cooperation is frequently not applied in Afghanistan.

#### Even so the lit is on our side, the USFG’s main form of cybersecurity strategies are OCO’s (offense/defending forward).

#### Hon, Lamar, Smith et al. ‘16, “*COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY*,” p. 118 1/8/2016.

To follow up on Mr. Swalwell’s question, he was talking about being on offense and the prosecution, but from the technology side, is it all defensive or are there proactive ways to combat hackers before they make their attack? Mr. SCHNEIDER. I mean, I think there’s a set of approaches that are not defensive and are much more proactive that are in place today and will continue to expand. So one example is around things like honey pots, so if the bad guys are attacking you and you give them a place that looks like a legitimate part of your infrastructure that they go to and spend all of their time and energy attacking, you protect your real assets and you’re able to study what they’re doing at the same time. There’s also things like shock absorbers where the harder an attacker hits you with traffic, the more you slow them down and do things like tar pitting. So there’s a whole set I think of defensive and more proactive defensive measures that aren’t offensive, don’t go directly after the attackers that are in place today and are actually very successful within the enterprise.

### A2 deterrence by denial vs. punishment

#### NATO uses both deterrence by denial & punishment- distinction is irrelevant in this context.

**Paulauskas ‘16,** PhD in Philosophy & International Relations and is Senior Strategy Officer in the Allied Command Transformation as well as a former NATO employee. “NATO Review - On Deterrence” *NATO Review*, 08/05/2016, <https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html>

Deterrence is a relatively simple idea: one actor persuades another actor – a would-be aggressor – that an aggression would incur a cost, possibly in the form of unacceptable damage, which would far outweigh any potential gain, material or political. The involvement of at least two actors makes deterrence a complicated social interaction. It is very much about human nature, psychology and basic human emotions: fear, courage, trust, lust for power, and revenge. Elevate all this to the level of state actors, with all the intricacies inherent in statehood and statesmanship, add the stakes of national survival, add nuclear weapons to the mix, and deterrence becomes a highly complex, volatile, intangible, but also combustible concept. From deterrence by denial to denial of deterrence – and back. During the Cold War, NATO pursued deterrence by punishment and deterrence by denial. Deterrence by punishment was based on the notion of ‘unactable damages’, including through massive nuclear retaliation for any Soviet attack – conventional or nuclear. Deterrence by denial was about making it physically difficult for the aggressor to achieve his objective, which NATO pursued through forward defense at its eastern border with the Soviet Union.