Ryan and I affirm:

[The benefits of the United States federal government's use of offensive cybersecurity operations outweigh the harms]

Contention 1 is Counter-Terrorism

Currently, **Wise '19 of the Hill finds one week ago** that the US military has withdrawn troops from Northern Syria.

As a result, **Kirkpatrick '19 of the New York Times** finds that Trump's troop pullout removes the spearhead of the campaign to defeat ISIS, thus giving ISIS their biggest win in more than 4 years.

Critically, **Vavra '19 of Cyberscoop** confirms that without physical troops or drones, our only option to stop ISIS is offensive cyber operations because kinetic options are no longer available.

Cyber operations prevent the rise of ISIS in two ways:

First, blocking their media capabilities:

Cyber offensives have already proven successful. **Bate '17 of the American Security Project** writes that offensive cyber operations have already inhibited communication between ISIS members and brought down media platforms critical to recruitment, concluding that ISIS's international recruitment collapsed after US OCOs.

Critically, **Castleberry '19 of George Washington University** explains that publicity and digital technologies are the lifeblood of terrorist groups, and since these assets are key to regrouping and planning physical attacks, media resurgence is a <u>precursor</u> to ISIS's physical revival.

Second, blocking financing

Temple-Raston continues that a key component of JTF-Ares is to disrupt crucial financial links and banking options for ISIS.

Overall,

Rogers '18 finds that American cyber efforts played an important role in reducing ISIS's territory by 98%.

The impact is preserving Middle Eastern stability:

Without OCOs, ISIS would be able to rise to power. Problematically, **Jamison '16 of NBC** finds that ISIS has killed more than 18,000 civilians and displaced millions. (1:37)

Contention 2 is a Peaceful Alternative

Segal '10 of the Council of Foreign Relations reports that in the early 2000s, Iran was pushing to weaponize its nuclear program, revealing a second uranium enrichment facility in 2009 that stoked fears of Iran's potential to produce a nuclear weapon.

Such developments were perceived as dangerous to Israel, as **Meir '10 of the International Journal for Peace** confirms that Israeli leadership viewed the Iranian nuclear program as an existential threat, bringing an Israeli attack on Iran's nuclear facilities to the forefront of considerations.

Thankfully, American use of offensive cyber operations provided a peaceful alternative. **Libicki '14 for the FIC** concludes that, had the US not used cyber operations and Stuxnet against Iran's nuclear facilities, Israel would have countered Iranian nuclear development with air raids.

Moreover, **Farwell '12 of Georgetown University** indicates that Stuxnet also set the precedent to the world that cyber weapons are a viable alternative to a kinetic strike preventing the risk of future escalation.

If Israel did strike, **Turse '13 of Mother Jones** reports that the air strike would have killed over 7 million people and devastated Iran's healthcare infrastructure. (2:50)

Contention 3 is Taiwan

Spencer '19 for Taiwan News writes that Taiwan is under constant cyber-attack from China: it suffers as many as 10 million cyber attacks a month.

Critically, Taiwan's defenses are weak, exacerbating the problem. **Bloomberg '18 reports:** Taiwan's cyber defenses cannot overcome mainland China's drive to isolate Taiwan diplomatically.

American cyber operations are key to alleviating this issue. **Chan '19 for the Asia Times** writes: the Americans host joint military exercises with Taiwan where they intentionally cyber attack

Taiwan in order to strengthen their responses and patch holes in their system, making them defend better against Chinese attacks.

The impact is preventing a bloody reunification.

As tensions begin to rise, **BBC '19** explains that China's main goal with Taiwan is to reunify with mainland China, finding that China will most likely use cyber strikes to undermine Taiwan.

Without the US, **Spencer, previously cited,** writes: cyber attacks are the *most likely* and *cost-effective* means that China could bring Taiwan to its knees. Thus, cyber security is Taiwan's most pressing national security issue.

Due to Taiwan's hardline approach against reunification, cyber strikes would instigate conflict. **Kristof '19 of the New York Times** writes that a China-Taiwan war would begin with a cyber attack against Taiwan's grid, concluding that China may act recklessly against Taiwan in the next few years, pulling the US into a conflict as well.

Critically, **Stone Fish '17 of Slate Magazine** writes that successful occupation of Taiwan would cement China's regional domination and undermine the US' position in Asia. Thus, a brutal war would ensue, ultimately causing millions to die.

Thus, we affirm.