Ryan and I negate:

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

Contention 1 is Global Cooperation

Currently, cyberspace is the world's Wild West. **Ferrante '19 of the Hill** explains that current cyber attacks are taking place in a lawless battlefield with very undefined rules.

America's offensive cyber operations are at fault. **Goldsmith '11 of Harvard Law School** explains that the US is widely regarded as a major source of cyber attacks and the major spur of the global cyber arms race. This causes foreign countries to lack trust in the US, leading to minimal concessions in diplomatic efforts.

Thus, **Goldsmith concludes** that American talk of a cyber-arms agreement is empty until the US clamps down on our cyber activities, furthering that the US will not get concessions from our adversaries until we restrain ourselves.

Cyber governance is critical to world peace:

Sangiovanni '17 of Cambridge University describes that such a cyber agreement would define rules as to what constitutes an act of war or a proportional response, preventing states from disproportionately retaliating and escalating conflict.

Merely negotiating is enough to have an effect. **Sangiovanni concludes** that the negotiation process itself can de-escalate existing conflicts, bringing political visibility to cyberspace and the beginnings of norms among countries. (1:00)

Contention 2 is Exploiting American Code

Bellovin '19 for the Journal of Cybersecurity notes that enemies copy American cyber weapons by tracking how the US infiltrates their network weaknesses and using this information to reconstruct the code. Once a cyber weapon has been reverse engineered, making more of the same is far easier and cheaper than manufacturing their own cyberweapons.

As a result, **Doffman '19 of Forbes** reports that state-sponsored hacking groups aim to capture and exploit American cyber weapons to achieve the same capabilities as the US RATHER THAN investing in their own cyber programs.

The impact is halting pharmaceutical innovation

Douthwale '19 from the EPM finds that the pharmaceutical industry is now the top target for cyber criminals around the world, as these companies are increasingly digitized and store valuable data online.

Consequently, **Stienberg '19 of CNBC** explains that since almost half of cyberattacks aimed at small businesses who are unprepared to defend themselves, cyberattacks cost businesses hundreds of thousands of dollars and 60% of small businesses who are victims of a cyber attack go out of business within 6 months.

Critically, **Taylor '19 of Securing Industry quantifies** that biopharmaceutical companies face 71 attacks per company on average over a three-month period.

These start-ups are key to drug innovation, as **Ioannou '18 of CNBC writes** that start-ups have become the main drivers of drug innovation, accounting for 63% of all new prescription drug approvals over the last five years.

Thus, every company that folds is a step backwards in the face of a solution, as **Samuel '19 from Vox** finds that 700,000 people die every year due to a lack of new antibiotics. (2:25)

Contention 3 is Iran

Greenberg '19 of WIRED finds that historically, Iran was a target for cyber attacks, but after the massive 2009 American offensive operation named Stuxnet, Iran pivoted to become an aggressor and develop their own cyber capabilities.

American OCOs have increased Iran's cyber proliferation by Incentivizing Development:

Kumar '15 for the Atlantic Council finds that Stuxnet exposed Iran's poor cyber capabilities, causing the nation to vow to never again be defenseless and increase its cyber security budget by 1200%.

Overall, **Brunner '19 of ASU** finds that Stuxnet taught Iran how to use cyberspace to their advantage, concluding that Iran's rapid development of cyber offensives stem from US OCOs.

Critically, **Fazzini ‘19 of CNBC** confirms that since Stuxnet, Iran has become one of the most significant cybersecurity powers.

The impact is preventing global catastrophe

Unlike other US adversaries, **Kennedy ‘19 of the National Interest** reports that Iran is less cognizant of red lines, seen by their brazen attacks carried out in recent years.

With their new capabilities, **O’Flaherty ‘19 of Forbes** explains 2 weeks ago that Iran has begun to target critical infrastructure and power grids, increasing their attacks by 10 times against the US.

Problematically, **Rovner ‘17 of American University** confirms that offensive cyber operations are impossible to control, concluding that these operations could inadvertently cause enormous collateral damage to other non-targeted critical infrastructure.

Straub ‘19 of North Dakota State University concludes that a cyber attack against critical infrastructure in one area that spreads to others would cause significant damage and rival death tolls of a nuclear weapon as water, food and power go down.

Thus, we negate: (3:57)