We negate, Resolved: The benefits of the United States federal government's use of offensive cyber operations outweigh the harms.

Our first argument is that Defense wins Championships.

Offensive cyber operations have been on the rise. Ken Dilian for NBC News reports last year: the U.S. military has stepped up its..., of foreign computer networks...the military...has conducted more operations in the first two years of the Trump administration than it did in eight years under Obama.

However, as offensive cyber operations have increased, they have traded off with more important *defensive* cyber operations. Josephine Wolff of the New York Times in 2018 finds: The...shift to an offensive approach...will...detract resources and attention from the more pressing issues of defense and risk management.

Aside from just strategy, prioritizing offensive cyber operations also drains resources from defense. Jennifer Li of the RAND Corporation explains in 2015: [the personnel for] offensive cyber warfare are distinctly different from those needed for defensive cyber warfare...only 2 percent [now work] in defensive operations.

The cumulative harm of this cyber operation tradeoff is losing the long term cyber war,

As John Donnelly of Market Intelligence explains: If cyber defenses are lacking, U.S. leaders not only will lack confidence in the reliability of their offensive weapons but will also worry that any U.S. offensive response could trigger a potentially debilitating cyber counterattack.

As a result, American cyber operations cause more harm than good in the field. Valeriano quantifies: Only...4 percent [of offensive cyber operations]...have produced even a temporary...concession…

The only route to form the best offense is a good defense. Gary McGraw writes in his 2016 book, "Conflict in Cyberspace": building systems properly from a security perspective...deals with.. .offensive cyber-warfare operations...Reducing vulnerabilities...reduces the risk of a successful cyber attack. [In Iran, for example, the defense systems have already neutralized 33 million attacks.]

This is crucial to protecting America's stability, as global cyberterror has been increasing. The Global Terrorism Index in 2018 reports: terrorist use of cyberattacks is the new frontier, as the centrality of cyberspace to everyday life has made cyberattacks more threatening and frequent. Allowing attacks to continue would wreak havoc on the country. Gary Wiemann for the Institute for Peace concludes: sophisticated cyberterrorists [can and will eventually] electronically break into computers that control [the country], wreaking havoc and endangering not only millions of lives but national security itself.

Our second argument is that offensive cyber operations prevent global solutions.

While our military operations are being brought into the realm of cyberspace, America is trying to seek peace. Lee Hartman on the Bureau of Global Affairs writes in 2018: the United States is leading a global effort to counter bad actors. [America has created agreements such as the Asia Pacific Economic Cooperation and the Organisation of American States.]

However, while countries used to sign onto US initiatives, they do not actually listen anymore. The Atlantic's Amy Zegart reported this February: [American] cyber norms have been contested.. by China, Russia, and their autocratic buddies...Cyber competition is here and it is getting worse, threatening to undermine democracies, upend the international order, and erode American power.

American cyber attacks are the reason for these failures of long term agreements. Jack Goldsmith for The New Republic concludes: [America] is widely viewed as--and actually is--a [root cause] of cyber attacks and a major spur to the cyber-arms race. Until [the government eliminates public and private offensive activities]...talk of a cyber-arms agreement is empty talk.

Thus, the impact of offensive cyber operations is reducing global development.

In a world in which America did not use offensive operations, effective agreements would be created. Tim Mauer for the Carnegie Center reports: [In] 2015...China and President Obama...agreed to [fight] cybercrime and related issues...after the Obama administration finalized the agreement..the number of Chinese operations...rapidly plummeted. Instead of 65 per month, by late 2015 there were less than five [which saved billions of dollars].

Without agreements, cyberspace is going in the wrong direction. Elena Cherneko for the Council on Foreign Relations writes: cyber threats...precipitate massive...damage, and international efforts need...to account for this new reality...cyberattacks already cost the global economy $300 billion annually, and...will total $8 trillion over the next five years. [This has meant millions in poverty, as countries lose a major sector of their economic growth.]

Because cybersecurity should be about creating peace rather than war, we are proud to negate.

Even worse, a lack of defense causes the infrastructure of cyber operations to be weaker. Zak Doffman of Forbes explains this year: The U.S. is vulnerable to attacks on its networked technology infrastructure...there have been changes in the defensive technology that allow [countries to fight back