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

Our sole point of contention 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 drastically stepped up its...hacking 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.

All in all, this tradeoff should be expected. Tyler Moore at the Center for Computation writes: The notion of a trade-off between offensive and defensive capacity in the national security context is not new. In WWII, for example, the Allies allowed some German attacks to succeed in order to hide their strategic advantage in...radar technologies.

As a result, the greatest harm of offensive cyber operations is not what they cause but what they remove. We should prefer defense the context of war for two reasons.

The first is effectiveness.

A study by Brandon Valeriano of the Cato Institute this year found: Only...4 percent [of offensive cyber operations]...have produced even a temporary...concession. [For example, the US's recent cyber attack on Iranian missiles was reported to have done no harm.]

On the other hand, defensive operations are extremely successful preventing attacks. KGary McGraw writes: building systems properly from a security perspective...can lessen the possibility of cyber war. [In Iran, the defense systems have already neutralized 33 million attacks.]

The second is through deterrence by denial.

As PW Singer of Foreign Policy Magazine explains in 2019: "deterrence by denial" [is] making attacks less probable by reducing their likely value. In cybersecurity, this is the magic idea of resilience. [If someone steals from you, you don't steal back-- you upgrade your security.]

Thus, Valeriano writes: Cyber deception and defense produce a position of advantage. New hardware and endless software updates produce new vulnerabilities at a continual, even if variable, rate. The only true security comes from making adversaries doubt the wisdom of attack.

As the United States has transitioned away from defense, attacks have only increased. An article in the Security Magazine reported: Sixty-one percent of [American] firms suffered a cyber attack in the past year, compared to 41 percent the year prior.

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

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 tensions rise, the current cyber strategy misses the mark on protecting the nation. The Worldwide Threat Assessment this year predicts: financially motivated cyber criminals" [will] target the U.S. [soon]..this could "disrupt U.S. critical infrastructure in the health care, financial, government, and emergency service sectors.

As a result, there will be long term escalation. Donnelly continues: Doubts about U.S. defense capabilities could cause [our] president to more quickly turn to nuclear weapons...the president could face an unnecessarily early decision of nuclear use [to protect the country].

Now more than ever, the US has its finger on the trigger. David Sanger of the New York Times in 2018 writes: A ...[new American] nuclear strategy ...would permit the use of nuclear weapons to respond to...cyberattacks...[The policy] will make nuclear war a lot more likely.

Any attack would be devastating. If the US struck back against Russia, a country who has already hacked US power grids, David Mosher of Business Insider projects: More than 91 million people...might be killed or injured within three hours following a single "nuclear warning shot"

Because phrases like "the best defense is a good offense" are best left for sports, not international politics, we are proud to negate.