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

Our sole contention is Left of launch.

Currently, the US is conducting offensive cyber operations, or OCO's.

According to **Ackerman of the Daily Beast in 2018**, Senior U.S. military officers have sought what's called "left of launch" options to disable adversary missiles before they leave the launchpad by developing digital weapons to corrupt or disable launch controls, guidance systems or aspects of the missile supply chain.

Problematically, this causes conflict to manifest in two ways.

First is with Iran

In the past the US has attacked Iran through Stuxnet.

Holloway of Stanford continues in 2015 that over fifteen Iranian facilitates were attacked and infiltrated by this worm. It destroyed 984 uranium enriching centrifuges. By current estimations this constituted a 30% decrease in enrichment efficiency.

However, **Glaser of the CATO institute reports in 2017** that later assessments said it only delayed Iran's overall nuclear program by a matter of months.

Not only are cyber attacks ineffective, but they also spur the very actions they sought to prevent.

Glaser furthers Iran actually increased the number of operating centrifuges and increased production of low-enriched uranium. They were spurred to boost production in the face of cyber attacks.

McKay of Gizmodo reports in 2019 Iran's Atomic Energy Organization has increased production of low-enriched uranium to levels that will exceed limits imposed in the 2015 nuclear deal between Iran and other world powers.

Problematically, Iran could restart to sell this uranium to terrorist groups

Emerson of the JPC writes Iran could provide a nuclear weapon to any of its proxy terrorist organizations in conflict with Israel. Iran already has smuggling routes to the group. Recently, it smuggled massive quantities of weapons to Hezbollah in Lebanon.

Wilson finds in 2017 depending on where and when it was detonated, the bomb could leave the heart of a major city a smoldering radioactive ruin, killing tens or hundreds of thousands of people and

wounding hundreds of thousands more. The idea of terrorists accomplishing such a thing is not out of the question.

Brill of the New York Times continues in 2012 an act of nuclear terrorism "would thrust tens of millions of people into dire poverty" and create "a second death toll throughout the developing world."

Second is with North Korea

North Korea sees their nuclear arsenal as the key to regime survival because it prevents the US from attacking them.

Ji of the Arms Control Association in 2017 explains North Korea has no intention of giving up its nuclear weapons capabilities. Their policy has been influenced by "U.S. schemes to overthrow independent countries" by "weakening their military self-defense capabilities.

This is why Panda of Foreign Affairs furthers in 2018, The new reality of North Korea's capabilities—including the threat to the continental United States—demands careful thought about how Washington might influence nuclear decision-making in Pyongyang. A stable deterrence relationship requires making Kim Jong-Un feel secure about his arsenal, not insecure.

Lin of Brookings finds in 2018 cyber attacks carry a unique risk in escalating conflicts**.** When both sides believe that defending against attacks is difficult, the initiator of conflict gains important warfighting advantages, creating incentives to strike first. The use of cyber weapons heightens these dynamics since cyberattacks are likely to precede conventional strikes by hours or days.

Panda continues, any perception that Washington is trying to disable North Korea's force could quickly convince Kim that he is in a "use them or lose them" situation. This could result in a much larger nuclear strike at the outset of a conflict than anyone anticipates, as Kim fears that he has a limited window to fire not only his theater-range missiles but also ICBMs at the United States.

Indeed, after 2012 in which **Lewis of The Chatham House writes in 2019**, that the United States has claimed to use this form of cyber attack against North Korea, **Poghani of PBS in 2019 finds** the pace of ballistic missile tests and nuclear tests has significantly escalated under Kim Jong Un.

The impact is Kim's contingency plan:

Panda warns, U.S. interest in left-of-launch capabilities might push North Korea to seek some sort of mechanism ensuring that Kim's untimely demise, or even rumors of it, would result in the release of any and all nuclear weapons that were available to the Korean People's Army.

Zagurek of 38North quantifies in 2017, Nuclear detonations over Seoul and Tokyo could result in as many as 2.1 million fatalities and 7.7 million injuries.

Save lives, and negate.

OTHER IMPACT:

chemical weapons:

As the **International Crisis Group** explains, “current North Korean doctrine states that every third [artillery] round fired would be a chemical round.” Indeed, **South Korea’s** own government estimates that the North has up to 5,000 tons of chemical agent stockpiled.

Critically **Kirby of the Bulletin of the Atomic Scientists** finds in June 2017 that due to the spreading effects of chemical attacks, even if South Korea could strike down all of North Korea's artillery, the attack would still kill 2.5 million people.

Save lives and negate.