We affirm.

Our Sole Contention is Winning in the Gray Zone.

Currently, our adversaries are operating in the "gray zone" between war and peace.

The Heritage Foundation explains that North Korea, Russia, Iran, and terrorists are making small, incremental acts of aggression so that they can gain influence without risking an American military response.

*Thankfully, offensive cyber operations solve in **three ways**.*

Subpoint A is Deterring Conflicts.

The Foreign Policy Institute explains that ignoring low-level aggression in the gray zone will embolden our enemies to test our limits until we are eventually forced to start a military conflict.

For example, if we don't show Iran consequences for attacking a US drone, the next attack could be the one that sparks a war.

Another example is Russia. John Carlin of CSIS explains that absent consequences from the US, Russia would gradually increase its aggression until the US is forced to take greater action. Thus, he concludes that the US needs offensive cyber capabilities to deter Russia and prevent military conflict.

Overall, the Army War College found that 16 countries around the world went through their own gray zones conflicts; and, of those 16, 12 resulted in miscalculations leading to war.

This would be disastrous, as Peace Research Institute finds that each year of a major conflict causes 2,500 deaths directly and thousands of civilian casualties.

Fortunately, American offensive cyber-operations stop low-level aggression from escalating. The Atlantic Council concludes that offensive cyber capabilities are a way to show our enemies consequences without crossing the threshold and starting a conflict.

Historically, they find that the US used cyber-attacks to respond to Iran's aggression without sparking a war. Moreover, The Washington Post explains that we have used cyber-attacks to covertly manage Russian aggression.

Subpoint B is Saving Civilians.

Since 2014, US-led airstrikes have killed 12,000 civilians.

Fortunately, The Atlantic writes that cyber operations can achieve the same goals as a conventional attack without bloodshed. Instead of bombing our enemies, we can hack them. TechRepublic furthers that "as countries become more dependent on the internet...cyber could be just as effective...as traditional military campaigns."

CNBC writes that America chose to cyber attack Iran instead of launching an airstrike, saving 150 lives. Worse still, Vox explains that an airstrike on Iran could have sparked a bloody war, killing hundreds of thousands of people.

Subpoint C is Terrorism.

Offensive cyber-operations help fight terrorism in two ways.

First, taking down propaganda.

The RAND Corporation explains that ISIS is capitalizing on increased internet access in the Middle East and Africa by spreading its propaganda on social media to millions of young people. For example, the ISN finds that 82 percent of Islamic militants in Bangladesh were radicalized by online propaganda. Thankfully, the National Security Archive finds that the US uses offensive cyber operation to shut down terrorist networks and remove propaganda from the internet. After the US operation, propaganda levels decreased and did not recover.

A failure to address propaganda would be disastrous. RAND furthers that ISIS online propaganda is setting the stage for a massive resurgence. Crucially, NPR finds that if ISIS resurges, it will be even more lethal than before. NBC finds that ISIS-related violence caused 18,000 civilian casualties.

Second, disarming bombs.

Improvised explosive devices, or IEDs, are bombs used by terrorists. Crucially, NBC finds that the majority of these bombs are triggered remotely using online connections.

This has left them vulnerable. Paul Szoldra of the Business Insider finds that US cyber operations have hacked into terrorist devices and prevented bombs from being detonated. Crucially, the Military Times finds that these bombs are the number one cause of US troop deaths, causing over 2,000 casualties. Worse still, the Guardian quantifies that over 53,000 civilians were killed or injured by such explosives in just two years.

Thus, we affirm.

The Brookings Institution finds that North Korea has limited its cyber-attacks to low-level aggression rather than a major attack that could trigger a crisis.

US offensive cyber-operations have created this stability. Following North Korea's hack on Sony, America took down North Korea's access to the internet. The Washington Post explains that North Korea fears that any cyber attack they carry out will be met with a larger, American response. In fact, the Defense Foundation explains that North Korea is limiting its cyber-attacks because it believes that more destructive cyber-operations create more risks than benefits.

Crucially, CNBC explains that a large cyber attack could create a financial crisis that would inevitably spread to developing countries, forcing hundreds of millions of people into poverty.

Thus, we affirm.

As h

Ankit Panda of the Diplomat explains that the United States uses unsophisticated tools to hack North Korea's networks. When attacking North Korea, he writes that America withholds sophisticated methods so that North Korea can't patch up its vulnerabilities.

Frontlines

Subpoint A: Deterring Conflict

F2 Cyber compellence fails because they can patch up vulnerabilities

University of Toronto: The offense can find new vulnerabilities faster than the defense can patch them.[1]
The Diplomat: The US purposely uses unsophisticated attacks to warn our enemies that we have more sophisticated capabilities without letting our enemies patch them up.[2]

F2 Cyber doesn't impose high enough costs

This is good, small costs means that the conflict doesn't escalate
We impose small costs for small acts of aggression

F2 States sustain long-term bombing campaigns without capitulating, so why does cyber work?

Smeets: Cyber is better than kinetic to respond to gray-zone for 4 reasons:[3]

1. Cyber-attacks can be reversed at any time. Conversely, if we bomb them, they can't get those lives/damage back, so they have less incentive to give into the US.
2. Cyber is covert/secret, so it allows the US and our enemies to manage escalation without them worrying about looking weak towards their population. Conversely, if we bomb them, it causes a rally-around-the-flag-effect.
3. Kinetic attacks are incredibly escalatory, so they are more likely to start flat-out wars compared to cyber-attacks
4. Cyber leads to less civilian casualties in general.

F2 We can use sanctions

Business Insider: Sanctions only work 5% of the time because states use the economic harms to rally their people. Cyber is better for two reasons: first, Smeets: covert. Second, puts harm/pressure on the GOVERNMENT (command-and-control systems, data), not on the people.[4]

---

[1] Lindsay (Routledge) BLock and Defense too hard
[2] Panda (Diplomat) NK frontlines
[3] Smeets (Air University 18) compliance; Smeets (Stanford) new option
[4] Badkar (BI) sanctions only work 5% of time; Smeets (Air University 18) compliance

F2 Countries escalating while we have OCOs

Heritage: Aggression is staying in gray zone right now

F2 Examples for 12/16 card

Carnegie Endowment: World War I began with gray zone violence, when Serbian militant group that was loosely tied to the government (hence why it was gray zone aggression) assassinated Archduke Franz Ferdinand[5]

F2 US can tell other countries about red line

Foreign Policy: Red lines have no credibility if we don't enforce it
Limited communication between US and adversaries

F2 Mutually Assured Destruction

Subpoint B: Replacing Conventional

F2 Didn't use in Libya, Syria, etc.

CNBC: Iran strike was a game changer, giving military commanders newfound confidence[6]

F2 Disable other countries, then attack

America isn't interested in getting into more conflicts

Subpoint C: Terrorism

F2 Economy is the root cause of terrorism

Northwestern: No empirical link between economic growth and ISIS membership. Terrorists join because of political and ideological reasons[7]

---

[5] Perkovic (Carnegie Endowment) WWI caused by the gray zone
[6] Gilchrist (CNBC 19) Iran cyberattack marks replacement
[7] Klor (Northwestern) F2 econ link in

First Warrant: Propaganda

F2 Our allies can do it

Defense One: Our allies are so dependent on US cyber capabilities that any offensive operation relies on the US.[8]
That's why National Security Archive: terrorist propaganda uniquely decreased after a US cyber operation[9]

F2 Anonymous can do it

Stanford: Anonymous doesn't have the ability to plant malware in enemy systems; they can only take down their Twitter posts, which is only a mild nuisance to ISIS since they can repost it.[10]

That's why National Security Archive: terrorist propaganda uniquely decreased after a US cyber operation[11]

F2 People who read propaganda are already radicalized

RAND: Lots of ISIS fighters have left, but ISIS uses a "nostalgia-driven" message in their propaganda to get these fighters back[12]
RAND: Sure, some of them are radicalized, but social media uniquely targets the millions of young, impressionable youth in the Middle East and Africa for whom social media is their first interaction with the group[13]

F2 Propaganda isn't the deciding factor for joining ISIS

RAND: ISIS tailors their propaganda to young, impressionable youth in the Middle East and Africa who are very susceptible to propaganda[14]
82% of militants were radicalized by propaganda[15]

---

[8] Tucker (Defense One) NATO depends on US for offensive
[9] (NSA) cyber works against ISIS
[10] (Stanford) anonymous not that good
[11] (NSA) cyber works against ISIS
[12] Clarke (RAND) isis propaganda k2 resurgence
[13] Ward (RAND) broadband in africa; Speckhard (HS Today) A2 ISIS
[14] Ward (RAND) broadband in africa
[15] Doyle (ISN) 82% recruit by social media

F2 ISIS can change servers

American Interest: US cyber capabilities are so advanced that we can shut down new servers as fast as they come up[16]
That's why National Security Archive: terrorist propaganda uniquely decreased after a US cyber operation and DID NOT COME BACK UP[17]

F2 Terrorist groups didn't use social media in the past

RAND: Osama bin Laden said that social media was crucial[18]
NPR: We used cyber against al Qaeda to take 4,000 fighters off the field[19]

F2 Terrorist groups like Boko Haram get recruits without social media

RAND: Boko Haram even uses social media to recruit
They'll recruit significantly more

F2 Propaganda going down because we're killing social media operatives

There are always going to be people in ISIS willing to upload social media
It doesn't take expertise to upload videos to Twitter

F2 Propaganda increasing

Westpoint: Multi-year analysis finds that propaganda has fallen by 94%[20]
Westpoint: Even when it has rebounded TEMPORARILY, it always declines again[21]

F2 Twitter can do it

Speckhard '19 of HS Today: Facebook and Twitter are ineffective at removing non-English posts [22]

Facebook and Twitter just delete the accounts, which can come back; US OCOs take down the entire server in the first place

[16] Van de Velde (AmericanInterest) OCO vital for ISIS communication
[17] (NSA) cyber works against ISIS
[18] Clarke (RAND) isis propaganda k2 resurgence
[19] (NPR) holy SHIIIIIIT terrorism
[20] Milton (Westpoint) frontline and FIRE 94%
[21] Milton (Westpoint) frontline and FIRE 94%
[22] Speckhard (HS Today) A2 ISIS

F2 We already have conventional operations

Van de Velde: Conventional won't work without a broader complementary strategy, including cyber-attacks. ISIS can neutralize any of the gains we can make by recruiting more fighters and portraying our military as foreign actors intervening in their affairs[23]
We agree conventional has been successful, but we have pulled our troops out of Syria. We need cyber-operations to prevent an ISIS resurgence[24]

Second Warrant: Bombs

F2 IEDs casualties by ISIS have increased

Relief Web: As of October 2019, IED attacks have been decreasing[25]
The argument isn't just about ISIS, Cyberscoop: US using cyber operations against terrorist groups around the world[26]

F2 Auto-detonate

That's kind of the point. We want to detonate them when no one is around.

F2 Terrorists use other methods

Relief Web: IEDs are 87% of civilian casualties[27]
IEDs enable other types of attacks, because terrorists surround communities with IEDs so that they can't escape and then terrorize them

[23] Van de Velde (AmericanInterest) OCO vital for ISIS communication
[24] Clarke (RAND) isis propaganda k2 resurgence
[25] (Relief Web) November 2019 IED attacks down
[26] Vavra (Cyberscoop) 2019 cyber attacks against isis
[27] (Relief Web) November 2019 IED attacks down

We affirm.

Our Sole Contention is Stability.

Offensive cyber operations keep us safe in two ways.

Subpoint A is A Better Option.

Subpoint B is A Better Option.

Patrick Lin of the Atlantic writes that cyber operations can achieve the same goals as a conventional attack without bloody warfare. Instead of bombing our enemies and causing civilian deaths, we can simply hack them. More broadly, Max Smeets of Stanford University furthers that offensive cyber capabilities will significantly decrease civilian casualties.

There are many examples. Karen Gilchrist of CNBC writes that, in response to Iranian aggression in 2019, America's chose to cyber attack Iran instead of launching an airstrike, saving 150 lives. Worse still, Alex Ward of Vox explains that an airstrike on Iran could have sparked a bloody war that would kill hundreds of thousands of people.

Another example is the 2010 Stuxnet attack. Herbert Lin of Columbia finds that America used a cyber attack on Iran's nuclear program instead of a preemptive military strike from Israel, preventing a bloody regional war that would have caused thousands to die.

Even if America doesn't use a conventional military response, doing nothing in response to enemy aggression is just as bad. For example, Josh Rogin of the Washington Post explains that if the US doesn't show Iran consequences for its actions, they will be emboldened to further test America's limits. Then, the next Iranian attack could be the one that sparks a conflict. Thankfully, Michael Eisenstadt of the Washington Institute finds that offensive cyber attacks are an effective way to constrain Iran and show clear consequences for their actions.

Another example is North Korea. Matthew Ha of the FDD explains that as North Korea advances its cyber capabilities, Kim Jong Un could deploy cyber attacks against America's critical infrastructure, supply chains, and industries as a way to project its power. *Fortunately, American operations have been able to deter such attacks.*

Following North Korea's hack on Sony, America took down North Korea's access to the internet. Nadiya Kostyuk of the Washington Post explains that North Korea now fears retaliation. They know that any cyber attack they carry out will be met with a larger, American response.

Crucially, Bob Pisani of CNBC explains that a large cyber attack could create a financial crisis that would inevitably spread to developing countries, forcing hundreds of millions of people into poverty.

Overall, the Atlantic Council summarizes that cyber is the perfect middle-ground: offensive cyber operations can show our enemies that their actions have consequences without crossing the line and using military force.

Thus, we affirm.

Weighing

WE HAVE THE BEST LINK INTO CYBER NORMS—OUTWEIGHS TREATY NEGOTIATIONS FOR 2 REASONS:

1. **ADAPTATION**. Silomon ‘18 of CFR: Formal negotiations fail because by the time the treaty ink dries, it will be irrelevant because cyber tech advances so fast. Citizen Lab ‘11: We need mechanisms to continuously create new norms as cyber evolves. This only happens with persistent engagement b/c we constantly adapt
2. **TRUST**. Fischerkeller ‘18: Cyber treaties will always fail because of a lack of trust between the US and our adversaries. Where agreements are reached, they are limited in scope and ineffective at addressing the matters they reach. Scheller: Persistent engagement is much better comparatively because it requires no trust whatsoever; it’s just nations rationally perceiving how other nations act.

Need to constantly update cyber norms rather than one-shot negotiations

https://citizenlab.org/cybernorms2011/cultivating.pdf

Cultivating cyber norms may best be viewed a continuing challenge rather than a discrete task. **Cyber insecurity is likely to be a chronic condition that must be constantly managed rather than a single problem to be solved and put to rest**. **As a consequence, cyber norms must continually evolve, and mechanisms to promulgate new norms must be developed**.

Subpoint A is Adapting to the Enemy.

Currently, David Eaves of Tech President finds that “There is no accepted norm for how to deal with a cyber attack. Consequently, it may be getting harder and harder to predict a state's response to an attack.”

Fortunately, America’s new offensive cyber strategy is the solution. By constantly engaging with our enemies, we can figure out what is acceptable and unacceptable in cyberspace.

Thomas Schelling of Harvard writes that when we are constantly hacking and being hacked, “each side tends to act in a recognizable pattern.” This allows the US and our enemies to adapt to each others’ behavior.

Overall, Jacquelyn Schneider of the Hoover Institution summarizes that “the norms created by [the US] will create a...pressure valve that allows…for competition without escalation.”

The impact is preventing a miscalculation.

Dan Palmer of ZDNet writes that without norms for cyber weapons, conflict can escalate. Since states are unsure of what is acceptable, they can miscalculate, leading to attacks and retaliations that cause unintended damage.

Problematically, Jeremy Straub of PRI furthers that a major cyberattack could cause irreparable economic damage and kill more people over time than a nuclear weapon.

Fortunately, James Miller of Columbia University explains that constant engagement and adaptation can reduce the risk of a cyber conflict escalating in the first place.