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

Our sole contention 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 in cyberspace. [America has developed measures that address cyber conflict with other nations and 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.

As a result, this attempt for peace has caused more failures than successes. Anthony Ferrante of The Hill reports last month: offensive cyber operations across the globe continues to escalate to new and dangerous points every day.

The US's Offensive Cyber Operations are responsible for these failures for two reasons.

The first is by putting countries on the offensive.

Brandon Valeriano of the Cato Institute explains: this year [American actions] risk exacerbating fear in other countries and creating a...spiral of tit-for-tat escalation...even though each actor feels [they are] acting defensively...

This summer's events are a prime example. Two weeks after U.S. Cyber Command hit Iran's...control structure... two cybersecurity companies reported a spike in Iranian cyberattacks against U.S. government.

The second is by contradicting claims.

While the US may advocate for peace in cyberspace now, its offensive actions signal to allies that America will not follow its own rules. Martha Finnemore at the Carnegie Center or Endowment explains in 2017: simply solving the puzzle of what...might address a given cybersecurity problem and announcing this to the world does not create a norm...The U.S. government preaching that commercial cyber espionage is bad did not create [cooperation] against cyber espionage.

Just last year, [The US] refused to sign the [recent Call for Trust and Security in Cyberspace] pact, as [its] strategies ...heavily relied on cyber warfare …

American hypocrisy means that countries are unlikely to trust long term agreements. Jason Healy in the Journal of Cybersecurity confirms: to achieve [peace], adversaries need to be assured that...they would not suffer [a] real or perceived cyber [attack] from the USA... [Offensive cyber] operations could well be perceived as hostile actions and proof the USA is itself ignoring restraint.

The cumulative harm of offensive cyber operations is reducing global development.

It is clear how America is the primary culprit in international failure for cooperation. 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.

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]. [Now, with Trump, China has been violating a US agreement aimed at stopping cyber espionage.]

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.

The United Nations thus concludes: The economic impact and consequences of cyberattacks against critical physical infrastructure, the banking system, [or] national health systems [are] extremely high. [That means millions of people pushed into poverty as countries lose economic growth.]

Because cybersecurity is a global decision, not just an American decision, we are proud to negate.

Protecting this development is crucial. Ann Cheng, executive director of the Global Developmental Lab concludes: digital tools and advances help developing countries break through to the next level of economic gains...the “digitization” of developing economies could yield as much as a $4.1 trillion increase in GDP among the most underserved 3.9 billion consumers.[

This may be part of the logic underlying the 2015 U.S.-China bilateral agreement on cyber espionage for commercial advantage. When powerful or influential actors publicly embrace a norm, this can have spill-over effects and induce others to follow suit (G20 countries, in the espionage example), strengthening the norm that prominent players support.

As Valeriano concludes: [Only] Restraint can also help shape norms in cyberspace and make escalation taboo...Data on cyber actions...suggest ...a policy of restraint...is strategically wise [in creating cooperation].

https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878

Current offensive actions disincentivize cooperation among other countries. Rebecca Slayton at the Belfer Center explains in 2017: An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, repeatedly conducting offensive cyber operations only increases distrust.

Persistent engagement could also fail if the USA, as a technology-dependent democracy, is unable to play the game hard enough to apply negative feedback. In either case, th**e USA may only be able to establish stability through non-cyber responses or forgoing the goal of superiority.** Fighting fire with fire might be viscerally satisfying but can be self-defeating if everyone is covered in gasoline and standing in the same knee-deep dry grass.

Need alternate strategies:

For some international crises, all but the most extreme hawks acknowledge that there may be no military solution. If persistent engagement leads to positive feedback, amplifying rather than dampening the response from adversaries, the USA may have to accept that this is one of those situations. All systems marked by positive feedback "are characterized by a self-impelled 'switch' or discontinuity between two extreme states" [96]. There is no "balance" and the system cannot, in the long-term, be "managed." It may be that the Internet's only stable states are (1) the original, mostly open and resilient model with mild attacks and few predators and (2) a free-for-all where "secure and reliable access to the global network is no longer a global right but a luxury good" and "cyber offense is no longer just better than defense, it is unbeatable" [97]. Cyberspace would no longer be merely the Wild West, but Somalia.

Deterrences fails- not a one size fits all:

Perhaps the imperatives of the new US Cyber Command Vision are the right ones, perhaps not. The risks discussed here may or may not turn out to be major concerns. N**o one—not US Cyber Command, a researcher in academia, or anyone else—can possibly know what comes next. What works with Russia, a declining power trying to regain global importance, may not work with a rising China.** The nation's response to a cyberspace of persistent engagement be an experiment: Try something. Measure what works. Abandon what doesn't. Repeat. This leads to hard tasks for both policymakers and researchers alike

Only diplomacy solves long term:

Persistent engagement will place military and intelligence forces in close contact, actively contending with each other. **If this dynamic isn't to spiral out of control,**

there must be military-to-military hotlines and diplomatic mechanisms to reduce the chances of miscalculation. The current gap between subtle strategies and fiery rhetoric threatens the process of "tacit bargaining" and could lead to the failure of the strategy. Which strategy is Putin and Xi likely to believe, the cautious one advanced by the operational commander, or the more aggressive one being pushed from the White House?

Cold war and other agreements prove cooperation comes first.

Just as important is developing a theory of communication which includes the full range of tacit bargaining, deterrence, signaling, and diplomacy. Persistent engagement has similarities to other examples of where military and intelligence forces of the two blocs during the Cold War were in routine belligerent contact. Joe Nye suggests exploring one parallel, as "**the US and the Soviet Union negotiated an Incidents at Sea Agreement in 1972 to limit naval behavior that might lead to escalation"** [98]. Additional examples include anti-submarine warfare, espionage-counterespionage, freedom-of-navigation operations, and intelligence, surveillance, and "exciter" flights against each other's homelands.

Acting in other country's interests key:

That said, several features could contribute to a given norm's success. Influential and widely respected leadership in promotion of a norm can be important in building shared beliefs and encouraging adherence to behavioral prescriptions. These leaders (or entrepreneurs) need not be the most powerful actors. E**fforts to ban landmines in the 1990s were led by civil society actors and coordinated by Canada over objections from more powerful states. This movement succeeded in part precisely because these actors were not perceived to be pursuing a geopolitical agenda.** Connections constructed between a new norm and widely accepted existing norms can similarly bolster the attractiveness of a new norm's claims and the likelihood of adoption.

NILAYS SOOO GOOD AT DEBATE
https://www.csis.org/analysis/state-practice-and-precedent-cybersecurity-negotiations
But the progress of international negotiations on cybersecurity remains slow, outpaced by the development of offensive techniques and their use, since there is no existential threat that would drive the major powers to make the concessions needed for progress in cybersecurity. Further progress will require painstaking effort that takes into account state practice and an international political dynamic that erodes support for Western norms; as one leading Chinese scholar put it, "We

are moving away from a state in which international norms are led by Western liberalism to a state where international norms are no longer respected." 9

But even if it leads to a reduction, and not an elimination, of such cyber espionage, the agreement supporting the norm should still be considered a success. After all, diplomacy isn't binary. It's a spectrum and if the norm leads to "less but not zero" – it is still a win for the US and other nations that have suffered Chinese commercially-motivated cyber espionage.Moreover, if norms are in fact "collective expectations for the proper behavior of actors" then actors that fail to live up to those expectations will suffer at least reputational costs, especially if heads of state personally and publicly committed to them.

a/2 tf

Thus, cyberspace intrusions by U.S. adversaries that are left unregulated by international law will begin to enjoy a level of international acceptance, no matter how many norms are advocated diplomatically. The effective shaping of cyberspace requires a combination of international norms promulgated on paper in international forums and clear, well-signaled responses to unacceptable activities.

Moreover, if norms are in fact "collective expectations for the proper behavior of actors" then actors that fail to live up to those expectations will suffer at least reputational costs, especially if heads of state personally and publicly committed to them.

Weighing

James Lewis of the Center for Strategic and International Studies, for example, has said, "We have a faith-based approach [to cybersecurity], in that we pray every night nothing bad will happen

Loosening the rules of engagement in pursuit of a more offensive posture, as the Trump administration advocates, violates norms and can lead to disastrous consequences for the entire system.

Historically, we see only *continued* trust creates peace. Healy continues: Persistent engagement...during the Cold War...[allowed] the US and the Soviet Union [to negotiate] an...Agreement in 1972 to prevent [war].

However, countries who push for peace rather than war always seem to fail. Matte Sangiovanni, in the 2017 issue of 'Technology and Philosophy' explains: Presently, the main international agreements governing cyber conducts…[are] severely limited...in terms of both their scope and membership. Calls for negotiating a comprehensive treaty to govern cyber conflict...have so far met with disapproval..

e **United States** and **Russia** have signed a landmark **agreement** to reduce the risk of conflict in **cyberspace** through real-time communication