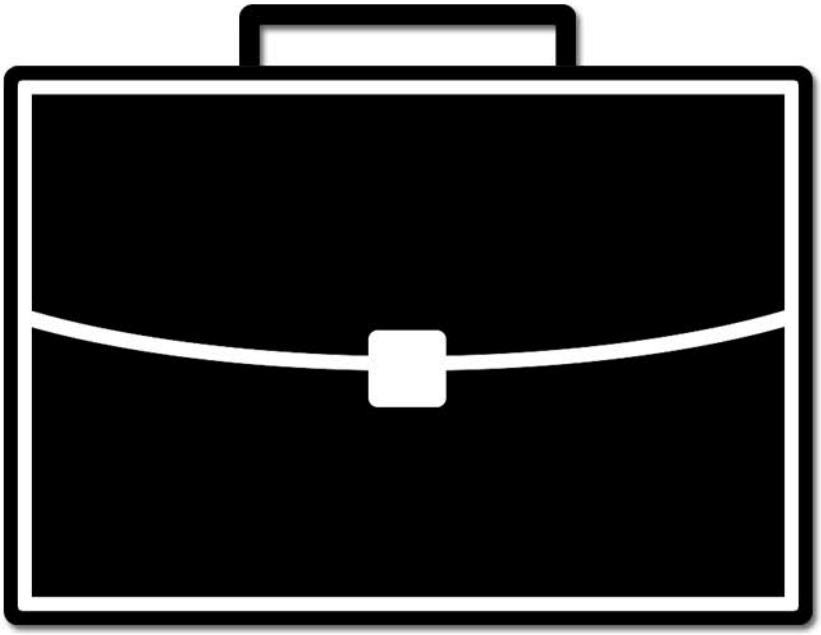
Champion Briefs

Nov/Dec 2019

Public Forum Brief



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

Champion Briefs

Resources for Speech & Debate

About Our Briefs

Our briefs help students expand their knowledge base, improve their analytical skills, and prepare for competition. Each brief includes:

- Varied perspectives from expert writers
- In-depth topic analyses
- Cited evidence sorted by argument
- Peer-reviewed and edited guidance
- Background information & topic framing

Subscription Packages

Lincoln-Douglas

Non-Subscription: $144.94

Subscription: $129.99

Includes briefs for every Lincoln-Douglas debate topic from September through April plus briefs for the novice topic and for NSDA National Tournament

Public Forum

Non-Subscription: $199.92

Subscription: $169.99

Includes briefs for every Public Forum debate topic from September through April plus briefs for the NCFL and NSDA National Tournaments

PF/LD Combo

Non-Subscription: $344.86

Subscription: $269.99

Save an additional 10%
Coupon: CHAMP19

Expires: 9/15/2019

We accept purchase orders and all major credit cards

www.ChampionBriefs.com

The Evidence Standard

Speech and Debate provides a meaningful and educational experience to all who are involved. We, as educators in the community, believe that it is our responsibility to provide resources that uphold the foundation of the Speech and Debate activity. Champion Briefs, its employees, managers, and associates take an oath to uphold the following Evidence Standard:

1. We will never falsify facts, opinions, dissents, or any other information.
2. We will never knowingly distribute information that has been proven to be inaccurate, even if the source of the information is legitimate.
3. We will actively fight the dissemination of false information and will provide the community with clarity if we learn that a third-party has attempted to commit deception.
4. We will never knowingly support or distribute studies, news articles, or other materials that use inaccurate methodologies to reach a conclusion or prove a point.
5. We will provide meaningful clarification to any who question the legitimacy of information that we distribute.
6. We will actively contribute to students' understanding of the world by using evidence from a multitude of perspectives and schools of thought.
7. We will, within our power, assist the community as a whole in its mission to achieve the goals and vision of this activity.

These seven statements, while simple, represent the complex notion of what it means to advance students' understanding of the world around them, as is the purpose of educators.

Letter from the Editor

For our second topic of the year, the National Speech and Debate Association has announced Public Forum debaters will argue the topic, "Resolved: The benefits of the United States federal government's use of offensive cyber operations outweigh the harms." As with September / October, this topic is my preferred choice because it's relatively clear with plenty of offensive arguments to explore on each side. As interstate conflict continues to move online, this topic will be a great chance for you and your team to learn about the United States' role in cyberspace.

This topic was likely chosen by the NSDA because of President Trump's promise to engage in more offensive cyber operations than his predecessors. Generally, the strategy of the Obama administration in cyberspace was one of restraint. President Trump has already used cyberweapons to interfere with Russia's electrical grid, Iran's military, and other powerful institutions. As you begin your research, I implore you to learn the history of the United States' cyber operations, and similarly cyberwarfare around the globe, to ensure you're prepared for this topic.

This resolution is perplexing in that it requires debaters to draw a line between offensive and defensive cyber operations. The Trump Administration argues that deterrence is essential to cyberdefense in 2019, meaning that some offence is actually defensive in impact. As such, there may be discussions about what an offensive cyber operation truly is, so I encourage you to have a definition on hand in case of emergency.

This topic has plenty of interesting arguments to dig into, and cyberwarfare is definitely an interesting subject to learn about, so I'm sure you'll have fun researching and debating throughout November and December. I wish you the best of luck!

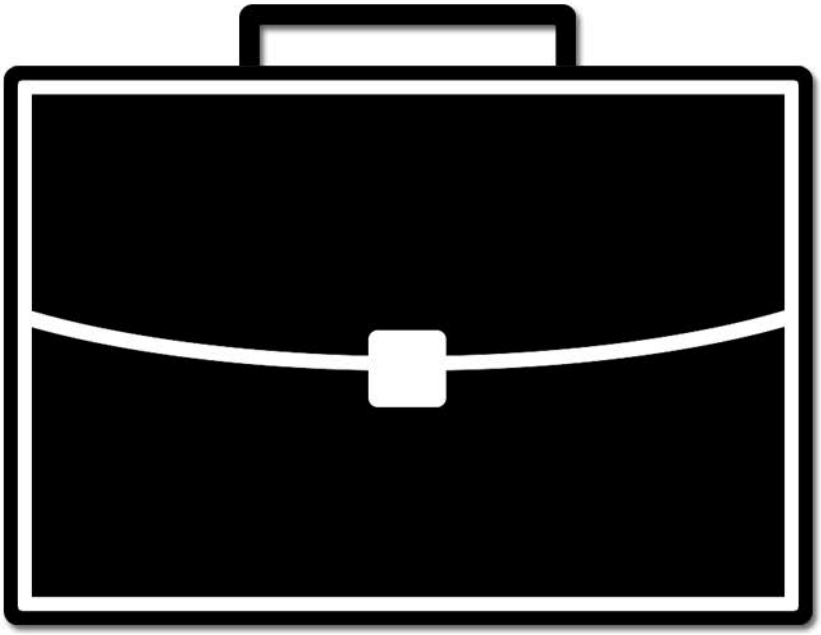
Michael Norton
Editor-in-Chief

Table of Contents

Champion Briefs

Nov/Dec 2019

Public Forum Brief



Topic Analyses

Topic Analysis by Sarah Catherine Cook

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

Introduction

After a seemingly long period of policy resolutions, i.e. a resolution that fiats passing a specific policy or signing onto a treaty, we are presented for these next two months with a value resolution. This means that rounds will no longer center around which "world" is better, as neither side gets to automatically fiat a world with or without offensive cyber operations. Value resolutions are much more straightforward: Is this policy a good or bad thing? That being said, I think there is also room for interpretation; one popular framing mechanism for these types of resolutions revolves around asking the question: Would we be better off without offensive cyber operations? In other words, what is the alternative? Especially with a somewhat simplistic resolution, it will be crucial to look into not only arguments about cyber operations being "good" or "bad", but also arguments about how they are better or worse than the alternative.

Into the Resolution Itself

Let's look into the specific wording of the resolution. "The benefits...outweigh the harms" indicates that there will probably be a bigger emphasis on weighing this month, or at least that teams should be very ready for debates to turn into weighing debates, especially with three-minute summaries. It may be strategic to emphasize principle arguments early in the

round, i.e. that deterrence through MAD does not really exist or that offensive attacks are always a bad thing, etc. While many arguments on this topic will be specific to offensive cyber, the resolution also has the potential to address a broader issue: whether the U.S. should respond or act offensively with regards to the military. For this reason, looking into more principle arguments of how certain countries are likely to respond based on their political interests and looking at the future of U.S. military operations might be valuable to frame the debate and attack your opponents' cases with more fundamental arguments.

The word "use" seems very straightforward, but could indicate very different things. Some teams may interpret "use" to mean use or attack. This would be strategic for the negative team because if they were to narrow the scope of the debate to whether specific attacks were positive or negative, they would avoid debates about things like deterrence, which could be a strong Aff argument. Some teams may interpret "use" more broadly to mean that cyber-attacks will become a core part of U.S. military strategy, which means that the debate will center around their role as an option for attacking or retaliating, rather than only discussing the efficacy and strategic value, etc. of attacks themselves. Technically, deterrence could fall under this more broad interpretation, as we would say we "use" our large military to intimidate other countries or change their decision-making in favor of not attacking the U.S. As with the interpretation of the BRI topic last month, there will probably be a more common interpretation of the resolution that is used or assumed once competition begins.

I would note that some teams may narrow or broaden the definition of offensive cyber operations. One of the questions that may be overlooked by some is: What exactly does offensive entail? Is it offensive if the U.S. responds to a cyber operation with a cyber operation?

Most interpretations will say yes, but ultimately it is up to each team to decide what interpretation of the resolution they see most accurate. Teams should be prepared to handle teams who may have wacky definitions of offensive cyber operations because there are always teams who will choose to interpret the resolution in a way that better benefits them.

The final question I would ask when interpreting this resolution in terms of building a case is whether or not to include future cyber operations as well. There is a fixed body of literature about current and past cyber operations, meaning that it is feasible to think about the topic in terms of those concrete examples of cyber-attacks being used. On the other hand, there are some interesting arguments to be made about whether the future of cyber operations is a positive or negative thing. Who will the cyber operations target in the next few years or decades? Will cyber operations turn from harmful to beneficial or beneficial to harmful in the future? It's definitely up for debate. I think it could be interesting in theory to focus a case around future cyber-attacks because it would allow a team to somewhat bypass or immediately disregard some of the arguments the other team is making about past cyber attacks or even current ones. The timeframe of arguments also matters in the sense of whether or not to evaluate past cyber attacks as part of the topic: Do past cyberattacks matter or is the resolution only discussing the state of cyber attacks right now? There are lots of interesting paths to go down with this topic.

Alright, folks, we've made it: What are offensive cyber operations and why do they matter?

What are offensive cyber operations and why do they matter?

While offensive cyber operations have only been utilized for a little over a decade, they have had major impacts. While Obama was hesitant to use offensive cyber operations often,[1] current and former officials confirm that the U.S. conducted an operation called Olympic Games which essentially destroyed around 1000 Iranian nuclear centrifuges.[2] The United States has conducted cyber attacks on China,[3] ISIL,[4] most recently Russia,[5] as well as other nations either publically or more secretly. Offensive cyber operations can refer to multiple different types of actual attacks. The two main broad categories are "counterforce" and "counter-value". Counterforce operations are operations that strike at the opponent's military forces or infrastructure, e.g. the strikes that are currently happening on Russian, and the Olympic Games operations. Countervalue strikes, on the other hand, target the sources of an opponent's national strength; the strikes conducted on ISIL could be an example, as they target ISIL's online strategies - which is key to their growth as a group.[6][7] These strikes seek to disrupt different strategies, whether they be military or geopolitical, and provide another option for leaders when responding to different scenarios. This means that that cyber operations in this topic would ideally be evaluated in a few different ways.

[1] Dilanian 2018.
[2] Nakashima 2012.
[3] Gertz 2019.
[4] Temple-Raston 2019.
[5] Sander and Perlroth 2019.
[6] Smeets 2018.
[7] Temple-Raston 2019.

The first is whether they are effective or not, i.e. whether the technology is effective and whether the people operating it are skilled at doing so. I don't think this will be a relatively important point of clash in most debates - the consensus of literature points pretty clearly in favor of offensive cyber technology and coding being pretty top-notch. In general, this issue or response brought up most likely by a Neg team would flow Aff, as even if the technology were not in great shape right now, we are constantly trying to improve our footing in the cyberspace world especially because other countries are also moving in the trajectory of cyber operations rather than direct conflict - this means that in the long term cyber operations are probably only going to get better in terms of minimizing errors. Whether or not cyber operations carry huge risks of error in the long term as well as negative externalities coming off of the attacks themselves are unlikely to be a huge point of clash on this topic, though with a deeper investigation it could produce some interesting and unique arguments if the literature exists.

The other consideration here is whether cyber attacks lower the cost to conflict. If the perception exists that cyber-attacks are somewhat less dangerous than other methods, even if each cyber attack is better than each alternative, the number of cyberattacks that would happen may be larger than the number of military interventions or economic responses that take place because there is a larger associated cost with each of those options. Even more so, when countries have cyber attacks as an option, are they more or less likely to engage in conflict as a whole? When the cost of conflict is higher, countries are more likely to resolve conflicts via diplomatic means rather than engaging in a more aggressive strategy. In that case, the existence of cyber attacks may encourage countries to instead approach situations via these

attacks. Even more so, cyberattacks could lead to other types of military conflicts, which we will discuss later.

The next consideration is about whether the operations themselves are on net beneficial or harmful. This will also center around the fundamental question that we have debated around in many other topics: Is U.S. intervention on net beneficial or harmful? On face, many of the cyber operations may seem justifiable by the authors writing about the operations. But is this the case? For example, one could argue that it is a bad thing that the U.S. destroyed around 1000 nuclear centrifuges because it took out Iran's ability to produce nuclear energy, which could be good for the environment or Iran's economy. The bottom line is that it is up for debate whether these operations, often targeting crucial infrastructure are necessary. Especially operations that attack power grids or key infrastructure can be very costly and deadly for the countries being attacked. This also brings the interpretation of the resolution: Do we only want to look at the impacts on the U.S.? The simple answer is no. This resolution is especially interesting because it will force debaters to evaluate these policies in terms of who they benefit and who they hurt. The difficulty here is that every possible result will probably hurt someone - it then comes down to the debaters to show which side is the least bad option per se. Going back to this fundamental question for the round, i.e. whether operations are good or not, the other side could easily argue that destroying nuclear centrifuges is a positive thing or that hacking into the Chinese company Huawei's infrastructure, or ISIL servers is a beneficial mission because it decreases the power of that group or gives the U.S. more insight. This view also will necessitate proving the U.S. strategy is a benevolent or positive one - one's immediate reaction to hacking would be negative if it were China or Russia hacking the U.S. I think this topic will be an

interesting one especially because teams will have the opportunity to not only look into the theories of intervention, but also look into specific types of offensive cyber operations and debate about whether they have a positive or negative affect.

The final factor will probably be one of the major focuses of this topic: the larger strategic implications of these operations. This is how the topic ties into the larger U.S. strategy as a whole. Let's guide our discussion around questions that this begs. First, are cyber operations better than the alternatives? What's key here is to define the alternatives, which is very much up for debate. The alternatives to cyber operations, as well as the use of cyber operations in general, is very much dependent on who is in office. During the Obama presidency, the alternatives to cyber operations were pretty much nothing, as Obama very infrequently used cyber operations or any response to hacking attempts to other countries. Trump, however, is more likely to wage war whether it be militarily, with cyber operations, or via economic means, as we've seen throughout the past few years. One of the potential arguments for an Aff team is that cyber operations provide an option that is somewhat less bad than other actions that the President might take in response to other countries' actions or just as an attack on some threat. On one side, cyber operations are much more likely to be effective, as many of the military operations the U.S. has undertaken in the past few decades, i.e. Iraq, Afghanistan, Syria, etc. have been drawn out and have not produced any conclusive positive endings. Cyber operations provide an option for fighting terror in a way that does less direct harm to the U.S. and less direct instability in the region. That being said, cyber operations also tend to target key infrastructures like power-grids or nuclear energy centrifuges. Especially with the power grid example, as well as other infrastructure-related targets, this could affect an

entire region or entire country rather than just certain areas; imagine hospitals going out of power, etc. Some may argue that U.S. military interventions are more effective in achieving desired goals. The other consideration is economic responses rather than cyber operations; Which is more likely to be effective at achieving the desired goals and produce the least amount of negative effects? An issue that is largely up for debate, as well as other alternatives to cyber operations. One thing to keep in mind with these arguments is that teams arguing for or against specific alternatives much have sufficient evidence to prove that a certain alternative is most likely in a world without the option of cyber operations.

The next question is: How do countries respond to U.S. offensive cyber operations? Some Aff teams may argue that the use of U.S. cyber operations will deter other countries from messing with the U.S. or hacking U.S. infrastructure or intel. This argument is pretty common on military-based topics and if warranted well and backed up with good studies, tends to be pretty successful. One of the counters to this argument is that when deterrence exists, countries will just have an incentive to improve their capabilities to the point where they then have the upper hand, i.e. an arms race. In this case, countries would be stuck in a sort of standoff - constantly trying to outdo each other. If attacks on the U.S. have not been that damaging, is it really necessary to greatly increase our capabilities if it sparks other countries to do the same? In addition, this increased capacity could increase the risks of miscalculation. If another country believes that the U.S. is going to strike them via cyber, they have an incentive to attempt to strike first - both to prevent an attack from the U.S. and damage the U.S. strategically. Even more so, countries who have been victims of U.S. cyberattacks might have an incentive to strike back. This begs the question: Do cyberattacks solve problems or exacerbate them? This topic

calls into question the larger geopolitical and military strategies of each country involved, i.e. how they act in times of conflict, how they will respond to an attack from a country who is more or less powerful, etc. Much of the core debate on this topic will center around whether cyber attacks will deter or stop future attacks or the capability to attack or whether it will increase tensions and exacerbate conflict.

Final Note about Cyber Operations

While most of my discussion on cyber operations is about their military value, there are other ways to view this topic. I think there are definitely interesting arguments to be made about destroying opportunities for nuclear power or hacking that relates to political events, i.e. deterrence could be applied to stopping Russia from interfering in U.S. elections again, or U.S. intrusion into Huawei could link into stopping some of the arguments related to Huawei and authoritarianism seen on the last topic. There are lots of interesting impacts and arguments to be made outside of the military realm, but they will need more time and more weighing. I think this topic could be really interesting - enjoy yourself when it comes to finding arguments!

Thoughts about November

November is a bit of a different beat from Septober. The prime difference is that most people will be somewhat unprepared for the topic when it starts, especially because many Septober tournaments directly back up to November ones. Teams will be most successful this month if they continue to update and improve strategies as the month progresses - many entirely new arguments will surface between tournaments and this month will keep you guessing as to what other teams will be running, depending on how many tournaments you will be attending. It's also strategic to have a fundamental thesis for each argument or case that you

make - what is the underlying logic of your case? Having something like this to rely on for responses, weighing, clarity, etc. will help you in rounds where you are blindsided with an argument you have not heard of. This is also the month where a lot of novices will no longer be as inexperienced as before - if this applies to you, use this month to really fine-tune your casing and rebuttal strategies! This topic should have a lot of clash on it, which makes it necessary for teams to dive into the warranting behind each argument - make sure that in addition to finding solid evidence, you are also looking into the reasons why things are true. This will be key especially on this topic.

Good luck and best of luck!

Works Cited

Dilanian, Ken. 2018. "Under Trump, U.S. ramps up cyber offense against other countries." *NBC News.* Available from: <https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281>.

Gertz, Bill. 2019. "U.S. hits back against Chinese cyberattacks." *The Washington Times.* Available from: <https://www.washingtontimes.com/news/2019/mar/6/us-counters-china-cyberattacks/>.

Nakashima, Ellen. 2012. "Stuxnet was work of U.S. and Israeli experts, officials say." *Washington Post.* Available from: <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>.

Sanger, David E. and Nicole Perlroth. 2019. "U.S. Escalates Online Attacks on Russia's Power Grid." *The New York Times.* Available from: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.

Smeets, Max. 2018. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly.* Available from: <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf>.

Temple-Raston, Dina. 2019. "How the U.S. Hacked ISIS." NPR. Available from: <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>.

About Sarah Catherine Cook

Sara Catherine Cook grew up in Birmingham, Alabama and competed for The Altamont School for 3 years in Public Forum. She was one of the first teams from her school to qualify for the Tournament of Champions and NSDA Nationals, being the only team from her state to qualify to the TOC in the 2018-2019 season. She reached late out rounds at tournaments like Yale, New York City Invitational (Big Bronx), and Peach State Classic, championed Holy Cross, and won state her junior year. Founding Beyond Resolved, an organization dedicated to combating issues of gender inequality within the debate community, is her proudest debate accomplishment. She now attends Dartmouth College in Hanover, New Hampshire, planning to study Math and Economics.

Topic Analysis by Tucker Wilke

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

Introduction

For the second time in Public Forum history, the same topic will be debated in November and December. For debaters looking to be selective in the topics they prepare, the double-month topic is an excellent investment. Debaters can frontload a lot of the research and preparation and then have nearly two full months of payoff, which include some of the most competitive regular-season tournaments of the year. That being said, debaters should also resist the temptation to simply write their cases for their first November tournament and just ride it out from there. Instead, they must be willing to see their strategies evolve over the course of the topic, as new arguments and research are discovered. Two-month topics often reward those teams always looking for a creative spin on the stock arguments. Luckily, the November-December topic provides plenty of room for interesting dynamics to keep debaters engaged, as it is "Resolved: The benefits of the United States federal government's use of offensive cyber operations outweigh the harms,". The first thing to notice here is that unlike the vast majority of Public Forum topics, which are *prescriptive,* which say that some actor or government *should* do something, this is one of the rare *descriptive* topics, that asks us to evaluate the benefits and harms of an already existing policy. This means that arguments on this topic will have fewer long, drawn-out link chains about the hypothetical actions and

reactions of the implementation of a policy. Instead, teams will be armed with already clear examples of benefits and harms of Cyberattacks by the United States. This means that weighing will likely be even more important than it is normally since both sides will have arguments that will be true at the end of the round. With that in mind, let's take a look at the tournaments, arguments, and strategies that will come to dominate the next two months.

Tournament Considerations

The November-December slate of tournaments is a good one, with a couple of big national tournaments and competitive regional tournaments on the other weekends. The biggest tournament on this topic is undoubtedly Glenbrooks which, along with Bronx and Harvard, is generally considered one of the three most competitive tournaments of the regular season. Glenbrooks attracts top competition from all around the country, and by virtue of its location right outside Chicago, provides a more regionally balanced pool than the more northeaster Harvard and Bronx. As far as national circuit tournaments go, Glenbrooks tends to have a large amount of pretty flow judging. While debaters should be ready for their fair share of parent judges, Glenbrooks tends to have an above-average number of panels chock full of experienced flow judges. The difficulty, however, is that due to the geographic diversity of the tournament, the flow judges at Glenbrooks will often have very different conceptions of how debates should go. As such, debaters should be ready for panels with judges who have differing views on rules such as frontlining in rebuttal and terminal defense in summary. It is therefore paramount for debaters to read paradigms and ask questions before the round and be extra ready to adapt to their judge's preferences. The other big tournament on this topic at which I have experience is

Princeton. Princeton tends to be dominated by more traditional and parent judges, in both early prelims and deep out rounds. Debaters should, therefore, prioritize keeping their cases on the shorter side, speak as clearly as possible, and eliminate as much "jargon" as possible from their speeches. Additionally, debaters should also be ready to tweak their in round framing and strategy based on their judges. Holistically, judges with less experience in debate tend to assume that topics about some sort of United States policy should revolve around the United States' interest, rather than one about developing countries. Teams that have strategies that rely upon the benefits or harms of cyberattacks to other countries should be prepared to do lots of work justifying why the interests of those countries are most important in the context of the round.

Background and Strategy

At first, this topic may seem very straightforward, and relatively simple to prepare. Once teams begin to do some research, however, they will quickly see that there are a couple of quirks that make this topic tricky.

The first issue is that, unsurprisingly, the United States keeps the vast majority of information about its offensive cyber operations completely classified, which means that in a topic that one would imagine would mostly just be a game of comparing beneficial and harmful offensive cyberattacks, examples of these operations may be in short supply. This has a few implications for debaters preparing the topic. First, it means that debaters should know the details of the few known examples of offensive cyber attacks by the United States inside and out, since the potential effects of those examples may come to dominate rounds. Second, debaters need to make sure that the examples that they find are credible, which may prove

more difficult than normal on this topic. Many articles written about US cyber-attacks, such as this excellent *New Yorker* article called “How Cyber Weapons Are Changing the Landscape of Modern Warfare” (an article that every debater preparing this topic should look at) will contain a line such as this: “According to an officer-involved, who asked to remain anonymous…”[8]. In other words, much of the information on cyber attacks come from anonymous sourcing. This is not to say that those sources are inherently untrustworthy or unusable in a debate round, but debaters should certainly know and be ready to defend, exactly where their information comes from.

The second wrinkle in this topic is that "offensive cyber operations" is a shockingly broad category of tactics, and one that many experts think is too broad to be particularly helpful. Zeger of Brookings explains that saying "cyber operations" would be equivalent to inventing a category of "vehicle-borne threats" that is supposed to encompass everything from terrorist attacks using truck bombs to carjacking. It is, in many ways, too broad to be that helpful.[9] Luckily, Zeger places offensive cyber operations into three general categories. “One is information, so espionage, compromising the integrity, availability, confidentiality of information. Two is beliefs, so we see with the Russian election interference and attack to hack our minds. And the third is physical effects or things that go boom.". Again, these three tactics are in many ways wildly different from each other, but what does this mean in the context of the topic at hand? A few things: first, since so many US operations can be termed "offensive

[8] https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare
[9] https://www.brookings.edu/wp-content/uploads/2019/04/BCP_Transcrtipt_Offensive-cyber-operations-in-US-national-security.pdf

cyber attacks", there are bound to be a number of ones that have become declassified or that the public has found out about, meaning debaters should be able to find evidence if they look hard enough. Second, it means that a topic that upon first glance may have seemed pretty narrow is very broad. This will give debaters lots of options when crafting arguments for each side of the topic and means that they should know which type of cyber operation their case is talking about. On the flip side, this also means that t debaters will have to be ready for many different types of arguments about many different types of operations. They should have a very good understanding of the benefits and harms of cyber operations in each of the above categories, even if their arguments only focus on one. Finally, it means that to reiterate a point above, weighing will be crucial for this topic, since it is the most efficient way to compare two very different arguments in a debate round.

Now having looked at the question of *what* "offensive cyber operations" are, and *where* our knowledge about them comes from, we can now turn our attention to the third aspect of the topic worth examing: *for who* do the "benefits...outweigh the harms". Debaters will need to be ready to deal with a couple of competing frameworks about whose interests should be prioritized in the round. The two standard frameworks tend to fall into two categories. First is "United States interests", which is a framework that generally asserts that since the policy in question, offensive cyber operations, is a *United States* policy, the benefits and harms of the policy need to be looked at through the lens of the interests of the United States and its citizens, which includes our general strategic interests. In other words, US cyber operations exist for the benefit of the United States, so they should be judged based on their benefits and harms to the United States. The second framework is generally "global interests", which is the

idea that since the resolution simply asks to compare the benefits and harms, the debate should look at whether US cyber operations are beneficial or harmful for the world-at-large, even if they help/harm US strategic interests. The United States centered framework will most likely be used primarily by pro teams, and the global centered framework will probably be favored by many con teams. It is worth noting that, holistically, US-centered frameworks do tend to play better with more traditional or lay judges, and global interests based frameworks tend to work well with judges with experience in debate. That trend is certainly not universal, and everything in a debate is up for debate, but it is worth keeping in mind when thinking about what framework to run at a given tournament or in a given round.

Pro Arguments

Pro teams have at their disposal many of the standard arguments in favor of any military operation, just applied in a slightly different way to cyber operations. As such, I would encourage teams preparing their affirmative cases to at least give strong consideration to the intuitive arguments, rather than trying to be sneaky. After all, people have been advocating for cyber spending for a long time, so it's worth looking into why that is. One such argument is that offensive cyber operations have been crucial in decreasing and eliminating threats around the globe. When researching this, I would consider teams to look into "Stuxnet", the infamous mysterious cyber operation about a decade ago. Stuxnet was a computer virus that infected Iranian nuclear centrifuge systems, and while nobody has claimed responsibility for the attack, it is now "widely accepted" among experts to have been developed by the United States and

Israel to attack the Iranian nuclear program[10]. Importantly, the operations were pretty successful, as "Although Iran has not released specific details regarding the effects of the attack, it is currently estimated that the Stuxnet worm destroyed 984 uranium enrichment centrifuges. By current estimations, this constituted a 30% decrease in enrichment efficiency"[11]. Those direct effects are nothing to gloss over, and pro teams should not be afraid to capitalize on examples such as these that show tangible benefits of offensive cyber operations.

In addition to being good in and of themselves, examples such as Stuxnet open the door for another path of pro argumentation: deterrence. After all, while we do not know the extent of US cyber operations, they are not capable of targeting every single threat posed by another country. What these operations can do, however, is serve as a threat to those countries about what the consequences of their continued actions can be. One can again look to the example of Stuxnet. In addition to directly hampering Iranian nuclear development, teams can also argue that it served as a deterrent to further nuclear enrichment of other countries. Reactors are super cost and labor-intensive, and from an economic perspective pouring tons of resources into projects that can be remotely derailed by a foreign power is something perspective nuclear developers must consider. Even worse, Stuxnet also opens the door for potentially even more destructive operations. If reactors can be sped up to the point of breaking down, it's certainly feasible that cyberattacks could also cause some reactor meltdowns that would threaten lives.

[10] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html
[11] http://large.stanford.edu/courses/2015/ph241/holloway1/

That does not seem to have happened, but the threat it poses can certainly deter countries from engaging in nuclear development.

Another possible route of argumentation for pro teams to consider is the idea that cyberattacks replace other kinds of military action. To make this argument, there are two questions that teams must answer: first, the obvious, do more cyber attacks mean less use of other forms of military action? Second, are cyber attacks better (or less harmful) than other forms of military action? For pro teams, that answer to both of these questions must emphatically be yes, cyber attacks trade-off with other kinds of military action, and that is a good thing. There are numerous different avenues of argumentation under this assertion, but most of them will rely on the idea that cyber-operations are far more targeted than other forms of military operations, so there is a lot less collateral damage and fewer (if any) human casualties. The benefit of this kind of argument is that it allows pro teams to get out of having to defend cyber-attacks in a vacuum, where con teams can easily point to some problems they cause and instead defend them comparatively. Even if they are not perfect, they are better than the alternative. After all, in the early 2000s, the US went to war because they thought a foe was developing nuclear weapons; in 2010, they used a cyberattack to disrupt the nuclear systems of another potential foe. If pro teams can manage to prove a trade-off between those kinds of actions, then they will certainly be in good shape to win.

Con Arguments

One place for many teams looking to plan their con cases to begin is with the exact inverses of many of the arguments outlined for pro. Con teams can answer the questions above

in the opposite way, arguing that cyber-attacks do not trade-off with other forms of military operations. Instead, they cause continued escalation between countries, which can result in far more harmful effects. For example, con teams can certainly argue that the US would never have invaded Iran with or without Stuxnet, or, to take a non-United States example, it is not as though Russia was going to invade the United States but instead decided to do election interference. Rather, that was simply the latest step in a years-long cyberwar between Russia and the United States, that has included the United States making numerous probes into Russia's power grid, that has continued to escalate, and is now poised to escalate even further during the Trump administration.[12] Importantly, these cyber attacks are not just some fancy computer games played between two powers. These operations have been directly probing into power grids, which people rely on for everything from preserving food to keeping houses arm to keeping life support machines in hospitals running. If both sides continue their offensive cyber operations, con teams should convincingly be able to argue that it is only a matter of time until people start to die. Again, the crucial thing for con teams to point out is that this bubbling cyberwar is not a replacement for conventional war, it is just an additional, potentially more dangerous, avenue for conflict.

Con teams can also attempt to turn some of the traditional, benevolent seeming cyber operations on their head by pointing out how dangerous they are. For example, any cyber weapon designed to target nuclear reactor carries enormous risks to safety should something within the reactor malfunction and a nuclear meltdown occur. After all, the two seemingly most

[12] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

common targets for US cyber-attacks, power grids, and reactors, are both exceedingly dangerous. This kind of thinking can help con teams to flip the other half of the pro's argument, as they can not only argue that cyberattacks do not replace other forms of military action but even if they did, they are in many ways more dangerous than other types of conventional espionage and action. If con teams can prove that that is the case, they will be in an excellent position to win rounds. Teams may find, however, that they will run into the same problem as teams often do when running arguments about the risk of nuclear weapons: despite the fact that tons of experts agree cyber operations are super dangerous, the fact that there has not yet been an all-out cyber war or cyber catastrophe that has killed people will make arguments about the risk of those events harder to sell to judges.

Another more unique route of negative argumentation can come from the second category of offensive cyber-operations discussed above: the “beliefs” category, which are cyber-operations aimed at manipulating the citizens of a country such as Russia did with the United States in the 2016 election. The United States, however, is no stranger in engaging in these actions ourselves, as a C.I.A. official said “f you ask an intelligence officer, did the Russians break the rules or do something bizarre, the answer is no, not at all...The United States “absolutely” has carried out such election influence operations historically” [13]. While this may not be the first definition of offensive cyber operations that judges intuitively think of, if con teams can effectively frame the discussion around foreign election interference, and can convincingly show that the US engages in this operations than there are numerous potential

[13] https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html

impacts. First, on a more moralistic level, con teams can argue that these operations are direct violations of national sovereignty and the autonomy of other countries by making the United States a puppet master of the world. This kind of impact, while important for real-life discussions, is probably pretty difficult to weigh in rounds. Thus, debaters can instead take a more practical line of argumentation, about how US operations normalize that behavior overall. In other words, the fact that the United States engages in foreign election interference cyber-operations makes it impossible to condemn Russia for doing the same thing in any meaningful way, and instead makes this behavior a global norm. Teams can then read impacts about the mass destabilization of election interference, and destabilization can have direct impacts on the social and economic well being of a country, giving teams a route to very concrete impacts for what may initially seem like a very abstract argument. Overall, the election-hacking argument is complex and will certainly require lots of research, but there is a large pay-off for teams up to the challenge.

Conclusion

Overall, despite the fact that this topic seems relatively simple, it should provide an excellent challenge for debaters on both sides. As a final point, it is worth noting that, as mentioned above, there is a lot that the general public does not know about the examples of offensive cyber operations, let alone their effects. Finding concrete historical evidence or good academic studies on this topic maybe even more difficult. While debaters should prioritize finding as good evidence they can, it is also paramount that debaters have their logical analysis and warrants as clear and fleshed out as possible in every speech they give, since the soundness of their reasoning may be the deciding factor in many of their rounds. Good luck!

About Tucker Wilke

Tucker is from Westchester New York, where he attended the Hackley School. He is now attending Brown University, where he hopes to study History and Economics. Over the course of his career, Tucker amassed 8 bids to the Tournament of Champions. In addition, he reached the Quarterfinals at Bronx, Glenbrooks, UK, Ridge and Princeton, Semifinals at Penn and Columbia, and championed the Scarsdale Invitational. He was ranked as high as 7th in the country in his senior year.

Topic Analysis by Jakob Urda

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

Introduction

Cyberwarfare studs the firmament of America's political, economic, and social horizons. From Russian election interference to the Iranian nuclear program, to WannaCry and Fancybear, cyber warfare is both highly relevant and ill-understood. Like many incipient technologies, cyber warfare requires extensive debate as to the direction which America should move towards in pursuing public policy. Doctrines are still being developed and resources are still being allocated. In cyber warfare, the only certainty is that the technology will be central to our national strategy; the question is how.

Some believe in a robust deployment of offensive cyber operations, and those who believe in a more risk-averse stance. These two schools would dramatically change the patterns of investment and study which America applies to cyber technologies for the foreseeable future. Much as America's decision to offset Soviet armor with nuclear weapons during the Cold War resulted in decades of cascaded nuclear strategy, the choices that we make in regards to cyber strategy will bear implications for all manner of downstream policies. America needs to consider the full spectrum of political, social, and economic consequences of a cyber doctrine.

Tournament Considerations

November-December topics will be debated at tournaments across the country. The length of the topic makes it advisable for teams to try and get in as many rounds as possible early on, in order to gain an advantage later in the topic. At the same time, teams should be mindful that these tournaments can be incredibly competitive, and that the extra length allocated to this topic will bring out fiercer competition. The length of the topic means that few teams can afford to ignore these pivotal months.

Glenbrooks is undoubtedly the most intense tournament of the topic and is considered one of the most difficult tournaments of the year. Its prestige put it on par with national invitationals such as Harvard and Yale. Glenbrooks has a national draw and works hard to bring in experienced judging. Therefore, one should expect the rounds to be intense and high quality. Teams should focus on technical argumentation, practice speed, and take notes on lengthy RFDs. The nation draw of the tournament will also expose debaters to different viewpoints that they can adopt for later tournaments.

One should not make the mistake of assuming that strategies that work at Glenbrooks will work at other tournaments. It is very possible that the judges at Glenbrooks—being debate coaches and veterans—are better able to separate the discussion that goes on in-round from their preexisting ideas about healthcare. For many other tournaments, this may not be the case, and more work will have to be done to make certain ideas palatable for laypeople.

Counterintuitive arguments (about high prices being good, for instance) might work well at Glenbrooks, but will certainly be a harder sell at other tournaments throughout the topic.

One of those other tournaments is the GMU invitational. GMU has historically been massive, with hundreds of entries. The judging pool could also not be more dissimilar to that of Glenbrooks. GMU has an east-coast draw and has a substantially smaller portion of technical judges in the judge pool. The tournament is also huge for speech, and the judges sometimes circulate between events because schools bring odd numbers of teams, and need to fill their judging requirements. This means that between non-traditional and lay judges, debaters need to focus on the art of persuasion. I would recommend cases no longer than 650 words, and arguments that are couched in intuitive logic. Winning the flow is less important than communicating with your judge, and what flies in Glenbooks may not work out at GMU.

Strategy Considerations

Like many topics, some of the most important factors to consider for November happen before any clash in argumentation. The resolution asks us about the "United States federal government's use" of cyber capabilities. This requires that debaters know, in a descriptive sense, how the US government uses cyber capabilities, and what the patters of use will be in the future. This means that even if the debaters in the room have ideas about what the use of cyberweapons *ought* to be, the resolutions asks students to evaluate the world as it is, and as it is likely to continue being. The idea that debaters need to worry about the most likely manifestation of a topic is called inherency.

What are the most likely implementations of cyber weapons? To understand this we need to look to the past to understand how and when the US government has deployed offensive cyber operations in similar cases. This allows us to make arguments about how the pattern of deployment for cyber operations may happen in the future and what the likely paths of investment are. The past also gives debaters an understanding of what the alternatives to cyber weapons are. Inherency cuts both ways: teams must also be able to say what the most likely alternative to the development of cyber weapons is, rather than cherry-pick alternative scenarios that are unlikely to ever materialize.

Three types of cyber weapons could reasonably be considered ‘offensive' in nature. These are cyber weapons made for surveillance, theft, and destruction. The US government uses all of these tools in different scenarios, and banning them would have different implications depending on which specific systems were blocked from development.

America has some of the most advanced surveillance capabilities of any nation on earth. These tools are arguably the least likely to be banned under a negative scenario, and so teams that focus on surveillance technologies should make sure to warrant their inclusion in the resolution. By some logic, cyber-surveillance could even increase under a world were ‘offensive' cyber weapons do not include surveillance, because funding might be rerouted towards espionage. Nevertheless, espionage often requires intrusion into enemy systems, laying the groundwork for future hacking operations, and creating actionable intelligence which can be exploited in subsequent noncyber operations. The most compelling reason to include surveillance in offensive operations is that the process of surveilling is an *offensive-cyber*

operation; The process often requires exploitation of enemy system vulnerabilities which ought to constitute offense. If the United States has to hack into the computers of an enemy intelligence network to conduct espionage, that could well be considered an offensive operation.

Theft involves the leveraging of cyber capabilities to steal sensitive information from an opponent's systems. This is typically more than movement, intentions, and communication, which would be included under surveillance. Theft often involves the stealing of secret research, such as intellectual property. In one well-known case, Chinese hackers used cyber weapons to steal chip designs from Taiwanese companies. These tools are significantly easier to classify as offensive because the physical world analog of theft is a violent action.

The final type of cyber operation is destruction. This involves the manipulation of an enemy's cyber systems to actively impede their progress towards a strategic objective. Destructive cyber operations can target either physical or virtual infrastructure. One example might be the deletion of important information or sabotage of an enemy's cyber tools. Perhaps the best example of destructive cyber operations is the American collaboration with Israel over the Stuxnet virus. Stuxnet targeted Iranian nuclear weapons facilities. It infected the computers which regulated Iranian Uranium centrifuges and forced them to spin out of control until they failed. The Stuxnet virus set Iran years backward in its nuclear program.

Being able to identify which capabilities and effects result from specific types of cyber operations is important for being able to address what exactly falls into the camp of offensive

cyber-attacks. Debaters need to be able to do this to sort out how cyberattacks have been used, will continue to be used, and what the relevant alternatives are.

Affirmative Argumentation

The affirmative side as the benefit of being able to draw from a world where the United States actively deploys offensive cyber-attacks. The negative side can draw from examples of cyber attacks gone wrong but must speculate over what the alternative doctrine might be, and where existing streams of funding might be rerouted.

The affirmative should start by considering how cyber weapons are used to enforce proportional retaliation against American adversaries. This means that cyber weapons allow America to respond to threats and provocation in a meaningful way, but without escalating the situation or acting in a manner that would provoke hostility from the broader international community. For instance, the United States has used offensive cyberattacks to disrupt and degrade cyber facilities in Russia and North Korea following cyber threats from those countries. The United States had to respond to the threats that these countries posed, and was limited in the number of alternative actions which it could pursue at the time. America was certainly not willing to bomb Russia or impose crippling economic sanctions in retaliation for Russian disinformation campaigns. Cyberweapons provide a tool short of kinetic military force which allows the United States to deal with adversaries. In the Iran example provided earlier, cyber weapons allowed the United States to delay Iranian nuclearization without resorting to a

massive bombing campaign or ground invasion. Either of these options would have killed thousands and cost America billions. Being able to use cyber operations gave America the option of punishing Iran without forcing the United States to choose between doing nothing and an unacceptable level of military force.

Negative Argumentation

The negative team should start by thinking of ways in which cyber weapons trade-off with other important priorities. This could include research into encryption and cyber defense, as well as enabling blowback from adversaries who steal American cyber weapons and use them against us.

On argument which negative teams should strongly consider is that offensive cyber weapons often get stolen and turned against the American government. This means that even if there are some benefits from using offensive cyber weapons, the harms are likely much worse. America can achieve some modest foreign policy goals by hacking, but because we are the world's most advanced economy and one of the most digitized, we are uniquely vulnerable to cyber-attacks. This was proven earlier this year when hackers stole a military cyberweapon developed by the NSA. The hackers posted the weapon online, allowing thousands to hackers and foreign governments to access the code. This cyber weapon has been since used around the world, especially against American targets. The city of Baltimore's computer systems were hacked and virtually destroyed by this virus, which caused millions of dollars in damage and

misery. Reports also suggest that countries such as Russia and China are stealing and reverse engineering American cyber weapons to use them in future engagements. The implication of these developments is troubling because it gives Russia and China a whole new form of leverage against third party countries. At the end of the day, America is worse off than before because the development of cyber weapons has empowered our adversaries.

Good luck and all the best!

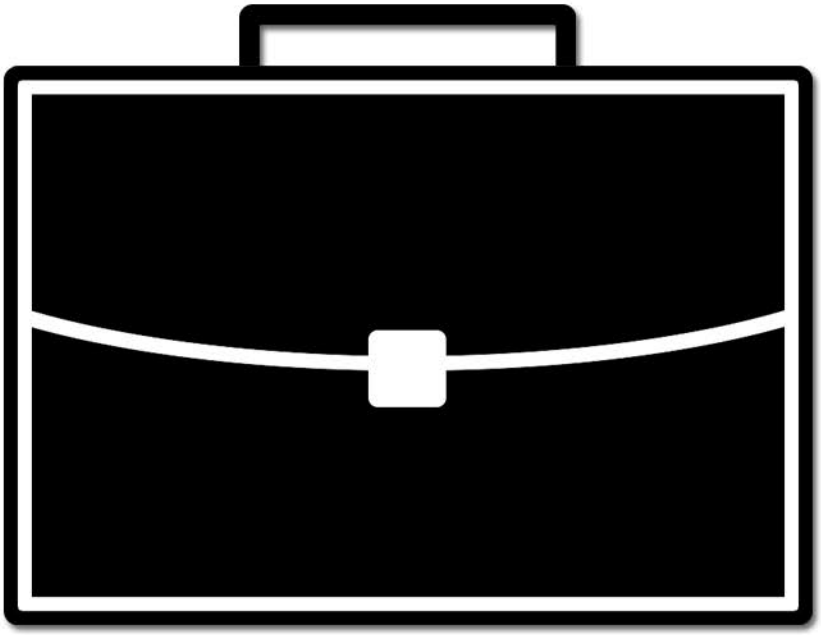
About Jakob Urda

Jakob grew up in Brooklyn, New York. He attends the University of Chicago where he hopes to receive a BA in Political Science in 2019, and is interested in security studies and political economy. Jakob debate for Stuyvesant High School where he won Blake, GMU, Ridge, Scarsdale, Columbia, the NCFL national championship, and amassed 11 bids. He coached the winners of the NCFL national tournament, Harvard, and Blake

Champion Briefs

Nov/Dec 2019

Public Forum Brief



General Information

General Information

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

Foreword: We, at Champion Briefs, feel that having deep knowledge about a topic is just as valuable as formulating the right arguments. Having general background knowledge about the topic area helps debaters form more coherent arguments from their breadth of knowledge. As such, we have compiled general information on the key concepts and general areas that we feel will best suit you for in- and out-of-round use. Any strong strategy or argument must be built from a strong foundation of information; we hope that you will utilize this section to help build that foundation.

What are Offensive Cyber Operations?

Offensive cyber operations are when the US engages in its own cyber attacks on other nations' or other adversaries' cyber networks. This can take many forms. For example, it can include hacking into their intelligence networks to gain information about future plans for cyber attacks the US or really anything for that matter. It can also include attacks on a country's power grid or government computer system to impose damage upon them.

This is in contrast to defensive operations, which are measures the US can take to stop other actors from launching offensive attacks on the US. This can include installing encryption to our information or robust firewalls that make it difficult for hackers to get access to our information networks.

Why are we discussing offensive cyber operations right now?

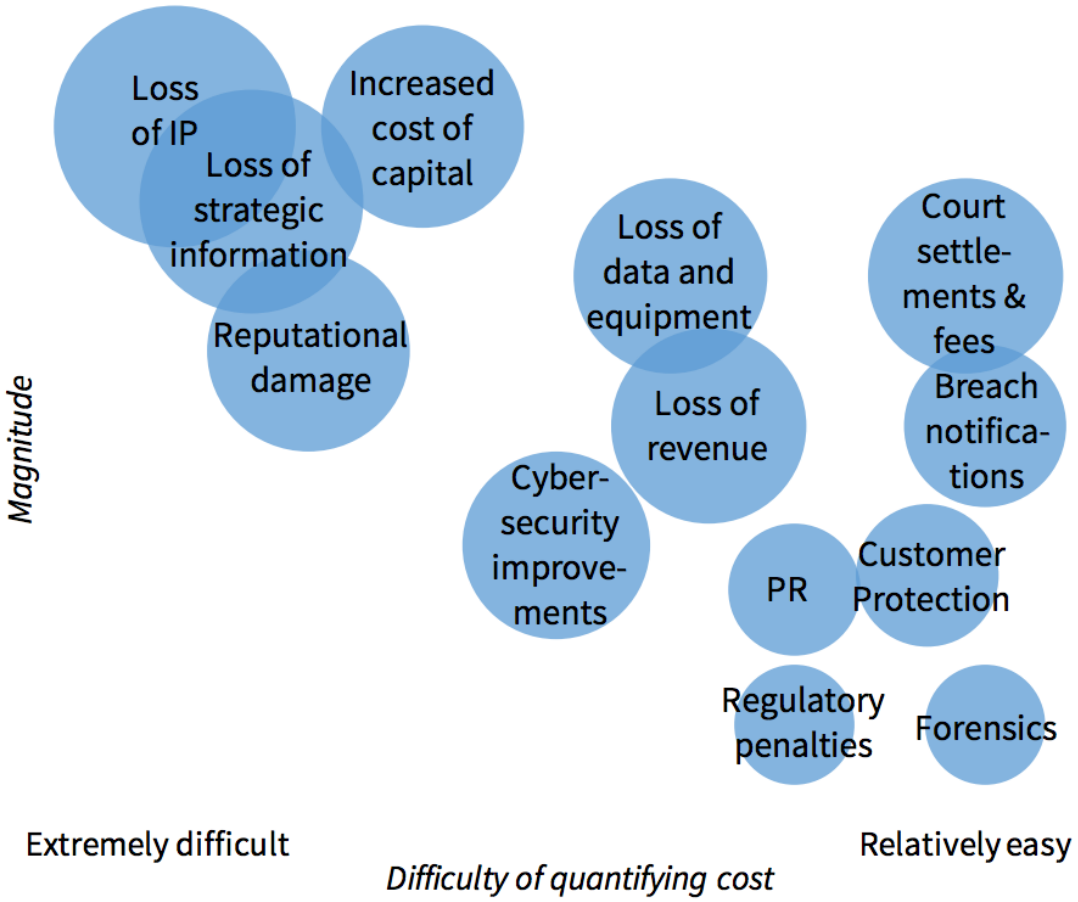
It is part of a new strategy to "defend forward" against adversaries' urge to meddle with our economy and electoral process.

According to John Bolton, our national security advisor, "We're now looking at — beyond the electoral context — a whole range of other activities to prevent this other kind of cyber interference … in the economic space, as well."

Shannon Vavra of Cyberscoop explains in 2019, "The U.S. faces many digital economic threats, including a particularly aggressive salvo from Beijing, which continues to steal intellectual property and conduct other cyber-espionage activities, according to the latest Pentagon assessment on Chinese military operations. The U.S. government traditionally has carried out offensive cyber-operations in the electoral context, such as a 2018 Cyber Command operation that interrupted the internet access of a Russian organization that spread political disinformation on social media. Now, according to Bolton, American focus is expanding to deter the theft of IP.

'We're now opening the aperture, broadening the areas we're prepared to act in,' Bolton said Tuesday, also citing Russian activity and Chinese influence operations underway in the U.S."

Figure 1. Cost Components of an Adverse Cyber Event



(Source 2)

What could the potential harm of a cyber attack be?

A cyber attack on the US could invoke a lot of damage on our nation. This could take many forms.

An economic attack could involve hacking into a company's data and stealing their information to gain an advantage in the market.

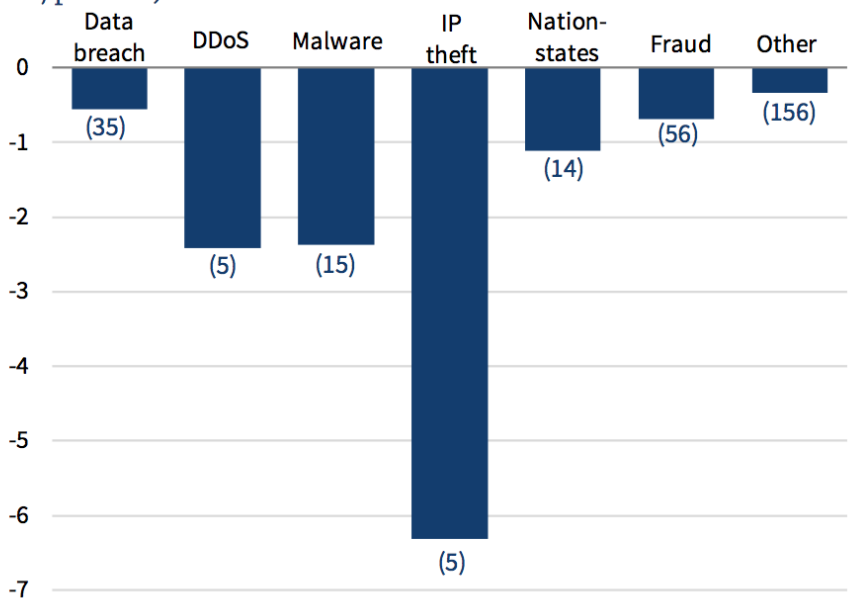
It could be an attack on a US power grid, which would leave large amounts of the country without power.

It could be an attack on our electoral system, where a country could change the vote counts for candidates and thus shift the result of our elections.

It could be an attack on the US government's data, whereby other nations can steal our intelligence.

This graph shows the average loss of returns for companies based on the kind of cyber attack they undergo.

Figure 3. Cumulative Abnormal Return by Type of Adverse Cyber Event
(CAR, percent)



Note: Number of observations is in parentheses.
Sources: Thomson Reuters; CEA Calculations.

Example of Offensive Cyber Attacks:

According to the Washington Post,

"President Trump approved an offensive cyberstrike that disabled Iranian computer systems used to plan attacks on oil tankers in the Persian Gulf , even as he backed away from a conventional military attack in response to its downing Thursday of an unmanned U.S. surveillance drone, according to people familiar with the matter.

The cyberstrikes, launched Thursday night by personnel with U.S. Cyber Command, were in the works for weeks if not months, according to two of these people, who said the Pentagon

proposed launching them after Iran's alleged attacks on two oil tankers in the Gulf of Oman earlier this month.

The strike against the Islamic Revolutionary Guard Corps was coordinated with U.S. Central Command, the military organization with purview of activity throughout the Middle East, these people said. They spoke on the condition of anonymity because the operation remains extremely sensitive.

The operation did not involve a loss of life or civilian casualties — a contrast to conventional strikes, which the president said he called back Thursday because they would not be 'proportionate.' "

Who are the major cyber powers?

Similar to the major military powers, the largest cyber powers are those with the largest economies and thus the largest budgets for spending on cyber defense.

According to the World Economic Forum, "The countries which are believed to have the most developed cyber warfare capabilities are the United States, China, Russia, Israel and the United Kingdom.

These cyber superpowers have responded to a rapidly growing number of attacks in recent years.

The United States stepped up its focus on cyber warfare in 2010 when US Cyber Command brought together the cyber capabilities of the Army, Air Force, Navy and Marines under one roof. Billions of dollars have been dedicated to the project. Two years ago the Pentagon announced a massive expansion of its cyber capabilities, upping staff from 1,800 personnel in 2014 to 6,000 in 2016.

China has followed a similar path, recently announcing it was unifying its capabilities to better develop its cyber warfare might.

Russia is also known to have heavyweight cyber capabilities. The country is strongly believed to have used cyber weapons to attack Georgia during the military incursion into the country in 2008. In early 2014, the Cyber Snake program that attacked the Ukraine is believed to be of Russian origin.

Israel's emergence as a cyber-powerhouse – with an estimated 10% of global sales of computer and network security technology – has meant it is well placed as a cyberwar superpower.

And in Europe, London is seen as the centre of cyberwar specialism with the British government having invested heavily in cyber capabilities over recent years.

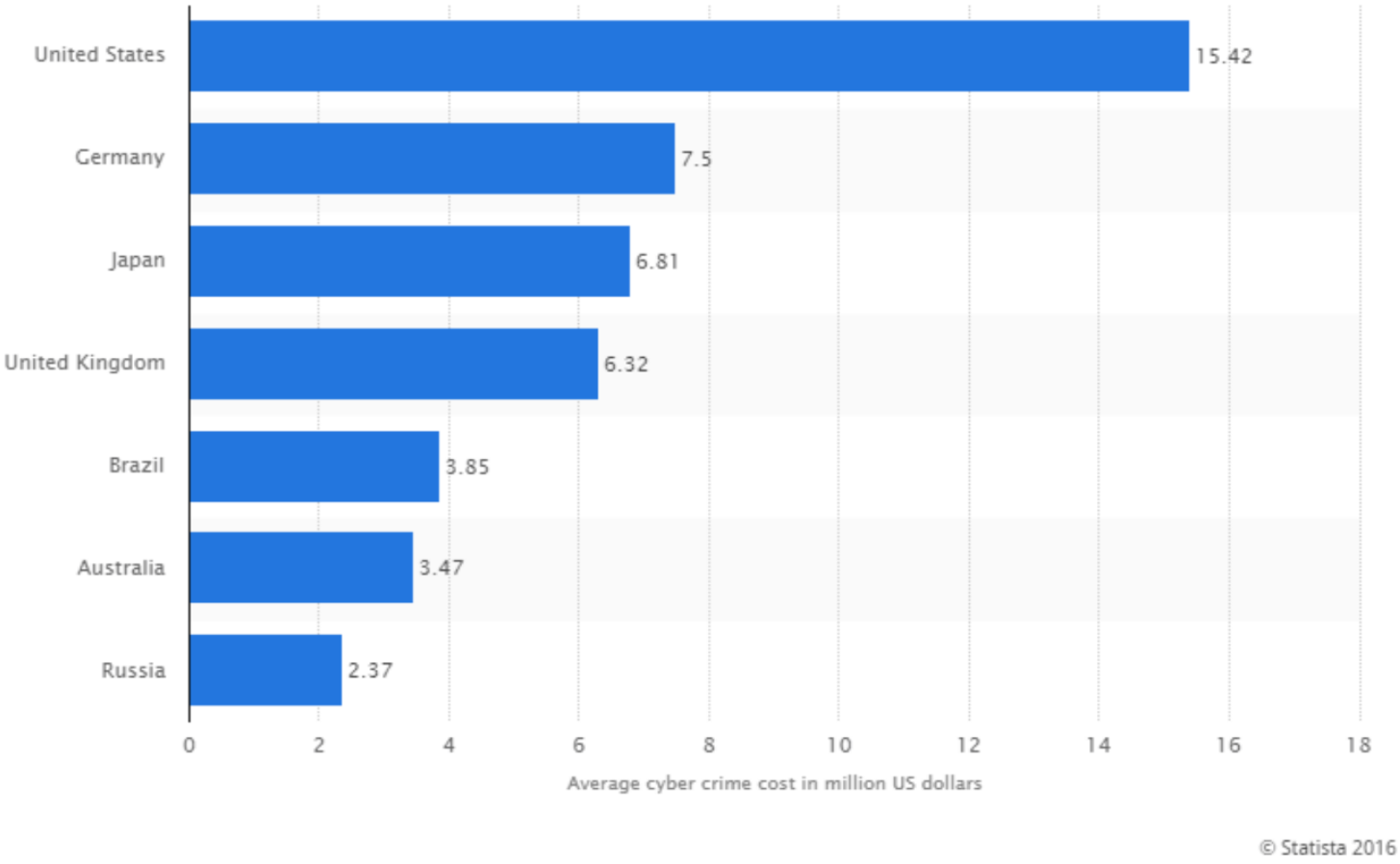
Two other notable players are Iran and North Korea.

North Korea is believed to be behind a significant number of attacks on the United States including the one which recently targeted Sony.

Iran is rapidly developing its cyber capabilities and is thought to be behind several major attacks in the region.

In 2012, Iranian hackers struck Saudi Arabia's national oil company, Saudi Aramco, nearly obliterating its corporate IT infrastructure, and bringing the company close to collapse.

There is concern that while there is something of a 'digital equilibrium' between the five cyber superpowers based on the assumption that attacks will result in reprisals, Iranian hackers seem more willing to cause damage."



What about Cyber Terrorism?

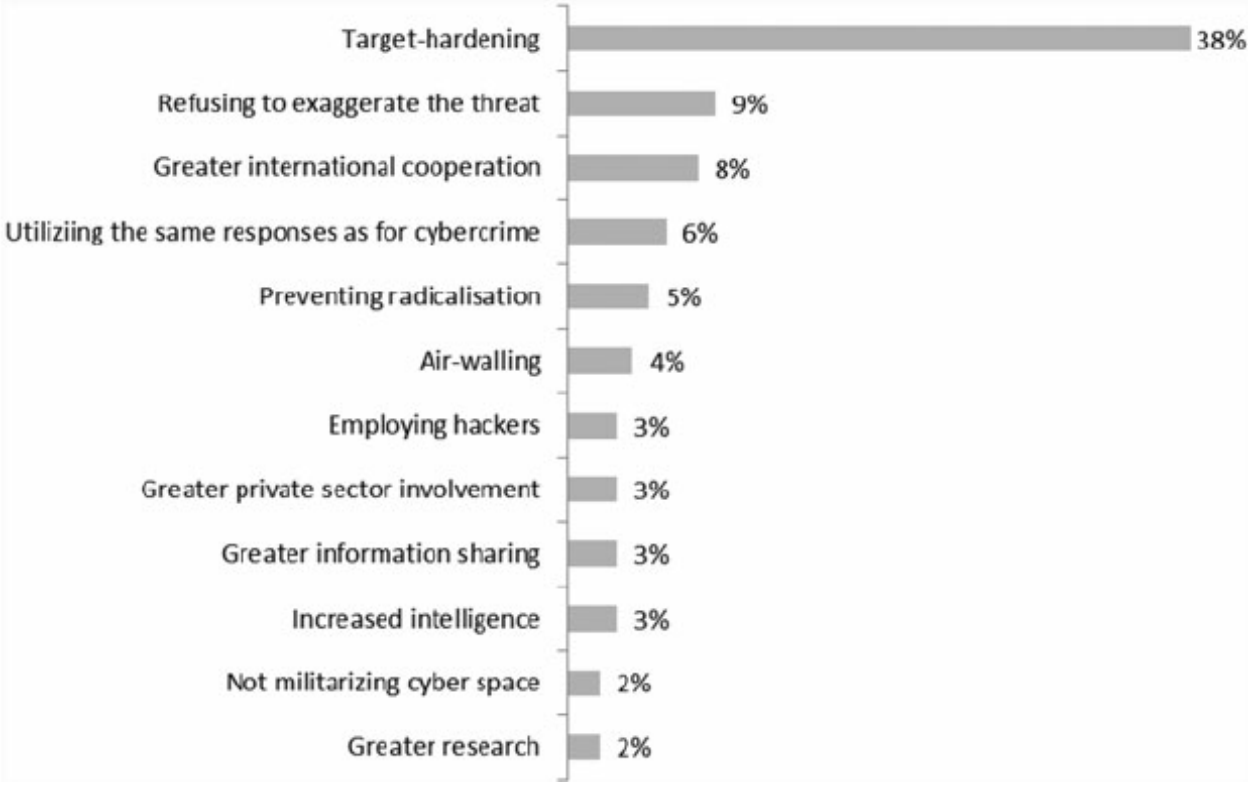
There are cyber terrorists just like there are terrorists who use conventional military tactics like bombs and shootings.

Cyber terrorists are usually referred to as "hackers," and they can be motivated by a variety of factors. Some seek personal economic gain by hacking into information about the

economy they can use for personal profit. Some seek to gather information they can use for blackmail.

Cyber terrorists are an elusive threat because they are hard to track down and it is hard to pin down the location of them.

Unfortunately, the threat of cyber terrorism has been growing in recent years, as computers have become more and more integral to the way our nation functions.



Works Cited

Vavra, Shannon. "U.S. Ramping up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says." CyberScoop, 11 June 2019, https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/.

US Federal Government (CEA). The Cost of Malicious Cyber Activity to the U.S. Economy. Feb. 2018.

Nakashima, Ellen. "Trump Approved Cyber-Strikes against Iranian Computer Database Used to Plan Attacks on Oil Tankers." Washington Post, 22 June 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

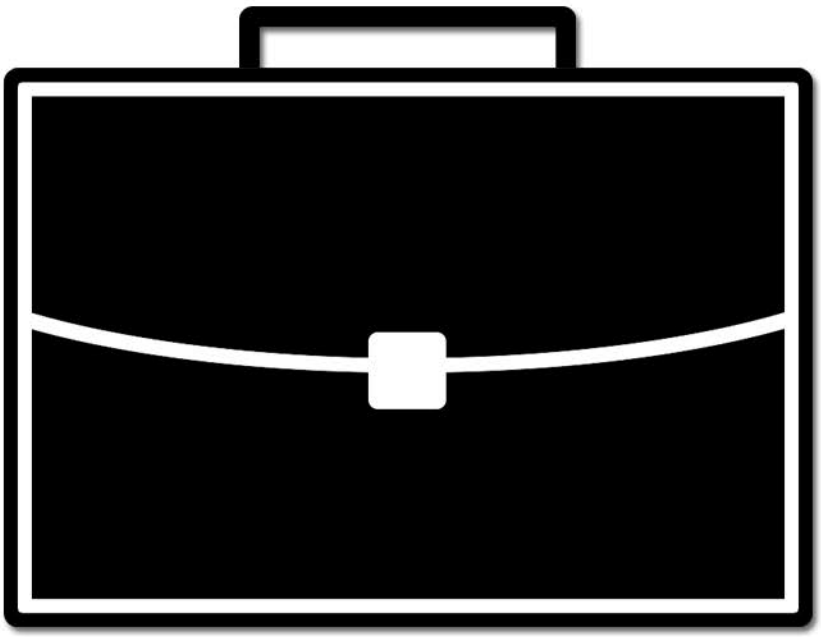
Kieth Breene. "Who Are the Cyberwar Superpowers?" World Economic Forum, 4 May 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

Jarvis, Lee & Macdonald, Stuart & Nouri, Lella. (2014). The Cyberterrorism Threat: Findings from a Survey of Researchers. Studies in Conflict and Terrorism. 37. 68-90. 10.1080/1057610X.2014.853603.

Champion Briefs

Nov/Dec 2019

Public Forum Brief



Pro Arguments with Con Responses

PRO: Offensive cyber operations help deter Russia

Claim: Offensive cyberwarfare operations can deter Russia

Warrant: Tensions between the two have been on the rise

Dorell, Oren. "Another Cold War? Tensions between U.S. may be higher now." USA Today. 3/29/18. https://www.usatoday.com/story/news/world/2018/03/29/united-states-russia-cold-war-putin-trump/467806002/

Is a second Cold War brewing? Not so fast.

President Trump's expulsion this week of 60 Russian diplomats over the poisoning of a Russian double agent in Britain eclipsed the 55 diplomats then-President Ronald Reagan expelled in 1986 during the height of the Cold War.

Measures to remove Russian diplomats by Western countries, and Moscow's retaliatory expulsions of the same number on Thursday, were a throwback. But much has changed since the collapse of the Soviet Union. The Russians have new tools at their disposal.

The rules of engagement for both countries are less clear. And the United States and its allies are much stronger now.

The differences make the tensions between Russia and the U.S. possibly more volatile, but they also create opportunities for the West. Here are a few ways what's happening now is not like the Cold War:

Warrant: The U.S is more willing to act offensively under Trump

"Trump boosting offensive capabilities in cyber strategy." APNews. 9/20/18. https://www.apnews.com/f309d407b5354a6e9104a715911499d7

The White House is warning foreign adversaries that the U.S. is preparing to step up its offensive cyber capabilities as part of a new government-wide strategy.

President Donald Trump on Tuesday is signing a National Cyber Strategy that furthers his lifting of Obama-era constraints on offensive actions.

National Security Adviser John Bolton says, “We’re going to do a lot of things offensively,” adding, “Our adversaries need to know that.”

Bolton says the reason for the new strategy is that “Americans and our allies are under attack every day in cyberspace.”

The strategy directs federal agencies to work with state and local governments to shore up government systems, and to coordinate with private-sector companies to address threats.

Bolton says the U.S. is aiming “to create the structures of deterrence” in cyberspace.

Warrant: The U.S has managed to infiltrate Russia’s grid

Klar, Rebecca. “Russia: Reported US cyberattack on power grid possible.” The Hill. 6/17/19. https://thehill.com/policy/national-security/448847-russia-reported-us-cyberattack-on-power-grid-possible

The Kremlin on Monday reportedly said it is possible the U.S. put implants into Russian power grids.

The New York Times first reported the U.S. allegedly gearing up for a cyberattack last week, citing unnamed officials describing the types of actions that had been taken toward Russian power grids.

Kremlin spokesman Dmitry Peskov told Reuters, “Undoubtedly this information shows the hypothetical possibility ... all signs of cyber war and military cyber action against the Russian Federation.”

The Hill has reached out to the Kremlin for comment.

Peskov told Reuters that Russian authorities are working to keep its economy safe after unnamed strategic parts had endured foreign cyberattacks.

According to the New York Times report, probes in control systems have been in place since at least 2012 but now the strategy is shifting toward offense.

Officials told the Times the U.S. had deployed computer code within Russia's grid to combat Russian disinformation and hacking in 2018 elections.

Impact: Acting offensively can deter Russia

"Trump boosting offensive capabilities in cyber strategy." APNews. 9/20/18. https://www.apnews.com/f309d407b5354a6e9104a715911499d7

The White House is warning foreign adversaries that the U.S. is preparing to step up its offensive cyber capabilities as part of a new government-wide strategy.

President Donald Trump on Tuesday is signing a National Cyber Strategy that furthers his lifting of Obama-era constraints on offensive actions.

National Security Adviser John Bolton says, "We're going to do a lot of things offensively," adding, "Our adversaries need to know that."

Bolton says the reason for the new strategy is that "Americans and our allies are under attack every day in cyberspace."

The strategy directs federal agencies to work with state and local governments to shore up government systems, and to coordinate with private-sector companies to address threats.

Bolton says the U.S. is aiming "to create the structures of deterrence" in cyberspace.

Analysis: The United States has been the victim of several attacks online at the hands of its adversaries, but now that it's announced that its willing to respond, it's less likely to be attacked in the future. Russia will think twice knowing that the United States is capable of hacking into its electrical grid and potentially shutting down the power for an extended period of time.

A/2: Offensive cyber operations help deter Russia

Claim: Russia may respond.

Warrant: Acting aggressively will lead to escalation.

Greenberg, Andy. "How Not To Prevent a Cyberwar With Russia." Wired. 6/18/19. https://www.wired.com/story/russia-cyberwar-escalation-power-grid/

In the short span of years in which the threat of cyberwar has loomed, no one has quite figured out how to prevent one. As state-sponsored hackers find new ways to inflict disruption and paralysis on one another, that arms race has proven far easier to accelerate than to slow down. But security wonks tend to agree, at least, that there's one way not to prevent a cyberwar: launching a preemptive or disproportionate cyberattack on an opponent's civilian infrastructure. As the Trump administration increasingly beats its cyberwar drum, some former national security officials and analysts warn that even threatening that sort of attack could do far more to escalate a coming cyberwar than to deter it.

Over the past weekend, The New York Times reported that US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. But judging by Russia's response, news of the grid-hacking campaign may have already had the immediate opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries, even as it claimed that Russia's grid was immune from such threats.

Warrant: Russia has threatened to retaliate

Goud, Naveen. “Russia to retaliate to cyber threats from United States.” Cybersecurity Insiders. https://www.cybersecurity-insiders.com/russia-to-retaliate-to-cyber-threats-from-the-united-states/

Reacting to the news published the New York Times (NYT) about the intrusions into the Russian national infrastructure, the government officials of Russian Federation have released a press statement yesterday saying it knows on how to retaliate to such threats from adversaries and have successfully thwarted them till date.

Announcing the same through RIA and TASS News agencies the government sources working under the regime of President Vladimir Putin have suggested that the cyber attacks were being carried out by Pentagon keeping the US president Donald Trump under sheer ignorance.

Trump, however, reacted to the news published on Saturday in NYT by saying the article is baseless and the news resource was working towards bringing political instability in the region.

Kremlin released a press statement on Monday saying that the news report was completely true as cyber attacks from the US on National Infrastructure of Russia were escalating on a weekly note- all as a part of cyberwarfare triggering World War 3.

“We have managed to neutralize such actions and have enough potential to thwart them with severity”, says Konstantin Yurivich Noskov, the Minister of Digital Development, Communications and Mass Media of Russia.

Analysis: Russia is willing to respond if the United States acts offensively in cyberspace. When the U.S. hacked into the Russian electrical grid earlier this year, Russia stated they were not only able to neutralize the attack, but also that they had the capacity to respond in kind. Doing so could cripple the U.S electrical grid, and put civilian lives at risk.

PRO: Offensive cyber operations are less likely to lead to conflict

Claim: Cyberattacks are less likely to escalate

Warrant: Cyberattacks don't convey consequences and therefore don't escalate.

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

However, cyberattacks are less likely to deter adversaries for the same reasons they are less likely to lead to escalation. Deterrence is all about sending signals to other countries that there will be consequences if they behave badly.

[How cyber operations can help manage crisis escalation with Iran]

As other scholars have noted, the best deterrence signals are ones that are costly, visible and credible. Here's why cyber-operations often fail this test: They may be hard to detect, hard to attribute to their source and hard to turn into a credible threat, because they may rely on vulnerabilities that are easy to plug if the target knows about them. This all makes cyber-operations less escalatory, but also harder to use to send clear signals.

Moreover, as Sanger and Barnes note, the United States is in a particularly vulnerable position when it uses cyberattacks, because the U.S. way of life is more dependent on digitally dependent technologies than Iranian society. So if Iran retaliates to a cyberattack with another cyberattack, the United States may come off worse.

Furthermore, the United States depends more on the global communications

infrastructure than Iran does, generating further vulnerabilities that might deter America from using cyberattacks.

Warrant: Cyberattacks make people less likely to respond with violence

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

Recent work by myself and Sarah Kreps finds that the American public is less likely to support retaliation against cyberattacks than against an airstrike, even when they create similar effects. U.S. government security decision-makers seem to feel the same way. Research by Brandon Valeriano and Benjamin Jensen, as well as evaluation of strategic war games, finds that players are less likely to respond to a crisis by escalating when they are given cyber-tools — and less likely to respond with violent escalation when the adversary conducts a cyberattack.

These researchers looked at responses from people in the United States for the most part. However, statistical analysis of international cyber-incidents reaches mostly similar conclusions, as does research on battlefield operations in Ukraine. The emerging consensus among researchers is that cyberattacks aren't unusually escalatory. If anything, the opposite is true.

Warrant: Cyberweapons can discourage conflicts.

Miller, Maggie. "US cyberattack took out Iran's ability to target oil tankers: report." The Hill. 8/28/29. https://thehill.com/policy/cybersecurity/459199-us-cyberattack-took-out-irans-ability-to-target-oil-tankers-report

A cyberattack carried out by U.S. Cyber Command against Iran in June severely impacted a database used by Iran to target oil tankers, The New York Times reported Wednesday.

Government officials told The New York Times that the secret cyberattack temporarily hurt Iran's ability to target shipping traffic in the Persian Gulf.

The officials discussed the consequences of the cyberattack in order to "quell doubts within the Trump administration" as to whether the attack was worth the loss of access to key intelligence sources in Iran, the Times reported.

U.S. Cyber Command targeted a network run by Iran's Revolutionary Guard Corps, Iran's paramilitary forces, that U.S. intelligence reported was involved in an attack on American oil tankers earlier this year.

Iran is still working to get all its systems back online and recover data that was lost during the June cyberattack, according to the Times.

The cyberattack took place the same day President Trump called off planned military strikes on Iran in retaliation for shooting down an unarmed U.S. surveillance drone. Iran claimed the drone was in its airspace, while U.S. officials said it was in international airspace.

Analysis: Cyberwarfare is different from conflict in that it doesn't have the same effects on human life, at least not directly. As such, it's less likely to escalate conflicts, and less likely to lead to retaliation. Cyberattacks can even be used to prevent future conflicts by disabling military technology, thus stopping counterattacks and rogue actions

A/2: Offensive cyber operations are less likely to lead to conflict

Answer: Cyberattacks have led to escalation and eventually conflict.

Warrant: Cyberattacks lave led to conflict (Israel)

Fazzini, Kate. "Israel says it bombed Hamas compound that committed cyberattacks." CNBC. 5/6/19. https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyberattack-will-lead-to-a-shift.html

The Israel Defense Forces said Sunday it responded to a cyberattack from a Hamas-controlled compound in Gaza with an airstrike, a rare mix of physical and cyber conflict on the world stage.

The cyberattacks emanating from the Gaza facility were aimed at harming Israeli civilians and was thwarted online before the strike, the IDF said, though they did not immediately release further details about the cyberattack.

In Gaza, Hamas militants have launched 600 rockets into Israel, while the country has retaliated with hundreds of strikes on military targets there.

International organizations and militaries have long debated how or when countries should use military force to respond to cyberattacks that could harm citizens.

The incident is certain to spark further debate on how cyberattacks and live conflict should mix. It's an important distinction as countries including the United States grow increasingly concerned at the possibility a cyberattack on the electric grid, water supply or other infrastructure could lead to loss of human life, and create norms for how they will respond to those threats, either immediately or preemptively.

Impact: Retaliatory strikes kill.

Cohen, Kelly. "Violence continues as Israel and Hamas exchange fire over 2 days of fighting." Vox. 5/5/19. https://www.vox.com/world/2019/5/4/18529287/israel-rocket-attack-hamas-450-rockets-idf-airstrikes-tel-aviv

Executing the prime minister's directive, the IDF said Sunday it has conducted attacks on more than 260 military targets in Gaza, including an assault on what the Israeli military described as a "building where Hamas cyber operatives work" and a targeted attack against a Palestinian militant commander it says funneled money to "terror organizations operating within the Gaza Strip."

The successful targeted attack against that commander, Hamed Ahmed Al-Khodary, was the first targeted killing Israel has conducted since 2014. Targeted attacks had been suspended as an olive branch; in previous conflicts, Palestinian critics have called the attacks assassinations.

Three other Palestinians are believed to have been wounded in the attack on Al-Khodary. All told, officials in Gaza say 20 people, including eight civilians, have been killed throughout the weekend.

Who is responsible for some of those deaths is disputed.

For instance, officials in Gaza said that Palestinian civilians Falastine Abu Arar, a 37-year-old pregnant mother, and her 14-month-old niece Siba, were killed by Israeli forces Saturday. However, the IDF has denied this, claiming the woman and child died due to a misfiring of a Hamas rocket.

At least four Israeli citizens have been killed.

Analysis: As cyberwarfare becomes more prominent and devastating, the responses to cyberattacks will be more dire in nature. For example, when Hamas attacked Israel in cyberspace, Israel launched a conventional attack killing 20 people including 8 civilians.

PRO: Offensive cyber operations can deter China

Claim: Offensive cyber operations could stop China's continued cyberattacks.

Warrant: China is engaging in cyberwarfare

Doffman, Zak. "Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities." Forbes. 8/3/19. https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#2fac32716758

The notorious Chinese state-sponsored hacking group APT10, which is believed to act for the country's Ministry of State Security, is the most likely culprit behind a cyber campaign targeting U.S. utility companies in July. The disclosure on August 1 was made by researchers at Proofpoint, who warned that "persistent targeting of any entity that provides critical infrastructure should be considered an acute risk—the profile of this campaign is indicative of specific risk to U.S.-based entities in the utilities sector."

The spear-phishing campaign targeted company employees with emails purporting to be from the National Council of Examiners for Engineering and Surveying (NCEES), emails that claimed to be delivering professional examination results but which were actually delivering "malicious" Microsoft Word attachments. Threat researchers at Proofpoint broke the news and dubbed the command and control malware "LookBack."

According to Proofpoint's Michael Raggi and Dennis Schwarz, once the emailed Microsoft Word attachment is opened, a malicious VBA macro drops files onto the host computer which then provide the malware with the command and control framework needed to access data on the machine. The malware can attack and mimic a wide range of processes on an infected machine—primarily, though, the objective is to steal data files and take operational screenshots.

Warrant: China is stealing US tech

Baker, Sinead. “The US says China is stealing technology to modernize its military, and that could erode American dominance.” Business Insider. 5/3/19. https://www.businessinsider.com/us-accuses-china-steal-military-technology-2019-5

A new Pentagon report said that China uses "cyber theft" and other methods to bolster its military, which the report claims will continue to grow rapidly.
"China uses a variety of methods to acquire foreign military and dual-use technologies, including targeted foreign direct investment, cyber theft, and exploitation of private Chinese nationals' access to these technologies, as well as harnessing its intelligence services, computer intrusions, and other illicit approaches," it said.
One example outlined in the report is from 2018, when China used "dynamic random access memory, aviation technologies, and anti-submarine warfare technologies'" to acquire "sensitive, dual-use, or military grade equipment."

Impact: Threat of retaliation creates deterrence.

“Trump boosting offensive capabilities in cyber strategy.” APNews. 9/20/18. https://www.apnews.com/f309d407b5354a6e9104a715911499d7

The White House is warning foreign adversaries that the U.S. is preparing to step up its offensive cyber capabilities as part of a new government-wide strategy.
President Donald Trump on Tuesday is signing a National Cyber Strategy that furthers his lifting of Obama-era constraints on offensive actions.
National Security Adviser John Bolton says, “We’re going to do a lot of things offensively,” adding, “Our adversaries need to know that.”

Bolton says the reason for the new strategy is that "Americans and our allies are under attack every day in cyberspace."

The strategy directs federal agencies to work with state and local governments to shore up government systems, and to coordinate with private-sector companies to address threats.

Bolton says the U.S. is aiming "to create the structures of deterrence" in cyberspace.

Analysis: China has been engaging in cyberwarfare against the United States for years. The United States has tried to stop these attacks, but China has been able to steal U.S. tech in the process and even used it against them. The United States must go on the offensive to effectively deter China, which requires retaliation.

A/2: Offensive cyber operations can deter China

Answer: Cyberwar with China has already begun.

Warrant: Tensions with China are rising

Shapiro, Ari and Daly, Robert. "Rising Tensions Between The U.S. And China Go Beyond Trade Dispute." NPR. 8/6/19. https://www.npr.org/2019/08/06/748810969/rising-tensions-between-the-u-s-and-china-go-beyond-trade-dispute

DALY: What we really see now is long-term contentious relations between the United States and China. This is a major development that is going to be worked out most likely over the course of decades. China is now, essentially, a peer competitor to the United States...

SHAPIRO: Meaning it has a comparably sized economy.

DALY: It means it has a comparably sized economy. It is narrowing the gap - military gap - especially in the Western Pacific, where it is using asymmetric tactics that can offset things like our aircraft carriers. China is also an education leader. It is becoming a technological leader. And it's the world's biggest trading nation.

So China is on the move all over the world. And the U.S.-China relationship is not anymore just Beijing to Washington. It's being measured in Africa, in South America, at both poles, in cyberspace and outer space.

SHAPIRO: And is it becoming a more adversarial relationship now because of China's growth, because it suddenly is big enough to really challenge the United States?

DALY: Well, there's a big argument in the United States about this. There's one group of folks who think that engagement policy failed. We engaged with China from 1979 until about 2013 when Xi Jinping came into power. And the idea of engagement was that

coevolution was in the American interest as well as in China's interest. And you could bring China along to be a responsible player to some degree.

Many hardliners in the United States government - and outside and including in the expert community - now claim that engagement was a sucker's game and that we have raised up a tiger which could now devour us. But there are different schools of thought about this, and many of us think that we still need to engage with China, albeit more strategically.

SHAPIRO: That image of raising a tiger that will devour us is very dramatic. Is that what we're talking about here? I mean, like, one or the other will triumph?

DALY: I don't think so. I'm actually borrowing from a Chinese phrase - (speaking Chinese) - you don't want to raise up a baby tiger because it grows up. But again, there are people like Steve Bannon and the Committee for the Present Danger: China, which now claim that China is an existential threat to the United States. And they're also claiming that the United States cannot coexist with the Chinese Communist Party, despite the fact that we've been doing so at least since 1949.

Warrant: China and US already engaged in cyberwarfare

Doffman, Zak. “Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities.” Forbes. 8/3/19. https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#2fac32716758

The notorious Chinese state-sponsored hacking group APT10, which is believed to act for the country's Ministry of State Security, is the most likely culprit behind a cyber campaign targeting U.S. utility companies in July. The disclosure on August 1 was made by researchers at Proofpoint, who warned that "persistent targeting of any entity that provides critical infrastructure should be considered an acute risk—the profile of this campaign is indicative of specific risk to U.S.-based entities in the utilities sector."

> The spear-phishing campaign targeted company employees with emails purporting to be from the National Council of Examiners for Engineering and Surveying (NCEES), emails that claimed to be delivering professional examination results but which were actually delivering "malicious" Microsoft Word attachments. Threat researchers at Proofpoint broke the news and dubbed the command and control malware "LookBack." According to Proofpoint's Michael Raggi and Dennis Schwarz, once the emailed Microsoft Word attachment is opened, a malicious VBA macro drops files onto the host computer which then provide the malware with the command and control framework needed to access data on the machine. The malware can attack and mimic a wide range of processes on an infected machine—primarily, though, the objective is to steal data files and take operational screenshots.

Analysis: China has been attacking the United States in cyberspace for years. Engaging in offensive operations will not change what has been a sustained effort on behalf of Chinese hackers. At a time when tensions between the U.S. and China are rising, it's unlikely that an attack would calm down this ongoing cyberwar.

PRO: Offensive cyber operations can deter cripple U.S. adversaries

Claim: U.S. cyberweapons can cripple opponents' defenses, deter conflict, and deescalate tension.

Warrant: Cyberweapons are becoming more powerful

Vinik, Danny. "America's secret arsenal." Politico. 12/9/15. https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331

The growth has been snowballing. Last year, the secretary of the Army created a new branch for cyber—the first new Army branch since Special Forces was created in 1987. By October of this year, there were 32 teams, coordinated out of a new joint force headquarters for cyber opened last year in Fort Gordon, Georgia. By next summer, the Army expects to have 41.

What's going on? The growth points to one of the most cutting-edge, but also obscure, realms of American military activity: its cyber strategy, and especially its strategy for cyber offense. The United States already has, most observers believe, the most powerful cyberattack capabilities in the world. Much less clear is just what its capacities actually are—and when the Department of Defense believes it should use them.

In conventional war, weapons and strategies are fairly well-understood; the international community has developed rules of the road for armed conflict. Even tactics wrapped in secrecy, such as covert military raids, are governed by some standards about when and how we use them.

That's not the case with cyber. It's widely acknowledged that offensive cyberattacks will be a necessary component of any future military campaign, and the weapons are being developed now. In April, the DOD released a 32-page document that laid out specific

strategic goals for U.S. cyber offense for the first time. But critics say that document still leaves many questions unanswered about how, when and where the government will use these capabilities.

Warrant: The US is investing

Howell O'Neill, Patrick. "U.S. Air Force invests millions this month on cyberweapons projects." Cyberscoop. 4/25/17. https://www.cyberscoop.com/us-air-force-invested-millions-on-new-cyber-weapons/

Three of the United States' largest military contractors each won multimillion-dollar projects in the last month to boost American offensive power in the cyber domain. Raytheon, Northrop Grunman and Booz Allen Hamilton have all seen their stock prices rise 10 to 20 percent since the November 2016 U.S. election. Investors sprinted to military contractors based on Trump's promises for higher spending on — among other warfighting capabilities — the cyber domain. Many of the world's biggest weapons manufacturers are expanding aggressively into offensive and defensive cybersecurity in search of the same level of profitability found in building conventional weapons systems.

Raytheon will build the Air Force's newest Cyber Command and Control Mission System (C3MS) operating location — at San Antonio's Lackland Air Force Base — after winning an $8.5 million contract this week. Lackland is home to the 24th Air Force, the organization tasked with operating and defending the Air Force's networks. It's currently commanded by Maj. Gen. Christopher Weggeman.

The C3MS system is designed, by the military's description, to extend the U.S. Air Force's "global reach, power and vigilance" into the cyber domain by providing permanent operational support to combatant commanders around the world. In addition to securing Air Force networks and information processing systems, C3MS includes offensive cyberspace operations, expansive real-world and cyber domain

surveillance capabilities and close coordination with other key cyber domain commands including the United States Cyber Command.

Warrant: Cyberweapons can take down opponents

"US launched cyber attack on Iranian rockets and missiles – reports." The Guardian. 6/22/19. https://www.theguardian.com/world/2019/jun/23/us-launched-cyber-attack-on-iranian-rockets-and-missiles-reports

The US military launched a cyber-attack on Iranian weapons systems on Thursday, according to sources, as President Donald Trump backed away from plans for a more conventional strike in response to Iran's downing of a US surveillance drone.

The hack disabled Iranian computer systems that controlled its rocket and missile launchers, two officials told the Associated Press, and were conducted with approval from Trump. A third official confirmed the broad outlines of the strike. All spoke on condition of anonymity because they were not authorised to speak publicly about the operation.

Two of the officials said the attacks, which specifically targeted computer systems of Iran's Islamic Revolutionary Guard Corps (IRGC), had been provided as options after two oil tankers were bombed. The IRGC has been designated a foreign terrorist group by the Trump administration.

Impact: Cyberweapons can disable offensive capabilities

Gilchrist, Karen. "US-Iran cyber strike marks a military game changer, says tech expert." CNBC. 7/2/19. https://www.cnbc.com/2019/07/02/us-iran-cyber-strike-marks-a-military-game-changer-says-tech-expert.html

After the U.S. launched a cyber strike on Iran's weapons systems last month, military warfare could increasingly look like a loss of connectivity — rather than a loss of life, according to a cybersecurity expert.

The attack on Iran's security systems — used to control its rocket and missile launches — was a "game changing" event for both the cyber-security industry and "how we think about geopolitics," Splunk's Haiyan Song told CNBC Tuesday.

"A military action got diverted to really becoming a cyber action," said Song.

U.S. President Donald Trump reportedly approved the cyber attack against the Islamic Revolutionary Guard Corps on June 22, days after Tehran shot down an unmanned U.S. surveillance drone.

Days before the cyberattack, Trump had called off a conventional military assault against Iran, saying that the expected loss of life — estimated to be about 150 people — would have been disproportionate to the downing of the unmanned drone.

The attack marked the latest chapter in the U.S. and Iran's ongoing cyber operations targeting each other. Tensions have been escalating between Washington and Tehran, after the U.S. unilaterally withdrew from the 2015 nuclear deal with Iran last year and began a policy of "maximum pressure" campaign aimed at ending its nuclear ambitions.

Analysis: Cyberweapons are able to shut down opponents before they're even able to strike. With the United States announcing it will take a more aggressive stance, they should be better positioned than ever to prevent conflict and cyberwarfare.

A/2: Offensive cyber operations can deter cripple U.S. adversaries

Answer: The US is not very prepared

Warrant: The U.S. is not prepared for cyberwarfare.

Sellin, Lawrence. "The US is unprepared for space cyberwarfare." Military Times. 10/4/19. https://www.militarytimes.com/opinion/commentary/2019/09/04/the-us-is-unprepared-for-space-cyberwarfare/

Virtually every aspect of American national security, including the detection of threats, the use of weapons, the deployment of forces and their resupply, is now dependent on the integrity of critical space-based capabilities.

In defense parlance, those systems are known as command, control, communications, computing, intelligence, surveillance and reconnaissance (C4ISR) and integral and expeditionary logistics.

Both our major adversaries, China and Russia, have placed a high priority on developing superiority within the electromagnetic battlespace with already demonstrable capabilities in electronic and cyber warfare.

Cyberattacks on space-based systems can produce data loss, service disruptions, sensor interference or the permanent loss of satellite capabilities. An adversary could potentially seize control of a satellite through a cyberattack on its command-and-control system, subtly corrupt the data it provides, or even redirect its orbit, essentially transforming it into a kinetic weapon against other space infrastructure.

Warrant: Countries can neutralize attacks

"Russia thwarts U.S. cyber attacks on its infrastructure: new agencies." Reuters. 6/17/19. https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCN1TI1U0

Russia has uncovered and thwarted attempts by the United States to carry out cyber attacks on the control systems of Russian infrastructure, Russian news agencies cited an unnamed security source as saying on Monday.

The disclosure was made on Russia's RIA and TASS news agencies days after the New York Times cited unnamed government sources as saying that the United States had inserted potentially disruptive computer code into Russia's power grid as part of a more aggressive deployment of its cyber tools.

The newspaper suggested President Donald Trump had not been informed of the intrusions. Trump, without providing evidence, said on Twitter that the article was not true.

The Kremlin had said earlier on Monday that the U.S. newspaper report was worrying and showed that a cyber war was, in theory, possible.

"We see and note such attempts," the Russian security source was quoted as saying in response to the report. "However, we manage to neutralize these actions."

Foreign intelligence services have stepped up cyber attacks against Russia in recent years and are targeting mainly transport, banking and energy infrastructure, the source told TASS and RIA.

Analysis: The United States has not prepared itself for modern cyberwarfare, as most of its adversaries have already developed defenses that surpass its capabilities. When the U.S. attempted to hack into Russia's electrical grid, Russia was not only able to detect these attacks, they were also able to neutralize them in the process.

PRO: Offensive cyber operations help punish adversaries

Argument: Offensive cyber operations are a weapons with significant destructive potential, which could be used to further American foreign policy objectives.

Warrant: Cyber operations are major zones of conflict for the United States

Harash, Yosef. "The Next War Will Happen in the Cybersphere, and Here's What It Will Look Like." Haartez, https://www.haaretz.com/us-news/.premium-what-a-future-cyberwar-will-look-like-1.7441901.

The United States has many reasons to fear cyberpowers like Russia and China. It's hard to say which country is the current leader in cyberwarfare, but the United States, Russia and Israel are all known to possess advanced offensive and defensive capabilities. In 2014 and 2015, there were two major blackouts in Ukraine. In December 2015, more than 200,000 people lost power for between one and six hours. The blackouts were determined to have been cyberattacks; security companies that investigated blamed a group of hackers they dubbed Sandworm. The name derived from references the investigators found to the 1965 novel "Dune" — later made into a film — in the code that caused the blackouts. The security companies believe the hacker group worked with the Russian government, but this has not been confirmed. This is one of the advantages of cyberattacks: It's impossible to be sure who the attacker is.

Warrant: The stakes are high for cyber warfare

Harash, Yosef. "The Next War Will Happen in the Cybersphere, and Here's What It Will Look Like." Haartez, https://www.haaretz.com/us-news/.premium-what-a-future-cyberwar-will-look-like-1.7441901.

The standards for the defense of vital infrastructure in Israel are very high and are set by the Shin Bet security service and government ministries. Israel also has offensive capabilities: In April 2018, a Syrian military official said his country's air defenses had been activated by an Israeli-American cyberattack. The industrial cyberthreat is also affecting purely commercial and nonmilitary companies. **"Nowadays, companies understand the danger of industrial cybersabotage. For example, a one-day shutdown of a plant that makes soft drinks could cost a lot of money, and that becomes a significant risk factor for the company," Giller says. "The big fear is that with the world all so interconnected, even networks that are ostensibly disconnected from the internet are basically connected. They can be reached in different ways, such as by exploiting the human factor, where mistakes are made like plugging in cellphones and doing software updates.** Some companies try to stay disconnected from the internet to reduce the hackers' room for attack, but no company is truly disconnected**."**

Warrant: The United States can use cyber attacks to achieve strategic foreign policy objectives

Kelley, Michael. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." Business Insider, November 20 2013, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

"The Stuxnet virus that ravaged Iran's Natanz nuclear facility "was far more dangerous than the cyberweapon that is now lodged in the public's imagination," cyber security expert Ralph Langer writes in Foreign Policy. **Stuxnet, a joint U.S.-Israel project, is known for reportedly destroying roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control. But the exploit had a previous element that was much more complicated and "changed global military strategy in the 21st century," according to Langer. The lesser-known initial attack was designed to secretly "draw**

the equivalent of an electrical blueprint of the Natanz plant" to understand how the computers control the centrifuges used to enrich uranium, Peter Sanger of The New York Times reported last June**."**

Impact: The world is full of opportunities to leverage cyber-attacks similar to Stuxnet

Kelley, Michael. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." Business Insider, November 20 2013, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

The sober reality is that at a global scale, pretty much every single industrial or military facility that uses industrial control systems at some scale is dependent on its network of contractors, many of which are very good at narrowly defined engineering tasks, but lousy at cybersecurity. Or as one of the architects of the Stuxnet plan told Sanger: "**It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand**." Given that the next attackers may not be nation-states, civilian critical infrastructure becomes a troubling potential target. Langer notes that **most modern plants operate with a standardized industrial control system, so "if you get control of one industrial control system, you can infiltrate dozens or even hundreds of the same breed more."**

Analysis: This argument is foundational for making the affirmative case. It is simply that cyber is a domain that is fast becoming one of the most critical in the future of war, and that America cannot ignore the hard-won opportunities before it. This knowledge is important because it allows you to appeal to the judge based on timeframe: cyber will only continue to become important, it is best for us not to write it off now.

A/2: Offensive cyber operations help punish adversaries

Answer: Offensive cyberattacks could lead to escalation

Warrant: The US could cause backlash

Valeriano, Brandon. "The Myth of the Cyber Offense: The Case for Restraint." CATO, 2 Jan 2015, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

We demonstrate that, **while cyber operations to date have not been escalatory or particularly effective in achieving decisive outcomes, recent policy changes and strategy pronouncements by the Trump administration increase the risk of escalation while doing nothing to make cyber operations more effective.** These changes revolve around a dangerous myth: offense is an effective and easy way to stop rival states from hacking America**. New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game. Cyberspace to date has been a domain of political warfare and coercive diplomacy. An offensively postured cyber policy is dangerous, counterproductive, and undermines norms in cyberspace.** Many have promoted the idea of a coming "Cyber Pearl Harbor," but instead the domain is littered with covert operations meant to manage escalation and deter future attacks. Cyber strategy and policy must start from an accurate understanding of the domain, not imagined realities.

Warrant: Escalation would hurt American interests

Valeriano, Brandon. "The Myth of the Cyber Offense: The Case for Restraint." CATO, 2 Jan 2015, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

New policy options proposed by Cyber Command and the Trump administration risk exacerbating fear in other countries and creating a self-reinforcing spiral of tit-for-tat escalations that risk war even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. **Shifting to a policy of preemptive offensive cyber warfare risks provoking fear and overreaction in other states and possibly producing conflict spirals. Even limited-objective cyber offensive action defined as "defending forward" can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, "intrusions into a state's strategically important networks pose serious risks and are therefore inherently threatening**."

Analysis: This argument is strong because it makes the case that even if some cyber operations are good for American interests, the balance of cyber operations functions to spur backlash to the United States. This is functionally a turn on the argument because it controls the impact.

Answer: Offensive operations are ineffective

Warrant: The advantages are overstated

Valeriano, Branden. "The Myth of the Cyber Offense: The Case for Restraint." Cato Institute, 15 Jan. 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.

The assumption that cyberspace favors the offense is widespread among policymakers and analysts, many of whom use this assumption as an argument for prioritizing offensive cyber operations. Faith in offense dominance is understandable: breaches of information systems are common, ranging from everyday identity theft to well-publicized hacks on the Democratic National Committee. **A focus on offense, however, increases international tensions and states' readiness to launch a counter-offensive after a cyberattack, and it often heightens cyber vulnerabilities. Meanwhile, belief in cyber offense dominance is not based on a clear conception or empirical measurement of the offense-defense balance.**

Warrant: Offensive cyber operations planning can increase vulnerabilities

Farrell, Michael B., et al. "Trump Is Rattling Sabers in Cyberspace — but Is the U.S. Ready?" POLITICO, 13 July 2019, https://politi.co/2jJjsVz.

"Prioritizing offensive operations can increase adversaries' fears, suspicions, and readiness to take offensive action. Cyber offenses include cyber exploitation (intelligence gathering) and cyberattack (disrupting, destroying, or subverting an adversary's computer systems). An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, not technical operation. The difficulty of distinguishing between offensive and defensive tactics makes mistrustful adversaries more reactive, and repeatedly conducting offensive cyber operations only increases distrust. **A focus on offensive operations can also increase vulnerabilities; for example, secretly stockpiling information about vulnerabilities in computers for later exploitation, rather than publicizing and helping civil society to mitigate those vulnerabilities, leaves critical infrastructure vulnerable to attack**."

Analysis: This argument is a turn to the aff argument because it assesses that on balance, cyber attacks actually increase the vulnerabilities of the aggressor county. This means that even if there are gross benefits to using cyber operations, the net effect is negative.

PRO: Offensive cyber operations protect democracy

Argument: With new and increasingly technology-reliant election processes, the US government needs offensive cyber capabilities to prevent harm to American democracy.

Warrant: Elections are becoming more reliant on technology.

1 Stuart, Jack. "Protecting Elections from Cyberattacks". United States Institute of Peace. Apr. 2019. Web. 8 Oct.2019. https://www.usip.org/blog/2019/04/protecting-elections-cyberattacks

With elections increasingly dependent on modern technology, cybersecurity has become a vital shield against election violence and manipulation. Cyberattacks present a growing threat to both nascent and mature democracies, as they can shape the election process, erode citizen trust and trigger other forms of election violence. The 2019 elections in Indonesia and Ukraine illustrate the threat cyberattacks pose, even in relatively consolidated and stable democracies**.** While cybersecurity measures can strengthen institutions and electoral processes, they also shape the tactical considerations of would-be perpetrators of election violence. **Cyberattacks could provide an alternative to more traditional forms of election violence as a method to shape election results, delegitimize the vote, or create general distrust in institutions.**

Warrant: Foreign governments have set the precedent in America during the 2016 election cycle

Wu, Nicolas. "Senate report calls for action against foreign election interference amid Trump-Ukraine controversy" USA Today. 8 Oct. 2019. Web. 8 Oct. 2019.

https://www.usatoday.com/story/news/politics/2019/10/08/senate-russia-helped-trump-against-clinton-2016/3909680002/

A new report released by the Senate Intelligence Committee on Russian interference in the 2016 election has concluded that Russia acted to boost Donald Trump at the expense of Democratic nominee Hillary Clinton and delivers a call for future action to prevent foreign election interference. The report's release comes as controversy swirls around President Donald Trump's requests to foreign nations to open investigations into his political opponent former Vice President Joe Biden. Trump asked Ukrainian President Volodymyr Zelensky to investigate the Biden family and has also called on China to investigate them as well, though China said it would reject the request. **The report says that the Kremlin-backed Internet Research Agency (IRA) "sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin."**Russia has denied any involvement in the 2016 election interference, though Russian President Vladimir Putin has joked about future interference in the 2020 election. **The IRA's activities were part of "a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society**" the committee wrote.

Warrant: Multiple adversary countries have the capability to disrupt US elections in the future

Eric Rosenbach, "America, Democracy, and Cyber Risk: Time to Act." United States Senate Committee on Homeland Security and Governmental Affairs. 24 Apr. 2018. Web. 8 Oct.2019. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Rosenbach-2018-04-24.pdf

Russia is not the only potential threat. North Korea, Iran and China also maintain sophisticated offensive cyber capabilities. These countries also enjoy asymmetric

advantages over the United States in cyberspace. Authoritarian societies often control their domestic media, censor online activity, and shield their citizens from outside information and cyber operations through national firewalls, such as the Great Firewall of China. Over the weekend, China's President Xi signaled that his government will increase its already tight control over internet and social media content as a national security priority, and Russia also has been intensifying its crackdown on internet and media freedoms in the past two years.By contrast, the United States is a digital democracy. Our technological advances, high levels of digital connectivity, and transparent, open society make us vulnerable to foreign cyber and information attacks. In short, we live in a digital "glass house.**"The cyber threat landscape we face is congested, and complex. Our adversaries are increasingly willing to attack non-government networks and private citizens, and to engage in widespread, indiscriminate attacks. North Korea's "WannaCry" cyberattack in 2017 affected organizations worldwide, including temporarily derailing operations at the UK's National Health Service. Russia's 2017 "NotPetya" cyberattack initially targeted Ukrainian organizations, but spread across the world, caused operations at major global transport and logistics companies to grind to a halt, and costing the private sector billions of dollars in damages**.

Warrant: Already shown to be effective in preventing election interference in America

Nakashima, Ellen. "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms." The Washington Post. 27 Feb. 2019. Web. 8 Oct. 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

The U.S. military blocked Internet access to an infamous Russian entity seeking to sow discord among Americans during the 2018 midterms, several U.S. officials said, a warning that the Kremlin's operations against the United States are not cost-free. **The strike on the Internet Research Agency in St. Petersburg, a company underwritten by an oligarch close to President Vladi-mir Putin, was part of the first offensive cyber-campaign against Russia designed to thwart attempts to interfere with a U.S. election**, the officials said. "They basically took the IRA offline," according to one individual familiar with the matter who, like others, spoke on the condition of anonymity to discuss classified information. "**They shut them down.**"

Impact: Cyber attacks erode public trust in election results and could cause backlash violence

Nakashima, Ellen. "Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers." The Washington Post. 22 Jun. 2019. Web. 8 Oct. 2019. https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html

As cyberattacks generally have a lower cost and provide the advantage of anonymity, an increase in the use of cyberattacks could perversely lower the risk of violence in the streets, at least in the short-term. **The subsequent loss of legitimacy in the electoral process can also increase the risk of post-election violence, for instance as delayed results announcements create the suspicion of fraud. Cyberattacks erode public trust in the electoral process and offer losing parties or candidates another reason to question and challenge the results.** Preventing cyberattacks requires not only the adequate funding for EMBs to secure their digital infrastructure, but also educating the public and election staff on the complexities of hybrid warfare and its associated risks.

Analysis: There is a large amount of evidence proving this argument to be true and a real threat. Because this argument covers one of the news stories given the most attention over the last few years, it might be a strategic choice, especially at tournaments or in rounds where you know you will be getting lay judges.

A/2: Offensive cyber operations protect democracy

Warrant: Democracies are inherently going to be more susceptible to cyber warfare

Naim, Moises. "How Democracies Lose in Cyberwar." The Atlantic. 13 Feb 2017. Web. 9 Oct. 2019. https://www.theatlantic.com/international/archive/2017/02/democracy-cyber-war/516351/

What made America uniquely susceptible to the attack from an authoritarian Russia is emblematic of what makes other democracies particularly vulnerable, relative to their authoritarian counterparts, to political cyberattack. For one thing, the 2016 election attack targeted the democratic process itself. In the words of the intelligence community's January 2017 report on the incident, the hacks and leaks worked to "undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency." **They aimed to take advantage of the free flow of information in a democratic society, the affect of that information on public opinion, and the electoral mechanisms through which public opinion determines a country's leadership.** (The assessment did not allege cyberattacks on voting machines, nor asses the actual impact Russian meddling might have had on the final outcome.) **If, on the other hand, a hacker leaked damaging information about Vladimir Putin, there are various obstacles in the way of its having an electoral effect. Restrictions on the media in Russia could prevent the information from circulating widely.** Even if it did manage to attract publicity and sway public opinion, what then? Putin has tight control over the country's electoral apparatus, meaning that a voting citizenry inclined to punish him for leaked evidence of misdeeds has no real mechanism to do so. The Panama Papers leaks of spring 2016, which resulted from the alleged hack of a law firm specializing in offshore banking, help illustrate the point. Though they

exposed shady financial dealings within Putin's inner circle, the Russian media covered them in a way favorable to Putin. The leaks made virtually no dent in his popularity.

Warrant: The real threat to elections isn't cyber attacks, it's Russia on a larger level.

Herb, Lin. 10-9-2019, "Election Hacking, As We Understand It Today, Is Not A Cybersecurity Issue," Lawfare, 5 Jan. 2017. Web. 9 Oct. 2019. https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue

Based on what is known today, improving the cybersecurity posture of the U.S. election infrastructure is certainly a useful measure to take, and the Secure Elections Act is an important step in that direction. But **make no mistake—even an enacted, fully funded and well-implemented Secure Elections Act will not ameliorate the effects of Russian efforts to increase the polarization of the U.S. electorate**. For this reason, **a focus on preventing the hacking of election systems is misleading and dangerous—it distracts us from the real danger to the republic today, which is the toxic nature of political discourse in an internet-enabled information environment that Russia can manipulate in entirely legal ways**. Dealing with this danger will force us as a nation to ask whether the information environment should still be characterized as an information marketplace in which the antidote to bad speech is more speech and good ideas rise to the top. If nothing else, the political events of the past year or two have called that premise into question.

Warrant: Cybersecurity experts say to trust election results

Patterson, Dan. 11-6-2018, "Election hacking: Why cybersecurity experts think we

should trust midterm election results,"CBS News. 6 Nov. 2018. Web. 9 Oct. 2019. https://www.cbsnews.com/news/midterm-election-hacking-cybersecurity-experts-think-we-should-trust-results

But Cris Thomas, a security researcher for IBM Security, is confident that his vote and the majority of Americans' votes will be counted accurately. **Most states and electoral districts still use distinct voting processes and a diverse array of systems. That very diversity, says Thomas, strengthens the outcome of the overall vote. "The resiliency of the electoral process will help ensure that citizens will have their votes counted and the right backups are in place to ensure it,"** Thomas says. Theresa Payton, former White House chief information officer, agrees that voting systems are vulnerable but not defenseless. "I have a high level of confidence that my vote will be accurately counted," says Payton. "The Board of Elections in each State have worked hard to assess their local processes, train their voting poll officials … to better understand the threats targeting the voting process."

Warrant: Cyber Capabilities create distrust within democracies

Hunt, Gus. 4-1-2019, "Building Citizen Trust in Government Platforms," Accenture, https://www.accenture.com/us-en/insights/us-federal-government/cyber-resilience-building-citizen-trust

Much discussion around government cybersecurity today revolves around the risk of losing sensitive data or perhaps even having data manipulated in harmful ways. But what sometimes gets lost in these conversations is something far more fundamental to government: citizen trust. To be successful, citizens must be able to trust that the government has ensured digital operations are secure, safe and authentic. This becomes even more important as the government invests billions of dollars to deliver more services and execute more missions digitally. Without that trust, basic government

functions—whether taking a census, collecting taxes or managing health care—will be questioned and put in peril. On our national journey toward a more digital government, we are gaining steam—but citizen trust must remain high to continue the momentum.

Warrant: Government cyber operations lead governments to become increasingly surveillance heavy

Tenove, Chris. 9-24-2016, "With authoritarianism and state surveillance on the rise, how can civil society be protected from digital threats?," Open Canada. https://www.opencanada.org/features/authoritarianism-and-state-surveillance-rise-how-can-civil-society-be-protected-digital-threats

Before the U.S. elections on Nov. 8, the government had been exploring options for a response to attempts by foreign actors to digitally disrupt elections, which some see as an act of hybrid warfare. **Since the election of Republican candidate Donald Trump, there are now fears of an American slide into a repressive surveillance state**, and the impact a Trump presidency may have on Canada's national security policies. At the same time, police in Quebec confirmed this month that they had been tracking the cellphones of six journalists, and CSIS was found to be illegally storing Canadians' metadat**a. In the UK, the controversial Investigatory Powers Bill, nicknamed the "Snoopers' Charter," was passed this week, allowing for unprecedented hacking powers. Seemingly every day, there are new stories on the surveillance and hacking of activists around the world.** These threats point to a global problem: states and conflict actors now routinely use digital technologies to spy on, hack, disrupt and silence their political opponents. **Sometimes these digital threats remain within state borders, and sometimes they target opponents around the world. This is yet another way in which war — and repression — are just a click away.**

Analysis: By countering the idea that cyber attacks are the most pressing issue against democracy, as well as the premise that cyber attacks can meaningfully change election results and vote count, neg is able to mitigate aff grounds. Strategic neg teams can also use the mitigation of this contention to weigh their cases over their opponents.

PRO: Offensive cyber operations key for future warfare

Claim: Due to various aspects of cyber attacks that make them easier and more preferable option than traditional warfare, cyber warfare is the warfare of the future. America needs cyber capabilities in order to be able to be a significant presence in the global future of fighting and deterring adversaries.

Warrant: Cyber warfare is preferable because it is cheap

"Information Warfare: Cyber Warfare is the future warfare" Sans Institute. 2004. Web. 8 Oct. 2019. https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165

Easy to organize and cheap. **One doesn't need more than a couple of computers with internet access to organize and launch cyber warfare.** Hackers often use tools that are free and simple to operate. For example, there is a tool on the Internet that can reveal any dictionary password in less than a minute [49]. With some software and some experience and know-how one would be able to do the job. Thus **it is far easier to finance cyber warfare than a conventional war. Some disgruntled programmers who are willing to sell their abilities to any buyer are probably easy to find anywhere.** On the other hand, a protection device such as a digital firewall can cost nearly $100,000 [50].

Warrant: Cyber warfare is preferable because it is difficult to detect and respond to.

"Information Warfare: Cyber Warfare is the future warfare" Sans Institute. 2004. Web. 8 Oct. 2019. https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165

Difficult to detect and hard to track. In the offensive mode, we may never even know who the attackers were; disinformation flow is very easy [46]. **If the attack is well planned and coordinated it is hard to find out where it came from and who is responsible for it. One might even be able to wage a clandestine war of sabotage, causing a lot of harm without being detected and thus subjected to retaliation**. That is an absolute illustration of the real challenge and opportunity that information warfare represents. We can launch an attack, and it can appear as if it came from somewhere far distant from its actual point of origin. Likewise, when an attack is launched against us, it's very, very difficult to discover where that attack came from**. Even if you can discover the source, it's very difficult then to launch a strike. What are you striking and why are you doing so?** What public response, public support, will there be for the actions that you are taking if thousands of people die? How do you actually persuade people that this was the right thing to do? There is no evidence to cite of dead babies lying in the street. There is no man standing on the street corner with a gun in his hand. It is not the kind of thing that people are used to. This presents a real challenge [47]. According to Jed Pickel, technical coordinator with the Computer Emergency Response Team (CERT) Co-ordination Centre, attacks were made even more difficult to combat if the perpetrators did not use one specific tool or method. **For the nation state the potential of cyber warfare is something that's attractive, but it's also extremely threatening, because cyber warfare is not about nations; it's about the power that is given to individua**ls [48].

Warrant: Many other countries are developing cyber warfare capabilities

Hoojidonk, Richard. “The Future of War will be Digital.” Richard Van Hoojidonk; Trendsetter and Futurist. 31 Jan, 2019. Web. 9 Oct. 2019. https://richardvanhooijdonk.com/blog/en/the-future-of-war-will-be-digital/

As the world's governments become increasingly aware of the dangers posed by cyber-attacks, they're stepping up their efforts to improve their cyber capabilities, not only to defend themselves from such attacks, but also to use them against their enemies if necessary. In fact, many countries now consider cyber capabilities as an essential part of their operational military capability and their strategic toolbox. **In a joint statement, US intelligence chiefs recently revealed that more than 30 countries of the world, including Russia, China, Iran, and North Korea, are currently building offensive cyber-attack capabilities.**

Warrant: Cyber warfare is the warfare of the future

Johansson, Anna. "The future of war is cyber," Next Web. Feb. 2019. Web. 9 Oct. 2019. https://thenextweb.com/contributors/2019/01/21/the-future-of-war-is-cyber

Gone are the days where battles are fought in person-to-person conflicts. In the coming years, most wars will be waged via computers, servers, and digital weapons. The question is, is the United States prepared for the future?Military battles have evolved a tremendous amount over the years – most of it due to advances in weaponry and technology. In early centuries, wars were fought with hands, fists, sticks, and stones. You had to be close to your enemy to kill. As weapons become more advanced, things like slingshots, bow and arrows, and catapults gave armies the opportunity to attack from a small distance.The first guns allowed for mass killing at a distance – though single-shot rifles were inefficient and time-consuming to use. As automatic guns and long-distance rifles entered the picture, it became possible for battles to be waged at distances. As airplanes, helicopters, and long-range missiles emerged, battles became even more sophisticated. **Today, we stand on the precipice of new warfare. No longer is it necessary for people or weapons to be present. Battles of the future won't be fought on the ground or sea – or even in the air. They'll be waged behind computers and servers**. As warfare evolves, two terms seem to get thrown around more than most:

electronic warfare and cyber warfare. And while related, these two ideas aren't the same. "Electronic warfare includes military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy," security expert Eric Chabrow writes. "Cyber warfare involves crippling adversaries through information systems and the Internet. Electronic warfare and cyberspace operations are complementary and have potentially synergistic effects**."Nations like Russia and China appear well-equipped for this new way of war. The United States, while not totally outmatched, certainly has room for growth.**

Warrant: America is behind on cyber operations

Wheeler, Tarah. "In Cyberwar, There are No Rules," Foreign Policy. 12 Sep. 2019. Web. 8 Oct. 2019. https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense

These days, warfare is conducted on land, by sea, in the air, across space, and now in the fifth battleground: cyberspace. Yet so far, **the U.S. government has fumbled on cybersecurity, outsourcing much of that area of conflict to the private sector in accordance with the Trump administration's most recent National Security Strategy—leaving the country exposed to foreign attack. Those third parties operate under exactly the same incentives as any pharmaceutical company.** If a company's service is the treatment of symptoms, preventive medicine is a threat to its business model. Meanwhile, **pundits, policymakers, and publishers take as gospel what they're told by so-called cybersecurity experts who have more social media followers than relevant credentials in the field,** which is how hysterical "The Hackers Are Coming for Us" editorials find their way into otherwise respectable publications. Increased fear, uncertainty, and doubt surrounding cybersecurity have led to a world where we cannot tell what has and hasn't happened. **The nature of cyberwarfare is that it is asymmetric. Single combatants can find and exploit small holes in the massive defenses of**

countries and country-sized companies. It won't be cutting-edge cyberattacks that cause the much-feared cyber-Pearl Harbor in the United States or elsewhere. Instead, it will likely be mundane strikes against industrial control systems, transportation networks, and health care providers—because their infrastructure is out of date, poorly maintained, ill-understood, and often unpatchable.

Impact: Undeterred cyber attacks can wreak havoc on nations

Knake, Robert K. 4-3-2017, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations. 4 Apr. 2017. Web. 9 Oct. 2019. https://www.cfr.org/report/cyberattack-us-power-grid

A large-scale cyberattack on the U.S. power grid could inflict considerable damage. The 2003 Northeast Blackout left fifty million people without power for four days and caused economic losses between $4 billion and $10 billion**. The Lloyd's scenario estimates economic costs of $243 billion and a small rise in death rates as health and safety systems fail.** While darker scenarios envision scarcity of water and food, deterioration of sanitation, and a breakdown in security, leading to a societal collapse, it would be possible to mitigate the worst effects of the outage and have power restored to most areas within days. At this level of damage, the American public would likely demand a forceful response, which could reshape U.S. geopolitical interests for decades. Traditional military action, as opposed to a response in kind, would be likely.

Analysis: If you frame the round in terms of America needing offensive cyber operations to be able to keep up with a trend towards cyber spaces for warfare, you are able to argue . In this case, American offensive cyber operations are important in order for America to not become irrelevant on the world stage while letting countries like China and Russia dominate.

A/2: Offensive cyber operations key for future warfare

Warrant: Cyber warfare will inherently blend with physical warfare

"The Implications of the Fourth Industrial Revolution for International Security," Freedom and Safety. 4 Nov. 2016. Web. 9 Oct. 2019. http://freedomandsafety.com/en/content/blog/implications-fourth-industrial-revolution-international-security

As robots relieve humans of their jobs, some societies will prove better prepared than others in their use of education and infrastructures for transitioning workers into new, socially sustainable and economically productive ways to make a living. Less prepared nations could see increasingly stark inequality, with economically-excluded young people undermining social stability, losing faith with technocratic governance, and spurring the rise of leaders who aim popular anger at an external enemy. Looking beyond individual technologies allows us to focus on the broader and deeper dimensions of the transformation coming our way. Professor Klaus Schwab, chairman and founder of the World Economic Forum, **argues that the collapse of barriers between digital and physical, and between synthetic and organic, constitutes a Fourth Industrial Revolution, promising a level of change comparable to that brought about by steam power, electricity and computing.** Something that makes this revolution fundamentally different is how it challenges ideas about what it means to be human. For instance, neuroscience is teaching us more about our own fallibility, and also just how 'hackable' humans are. As science continues to uncover difficult truths about how we really operate, we will have to confront basic assumptions about the nature of human beings. Whether this deep transformation will reinforce or undermine a shared sense of human dignity, and what effects it will have on our relationship with organized violence, remain open to question.

Warrant: Cyber war may be overblown as a possibility.

Gartzke, Eric. "The Myth of Cyberwar: Bringing War Back Down from Cyberspace to Earth". MIT Press Journals. 9 Oct. 2019. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136

There is a significant fault, however, in the theme of impending cyber apocalypse: it is far from clear that conflict over the internet can actually function as war. Predictions about the nature or significance of cyberwar generally commit a common fallacy in arguing from opportunity to outcome, rather than considering whether something that could happen is at all likely, given the motives of those who are able to act. Cyber pessimism rests heavily on capabilities (means), with little thought to a companion logic of consequences (ends). Much that could happen in the world fails to occur, largely because those who can act discern no meaningful benefit from initiating a given act. **Put another way, advocates have yet to work out how cyberwar enables aggressors to accomplish tasks typically associated with terrestrial military violence. Absent this logic of consequences, cyberwar is unlikely to prove as pivotal in world affairs, and for developed nations, in particular, as many observers seem to believe**. This article asseThis article assesses the salience of the internet for carrying out functions commonly identified with terrestrial political violence. War is fundamentally a political process, as Carl von Clausewitz famously explained.6 States, groups, and individuals threaten harm to deter or compel, generating influence through the prospect of damage or loss. Military force can also be exercised to maintain or alter the balance of power and resist or impose disputed outcomes. **The internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest. Cyber "war" is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence**.7 The capacity for internet coercion is further limited by some of the same factors that make cyberwar appear at ªrst so intimidating. For threats or demands

to prove effective, targets must believe both that an attack is likely to follow from noncompliance and that the attack is destined to inflict unacceptable harm. Yet, as I detail here, the need to apprise targets of internet vulnerabilities to make cyber threats credible contrasts with the secrecy required to ensure an effective attack.

Warrant: Drone swarm technology is on the rise

Kallenborn, Zachary. 10-25-2018, "The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It," Modern War Institute. 25 Oct. 2018. Web. 9 Oct. 2019. https://mwi.usma.edu/era-drone-swarm-coming-need-ready/

Drone swarm technology—the ability of drones to autonomously make decisions based on shared information—has the potential to revolutionize the dynamics of conflict. And we're inching ever closer to seeing this potential unleashed. In fact, swarms will have significant applications to almost every area of national and homeland security. Swarms of drones could search the oceans for adversary submarines. Drones could disperse over large areas to identify and eliminate hostile surface-to-air missiles and other air defenses. Drone swarms could potentially even serve as novel missile defenses, blocking incoming hypersonic missiles. On the homeland security front, security swarms equipped with chemical, biological, radiological, and nuclear (CBRN) detectors, facial recognition, anti-drone weapons, and other capabilities offer defenses against a range of threats. But while drones swarms represent a major technological advancement, unlocking their full potential will require developing capabilities centered around four key areas: swarm size, customization, diversity, and hardening….Developing drone swarm technology is a multi-service, interagency challenge. Drone swarms offer significant capability for the US Navy in searching for submarines or serving as surface weapons platforms. **The Navy is already developing a basic autonomous boat swarm capability, and the US Marine Corps has successfully tested small swarms for infantry to carry out strikes and electronic warfare attacks.** Drone swarms offer the US Air Force

a novel platform for operations to suppress enemy air defenses, and Greg Zacharias, former chief scientist of the Air Force, believes future F-35 pilots will incorporate information collected from drone swarms. Robotic collaboration could improve the Department of Homeland Security's ability to detect CBRN usages and map disaster impacts.

Warrant: Cyber development creates cyber arms race

Kalnins, Ints. 10-18-2018, "Understanding the Proliferation of Cyber Capabilities," Council on Foreign Relations, 10 Oct. 2018. Web. 9 Oct. 2019. https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities

There is a dire need for systematic, academic analyses on the adoption of cyber capabilities in the international system. Investigating this issue is important for both policymakers and academics because of the potential effects of cyber capabilities on international stability. **The spread of cyber weapons could theoretically lead to a greater likelihood of cyber conflict or a reconfiguration of the global distribution of power, so an understanding of the proliferation of cyber capabilities is critical. One example of an observable development in cyber capability is the creation of military computer network operations** (CNO) units, which I define as government entities located within a state's military structure that are tasked to engage in operations involving computer networks. An obvious example would be U.S. Cyber Command created in 2010. Using this variable, **the first thing that can confirmed by the data is the rapid acquisition of cyber capabilities**. Figure 1 shows the increase in military CNO units from 2000 to 2017 among the ninety-five countries listed as victims in the Council on Foreign Relations' cyber operation tracker. **The number of these units has risen from just five in 2000 to sixty-three in 2017. When compared to previous military innovations such as nuclear weapons, battleships, or aircraft carriers, the rate at which military cyber capabilities have been adopted is notably high**.

Analysis: While cyber operations could potentially grow in popular usage in the future, this does not in any way mean that it is going to serve as a replacement for actual methods of war. There is part logical part factual analysis to be made regarding the practicality of the statement that cyber warfare is the warfare of the future, something that neg should capitalize on in round. By focusing on the current popular methods of war along with skeptics of the power of cyber warfare, neg builds a compelling defense surrounding aff claims.

PRO: Offensive cyber operations key for NATO alliance

Claim: NATO (or the North Atlantic Treaty Organization) is in the process of creating an alliance wide initiative in order to face future cyber attacks. NATO is important for American foreign policy, so America following NATO initiatives is a beneficial foreign policy move.

Warrant: America needs to improve relationship with NATO

Fordham, Alice. 7-10-2018, "NATO Worries How Seriously The U.S. Takes The Alliance's Role," NPR.org, 10 Jul. 2018. Web. 9 Oct. 2019. https://www.npr.org/2018/07/10/627588094/nato-worries-how-seriously-the-u-s-takes-the-alliances-role

DONALD TUSK: **America, appreciate your allies. After all, you don't have that many**. MARTIN: And of course, **NATO leaders are skeptical, to say the least, of President Trump's desire to have a closer relationship with Russia's leader Vladimir Putin, whom Trump will meet after that NATO summit.** From NATO headquarters in Brussels, NPR's Alice Fordham joins us now. **MARTIN: What's the European view on President Trump's demand that NATO allies boost their defense spending?** FORDHAM: Well, **they don't like the tone very much**. But the funny thing is that speaking to diplomats and analysts here, a lot of them actually do agree with the substance of his assertions. They say that NATO urgently needs to take threats more seriously and step up both spending and action. NATO has in fact already been going through huge changes since 2014 when it was really battled by Russia annexing Crimea from Ukraine, which isn't a member of NATO, but it does cooperate with it. So since then it has done things like deploy several groups of troops in countries near the Russian border. It's identified quite a lot of stuff that it doesn't do very well at the moment. There are - different countries' equipment isn't always compatible. Like, it's not clear if their radios can talk to each other

sometimes. And there are concerns that in an emergency it could take weeks for troops and hardware to go over to a frontline because of infrastructure that's been neglected. So, yes, a lot of people do want NATO troops to do more exercises, which does take more money and initiative.

Warrant: Strong NATO is key for potential future conflicts

Hodges, Ben. "Why the United States Needs a Cohesive NATO," German Marshall Fund of the United States. 7 Dec. 2019. Web. 9 Oct. 2019. http://www.gmfus.org/publications/why-united-states-needs-cohesive-nato

If a conflict with China arises, the United States will need a strong, cohesive NATO, as well as other partnerships around the world to maintain order and security in Europe's neighborhood, and perhaps even beyond. The United States remains committed to Europe's security and stability. But it also expects its European allies to pick up their share of the burden for collective security so as to help maintain order in the continent and around the globe. **It is of vital importance to the United States that its defense and security relationship with European countries, especially within NATO, not only remains healthy but is correctly oriented to current and likely future challenges.** Several things remain to be achieved if Europe and the United States in this regard. First, they must build a common approach not only in defense, but across economic, information, and political domains. Second, they must solve the continued inequity in burden sharing that hinders a stronger relationship between them and erodes the confidence of many Americans in the efficacy of NATO. Third, it is necessary to achieve greater coherence on NATO's eastern flank, particularly in the Black Sea region. Fourth, NATO must continue its efforts to improve its deterrence capability against Russia's aggressive behavior.

Warrant: NATO is making an effort to become a more legitimate contender in cyber capabilities.

Tucker, Patrick. 5-24-2019, "NATO Getting More Aggressive on Offensive Cyber," Defense One. 5 May, 2019. Web. 9 Oct. 2019. https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/

In the latest signal NATO is adopting a tougher posture against cyber and electronic attacks, Secretary General Jens Stoltenberg this week said that **the defensive alliance will not remain purely defensive. Stoltenberg told attendees** at the Cyber Defence Pledge conference in London, **"We are not limited to respond in cyberspace when we are attacked in cyberspace." NATO members have already "agreed to integrate national cyber capabilities or offensive cyber into Alliance operations and mission**s," he said. But the parameters of a NATO response to cyber attacks remains undefined. In 2015, Stoltenberg said that **a cyber attack against one member nation could trigger an Article 5 collective response by all members**. Yet only once has a collective response ever been invoked, at the request of the United States following the attacks of September 11, 2001. NATO is a defensive organization, so what an offensive cyber posture looks like remains something of a mystery. An Article 5 response can take many different forms.

Warrant: Cyber attacks against a NATO nation could trigger Article 5 response.

Lewis, James. "The Role of Offensive Cyber Operations in Nato's Collective Defense." The Tallinn Papers. 2015. Web. 9 Oct. 2019. https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf

New military technologies are destabilising. Computers used for attack are one such technology. **NATO has made considerable progress in its efforts to integrate cybersecurity into its planning processes, but while it may have gone as far as the political environment allows, it needs to do more.** NATO's September 2014 summit established that cyber defence is part of the Alliance's core tasks of collective defence, crisis management, and cooperative security. Consistent with its long history as a defensive organisation, the policy emphasised "prevention, detection, resilience, recovery."2 Cyber defence has become a central component of NATO planning, given the success of Russia and others in compromising NATO networks. US intelligence sources assess that any unclassified NATO network that is directly connected to the internet should be considered potentially compromised and that cyber espionage is the principle threat to NATO systems over the next three years. They also assess that Russia, given its record of effective cyber collection, poses the greatest espionage threat to NATO computer networks.3 **The vulnerable state of many NATO members' national networks makes defence a priority, but it cannot be the only priority. Discussion within NATO has focused on a defensive role and on the issue of when a cyber incident could trigger the collective defence provision of Article 5 of the North Atlantic Treaty.** NATO's Computer Incident Response Capability (NCIRC), co-located with Allied Command Operations (ACO), is responsible for defending NATO networks. NATO is improving its cyber defence and helping member states improve their own cyber defences through information sharing, training, and if necessary, the deployment of rapid reaction cyber defence teams.

Impact: Russian containment needs functioning NATO

Ruhle, Michael. "A world without NATO?," NATO Review. 8 Aug. 2018. Web. 9 Oct. 2019 https://www.nato.int/docu/review/2018/Also-in-2018/a-world-without-nato-military-europe-united/EN/index.htm

By contrast, **the end of NATO would dramatically increase Russia's position in European security**. With the United States effectively ceding its status as a "European power", the temptation and the opportunities for Russia to divide or intimidate its European neighbours would grow. It has been said that NATO's continued existence creates a problem for Russia. That may well be true, but **the disappearance of the Alliance would create a problem for Europe: without the NATO protective umbrella, Europe would lack the self-confidence required for a coherent and constructive engagement with the Eurasian power.** Some European countries would seek their own deals with Moscow. Moreover, for many countries in the post-Soviet space, which want to demonstrate their independence from Russia through their relations with NATO, the end of an American security role in Europe would be a strategic disaster. **The new "post-American" power balance in Eurasia would condemn them to remain permanently in Russia's sphere of influence.**

Impact: American interests would be harmed if NATO dissolves.

Ruhle, Michael. "A world without NATO?," NATO Review. 8 Aug. 2018. Web. 9 Oct. 2019.https://www.nato.int/docu/review/2018/Also-in-2018/a-world-without-nato-military-europe-united/EN/index.htm

And what about transatlantic burden-sharing? Would the end of NATO not at least ensure that the United States were finally relieved of an "unfair" financial and military burden? Hardly. The United States defence budget reflects the military expenditures of a global power. It therefore goes well beyond NATO, which at the highest estimate represents no more than 15 per cent of total United States defence spending. **Consequently, the dissolution of NATO would translate into relatively small savings for the United States, yet Washington would lose allies, military bases and the political**

predictability established through daily multilateral consultations in the Alliance framework. The geopolitical winners would be China, Russia and all those who, by using the clarion call of the need to build a "multipolar world", seek to weaken the United States' role in upholding international order. In sum, for all these reasons, a world without NATO would be a bad deal for the United States, for its Allies, and for partners in Europe and beyond.

Analysis: American commitment to NATO is an important international platform. If aff is able to prove the relative important of NATO to both America and sustaining world order as well as establishing the specific need for America to get on better terms with NATO then this argument could be strong. This is a large scale argument that, if argued correctly, can be impacted out to promoting global stability.

A/2: Offensive cyber operations key for NATO alliance

Warrant: Donald Trump has made NATO alliance stronger

Thiessen, Marc. 7-12-2018, "Trump isn't attacking NATO, he's strengthening it," Washington Post. 12 Jul. 2018. Web. 9 Oct. 2019. https://www.washingtonpost.com/opinions/trump-isnt-attacking-nato-hes-strengthening-it/2018/07/12/f3e6d33a-85e8-11e8-8553-a3ce89036c78_story.html

This is not a gift to Russia, as his critics have alleged. The last thing Putin wants is for Trump to succeed in getting NATO to spend more on defense. And if allies are concerned about getting tough with Russia, there is an easy way to do so: invest in the capabilities NATO needs to deter and defend against Russian aggression. Trump's hard line also does not signal that he considers NATO irrelevant. **If Trump thought NATO was useless, he would not waste his time on it. But if allies don't invest in real, usable military capabilities, NATO will become irrelevant. An alliance that cannot effectively join the fight when one of its members comes under attack or runs out of munitions in the middle of a military intervention is, by definition, irrelevant.** NATO needs some tough love, and Trump is delivering it. **Thanks to him, the alliance will be stronger as a result**.

Warrant: NATO stronger than ever

Shaffer, Tony. "NATO is now stronger than ever." The London Center. 4 Feb. 2019. Web. 9 Oct. 2019. https://londoncenter.org/nato-is-now-stronger-than-ever/

The North Atlantic Treaty Organization (NATO) is now stronger than ever. What was a Cold War relic is now returned to service with renewed vigor and teeth. Take it from

NATO Secretary General Jens Stoltenberg himself, who said that **President Trump's pressure on European allies to meet their military funding commitments has had "real results.**" "President Donald Trump is having an impact," Stoltenberg told Fox News in a Sunday morning interview. In all, Stoltenberg continued, "**by the end of next year, NATO allies will add $100 billion extra toward defense. So we see some real money and some real results.** And we see that the clear message from President Donald Trump is having an impact." When asked if he was concerned that President Trump's tough rhetoric might be "helping Putin splinter NATO," Stoltenberg said the exact opposite is happening. "What I see is that actually **NATO is united because we are able to adapt to deliver,**" he explained. "**North America and Europe are doing more together now than before."** For context, U.S. defense spending amounted to just under $686 billion in 2017, equating to 3.6 percent of GDP. By comparison, Germany spent around $45 billion on its armed forces last year, or 1.2 percent of GDP. For years, our NATO allies in Europe have shortchanged the system and relied on the United States to foot most of the bill for our mutual defense, but President Trump shocked the elites of Washington and Brussels by demanding that those countries actually meet their pledges to spend at least 2 percent of GDP on defense.

Warrant: NATO cannot uphold global stability

Gliniecki, Ben. "The inability of NATO to prop up global stability," In Defence of Marxism. 9 Sep. 2014. Web. 9 Oct. 2019. https://www.marxist.com/the-inability-of-nato-to-prop-up-global-stability.htm

In the run up to this summit it has been clear that **NATO is out of its depth. It is fighting battles on multiple fronts, from Ukraine to Iraq and Syria, and it is not up to the task. This impotence is thanks in part to NATO's own internal weaknesses, both economic and political.** The ruling classes in all 28 of NATO's member states are wrestling with decline, stagnation or anaemic recovery in their own economies as a result of the global

crisis of capitalism. None are particularly keen to deal with instability abroad which could further escalate the developing class struggle at home. Furthermore, relations between member states are increasingly strained, as each national ruling class seeks to defend its interests in the midst of economic crisis. For example, it is no secret that the USA and Germany have been somewhat at odds over how to deal with the crisis in Ukraine. Germany is heavily dependent on Russian gas for its fuel and so has been more hesitant than the USA, with its plentiful supply of home-grown shale gas, to pursue a path of harsh sanctions and belligerent rhetoric towards Russia. **Divisions like this serve to paralyse NATO and compound its inaction.** This chaotic state of affairs is one that the rest of the world watches with interest. The relative stability given to world relations since the end of the Cold War by the collapse of the Soviet Union and the creation of US hegemony is clearly being undermined. NATO's apparent incompetence is a large advertisement for that fact**. As Russia and China begin to assert themselves on the world stage, small nations traditionally allied to the West and searching for security will begin to question the ability of the USA, the EU and NATO to stand up for them when push comes to shove. This questioning attitude among the rest of the world threatens to break up alliances and destabilise world relations even further – a scenario NATO can ill afford to deal with.** NATO's answer to this situation has been the announcement of a rapid response unit of 4,000 troops than can be deployed into Poland or the Baltic republics within 48 hours. The aim is to allow more flexibility to deal with fast moving situations such as those in Ukraine and the Middle East. In essence, this is supposed to be a muscle-flexing exercise by NATO, on behalf of the USA, to demonstrate to its smaller allies that it is still strong enough to defend them and that it is still worthwhile to stick with the West rather than turning towards China or Russia. It is an attempt to shore up the relative stability which characterised world relations from the collapse of the USSR until 2008.

Warrant: NATO cyber security policies are not enough.

Brent, Laura. 12-2-2019, "NATO's role in cyberspace," NATO Review. 2 Dec, 2019. Web. 9 Oct, 2019. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

Given the centrality of cyberspace to the modern way of warfare, it is imperative that the Alliance be equally capable in this domain as the others. The approach of the Alliance is sensible: it seeks to address the most significant challenges associated with operating in cyberspa**ce. Ultimately, though, the Alliance must continue to consider how it can do more, since cyber threats are trending only towards more serious impact.** What more, then, should the Alliance be doing? Allies may wish to consider what aspects of their current work should have the greatest priority and resourcing. The CyOC, for example, is the most significant aspect of adapting the NATO Command Structure for cyberspace. **As the CyOC moves towards first initial then final operating capacity, it will be critical that it is resourced with sufficient – and sufficiently expert – personnel.** The level of malicious cyber activity below the threshold of armed conflict will remain a continuous challenge; as Allies consider how best to respond, both individually and as an Alliance, they may wish to consider existing tools. In addition to Article 5, generally the most well-known part of the Washington Treaty, Allies also have Article 4 at their disposal, which allows for consultation whenever any Ally believes an Ally's "territorial integrity, political independence, or security" is threatened. **Finally, when seeking to keep pace with change in this domain, Allies might see benefit in continuing to evaluate how collaboration with industry might evolve – both how it shares information and how it procures technologies.** The Alliance, in short, should continue on its current path, ensuring that through continued attention and resources, cyberspace can become an ordinary part of business.

Analysis: If NATO is already in a strong position, specifically because of current American influence in the policies of the organization, then it makes it difficult to link into the argument that America needs to "stay in favor" or "make up ground" in NATO. Furthermore, supporting America following NATO's cyber measures may be bad if they are not advanced enough. And delinking aff from the importance of NATO as an organization minimizes aff ground.

PRO: Offensive cyber operations can stop Iranian oil threat

Claim: Currently, Iran is dangerously in control of an important international oil passageway. Because of the threat of Iran closing the Strait, America needs cyber attacks to be able to respond in order to prevent a global oil crisis.

Warrant: The Strait of Hormuz is incredibly important internationally for oil

Letzing, John. 7-29-2019, "Why is the Strait of Hormuz so important?," World Economic Forum. 5 Jul. 2019. Web. 8 Oct. 2019. https://www.weforum.org/agenda/2019/07/why-is-the-strait-of-hormuz-so-important

When Iran's Islamic Revolutionary Guard Corps seized a British-flagged ship in the Strait of Hormuz on July 20, it further escalated an ugly geopolitical standoff – and underlined the crucial importance of this passageway to the Persian Gulf. Iran's move came after the British Navy seized an Iranian ship near Gibraltar, on the grounds it may have been violating an embargo on oil sales to Syria. The naval tit-for-tat is a result of a broader deterioration of relations between the United States and the United Kingdom on one side, and Iran on the other. In a recent Twitter post, Iran's foreign minister suggested the UK's seizure of the Iranian ship was done at the behest of the US, and stated that Iran doesn't seek confrontation – but will "protect our waters". **The Strait of Hormuz is a logical flashpoint for this geo-economic gamesmanship, due to its location and strategic value for so much of the world. The hook-shaped waterway between Iran and Oman flows from the Persian Gulf to the Gulf of Oman – and beyond that to the Indian Ocean – and is considered the world's most important oil transit chokepoint. The 20.3 million barrels of oil per day shipped through the strait during 2017 accounted for nearly a third of global maritime oil trade that year, and volumes in 2018 accounted for more than a fifth of global consumption**, according to the US

Energy Information Administration. **Also in 2018, 1.4 million barrels per day specifically transited through the strait on their way to the US, in addition to more than a quarter of all global trade in liquefied natural gas.**

Warrant: Iran has power to cripple the Strait

Khatiri, Shay. "Iran Could Close the Strait of Hormuz. America Needs to Be Prepared.," Bulwark. 3 Jan 2012. Web. 8 Oct. 2019. https://thebulwark.com/iran-could-close-the-strait-of-hormuz-america-needs-to-be-prepared

Did Iran attack two oil tankers in the Gulf of Oman? The U.S. government says they did. America's allies, including Japan and Germany, say they want to see more proof. Because every question must invariably become about Donald Trump—is he lying? is this the price of his lack of credibility?—we seem to be ignoring one of the key elements in the situation: the nature of the Islamic Republic regime. **Iran has been threatening to close the Strait of Hormuz—the connection from the oil-rich Persian Gulf to the Sea of Oman to oceans and international waters—for several years now. And one way to read the recent attacks is as an indication that they are demonstrating a willingness to back up with these threats.** Iran could not win a conventional fight with the U.S. Navy. But then, they would have no intention of conducting a conventional fight. **They would seek to cripple shipping, raise the cost of sending trade through the strait, create uncertainty in world financial markets, and sow dissension between America and our allies.** It's not even clear that Iran would openly conduct operations under their own banner. It's just as likely that they would employ maskirovka in order to launder the fight through non-state actors. In other words, **there is a reason that Iran has proved to be such an intractable problem.**

Warrant: Iran historically has acted aggressive in the Strait of Hormuz

Etehadstaff, Melissa. 7-19-2019, "What's behind Iran's actions in the Strait of Hormuz?," Los Angeles Times. 19 Jul. 2019. Web. 8 Oct. 2019. https://www.latimes.com/world-nation/story/2019-07-19/iran-strait-of-hormuz-oil-tanker-seizure

Experts said Iranian officials are trying to demonstrate to the U.S. and its allies that the Islamic Republic is able to push back and gain leverage against the Trump administration's "maximum pressure" policy, which intensified after President Trump pulled the U.S. out of the landmark nuclear deal in May 2018 and reimposed crippling sanctions, making it difficult for Iran to export oil, the foundation of the country's economy. China, Russia and leading Western European countries have sought ways around the U.S. sanctions, but it has been difficult to bypass them. **"The message that Iran is sending is that it is capable of making international waters unsafe not just for the U.S., but for international trade,**" said Reza H. Akbari, a program manager and Iran expert at the Institute for War and Peace Reporting. **By escalating the risk of conflict in the Strait of Hormuz**, Ariane Tabatabai, an associate political scientist at Rand Corp., said that **Iranian officials will be able to use that as leverage and as bargaining chips if they were to resume negotiations with the U.S**. "The Iranian strategy is designed to get Europeans and the international community to step up and force the U.S. to change its policy," Tabatabai said

Warrant: Historically, US cyberattacks against Iran interfere with Iran's ability to close the Strait

Press Team, 10-1-2019, "US cyberattack temporarily paralyzed the ability of Iran to target oil tankers in the Gulf," Cyber Defense Magazine, 1 Oct, 2019. Web. 8 Oct. 2019. https://www.cyberdefensemagazine.com/us-cyberattack-temporarily-paralyzed-the-ability-of-iran-to-target-oil-tankers-in-the-gulf

The New York Times revealed that the US carried out a cyberattack in June on a database used by Iran's Islamic Revolutionary Guard Corps to plot attacks on oil tankers in the Gulf. "**A secret cyberattack against Iran in June wiped out a critical database used by Iran's paramilitary arm to plot attacks against oil tankers and degraded Tehran's ability to covertly target shipping traffic in the Persian Gulf, at least temporarily,** according to senior American officials." states the NY Times. The attack took place on June 20, the US hackers had interfered with the cyber capabilities of Iran's paramilitary arm to target the shipping in the Gulf. The database was used by Iran Guards to choose the tankers to target. **Iranian experts are still working to recover the database and the computer systems, including military communications networks, affected by the attack**. The attack launched on June 20, 2019, is just the last battle in a silent cyber conflict between the US and Iran. The US Governments believe that the cyber attack is a proportional response against the attack against one of its drones. Analysts believe that the cyberattack went ahead after President Donald Trump had called off a retaliatory military airstrike against Iran for shooting down a US drone. Experts pointed out that since the June 20 attack, Iran's Islamic Revolutionary Guard Corps did not target US tankers. The Guard only seized a British oil tanker after one of the vessels of its fleet was detained.

Impact: If Iran closes the strait, global oil prices would surge

Clifford Krauss, 1-4-2012, "Oil Price Would Skyrocket if Iran Closed the Strait of Hormuz," New York Times, 1 Jan. 2012. Web. 8 Oct. 2019. https://www.nytimes.com/2012/01/05/business/oil-price-would-skyrocket-if-iran-closed-the-strait.html?searchResultPosition=1

Energy analysts say even a partial blockage of the Strait of Hormuz could raise the world price of oil within days by $50 a barrel or more, and that would quickly push the price of a gallon of regular gasoline to well over $4 a gallon. "You would get an

international reaction that would not only be high, but irrationally high," said Lawrence J. Goldstein, a director of the Energy Policy Research Foundation. **Just the threat of such a development has helped keep oil prices above $100 a barrel in recent weeks despite a return of Libyan oil to world markets, worries of a European economic downturn and weakening American gasoline demand.** Oil prices rose slightly on Wednesday as the political tensions intensified. American officials have warned Iran against violating international laws that protect commercial shipping in international waters, adding that the Navy would guarantee free sea traffic.

Analysis: The Strait of Hormuz is a contentious and important region in the world with lots of literature surrounding the interaction between Iran and America in the Strait. Teams should make sure to learn the full history surrounding aggression within the Strait in order to understand the intricacies of the argument completely. To make this argument the most strategic, teams should consider arguing Iran's ability to partially close the Strait or look further into the reaction when Iran threatens closure.

A/2: Offensive cyber operations can stop Iranian oil threat

Warrant: American backlash will prevent Iran from agressing in the Strait of Hormuz

Johnson, Keith. "Iran's Hollow Threats to Close the Strait of Hormuz." *Foreign Policy*, Foreign Policy, 5 May 2016, Web . 8 Oct. 2019 foreignpolicy.com/2016/05/05/irans-hollow-threats-to-close-the-strait-of-hormuz

Mine clearance remains a challenge for U.S. forces, which have a small number of ships that can do so. It would require the area cleared of any missile threats beforehand, meaning it would need a much broader military effort. Last month, the United States and other nations conducted a minesweeping exercise in the Persian Gulf centered on the threat posed by underwater improvised explosive devices, rather than the 5,000-odd traditional mines that Iran has in its arsenal."Any form of mine warfare is difficult to deal with," Cordesman said, "and recent exercises have not been reassuring." But, he said, **in the event of any Iranian effort to mine the Persian Gulf or block the Strait of Hormuz, Washington has a lot more tools in its arsenal than minesweepers — and that could be enough to dissuade Iran from ever seriously trying.** "They have a very good understanding of what we did to Iraq's power grid and transportation system in 1991 with precision air power," Cordesman said.

Warrant: Fear of backlash from China will prevent full closure of the Strait.

Michael Singh, "Will Iran dare close the Strait of Hormuz?". The Iran Primer. 6 Jan 2012. Web. 8 Oct. 2019. https://iranprimer.usip.org/blog/2012/jan/05/will-iran-dare-close-strait-hormuz

China, however, is heavily dependent on Gulf oil sources, particularly from Saudi Arabia. **China also happens to be Iran's largest oil customer and provides Iran with critical support in the form of weapons sales and diplomatic cover at the United Nations. Iran can ill afford to anger Beijing.** The United States, the presumable target of an Iranian move against the Strait, would probably suffer like the rest of the world from the effects of rising oil prices. But U.S. oil supplies would not be meaningfully imperiled. The United States imports 49 percent of the petroleum it consumes, and only 25 percent of those imports come from the Persian Gulf, far less than is available in the U.S. Strategic Petroleum Reserve. **China, however, is heavily dependent on Gulf oil sources, particularly from Saudi Arabia. China also happens to be Iran's largest oil customer and provides Iran with critical support in the form of weapons sales and diplomatic cover at the United Nations. Iran can ill afford to anger Beijing.**

Warrant: Closing the Strait of Hormuz would majorly harm Iran's economy

Michael Singh, "Will Iran dare close the Strait of Hormuz?". The Iran Primer. 6 Jan 2012. Web. 8 Oct. 2019. https://iranprimer.usip.org/blog/2012/jan/05/will-iran-dare-close-strait-hormuz

Iran is unlikely to try to close the Strait for several reasons. **The regime** surely recognizes its military disadvantage; it **is also cognizant of its own dependence on the Strait. About 70 percent of Iran's budget revenues are generated by oil exports, all of which must transit the Strait. This fact alone would make a preemptive effort to close the Strait self-defeating.** The United States, the presumable target of an Iranian move against the Strait, would probably suffer like the rest of the world from the effects of rising oil prices. But U.S. oil supplies would not be meaningfully imperiled. The United States imports 49 percent of the petroleum it consumes, and only 25 percent of those

imports come from the Persian Gulf, far less than is available in the U.S. Strategic Petroleum Reserve.

Warrant: Cyber attacks against Iran will lead to an aggressive reaction

Reuters Editorial, "Iran says it will destroy any aggressor," Reuters. 9 Sep. 2019. Web. 8 Oct. 2019. https://www.reuters.com/article/us-saudi-aramco-iran/iran-says-it-will-destroy-any-aggressor-id USKBN1W603G

Iran will pursue any aggressor, even if it carries out a limited attack, and seek to destroy it, the head of the elite Revolutionary Guards said on Saturday, after attacks on Saudi oil sites which Riyadh and U.S officials blamed on Tehran. "Be careful, a limited aggression will not remain limited. We will pursue any aggressor," the head of the Guards, Major General Hossein Salami, said in remarks broadcast on state TV. **"We are after punishment and we will continue until the full destruction of any aggressor."** U.S. President Donald Trump on Friday approved sending American troops to bolster Saudi Arabia's air and missile defences after the Sept. 14 attacks. Iran denies involvement in the attack, which was claimed by Yemen's Houthi movement, a group aligned with Iran and currently fighting a Saudi-led alliance in Yemen's civil war.

Analysis: If by closing the Strait of Hormuz Iran would suffer massive backlash, then they would be extremely unlikely to do so, rendering American attention to cyber operations irrelevant. Furthermore, countries don't intentionally cripple their own economies, so if you can prove that closing the Strait would harm Iran, then you have a very convincing narrative against the claim that Iran is a threat to the Strait.

PRO: Offensive cyber operations stop cyber terrorism

Argument: Offensive operations can help show terrorists that we are able to strike back in response to cyber terrorist attacks.

Warrant: The threat of cyberterrorism is growing

Cronin, Cat. "The Growing Threat of Cyberterrorism Facing the U.S." American Security Project, 2019, https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/.

The 2019 Worldwide Threat Assessment by the U.S. Intelligence Community highlights the concern that "financially motivated cyber criminals" may target the U.S. within the next few years. They warn that this could "disrupt U.S. critical infrastructure in the health care, financial, government, and emergency service sectors." Officials are also concerned that terrorists may hack into databases and obtain personal information that could be used to inspire and enable physical attacks. **The threat of cyberterrorism has grown ever more pressing in the past few years.** As of 2018, 81% of Americans viewed cyberterrorism as a critical threat—an increase from 73% in 2016. There is bipartisan consensus regarding the danger, as Democrats and Republicans express similar concern. Cyberterrorism is considered the second most critical threat to our country, just behind the development of nuclear weapons by North Korea. **Moreover, American military servicemembers assess cyberterrorism to be the greatest danger to U.S. national security. 89% of service members believe that it is a significant or very significant concern, but the majority thinks the U.S. lacks preparedness for a cyberattack.** About a third disapprove of existing policies on combatting cyberterrorism, with many believing the guidelines do not go far enough.

Warrant: The Government needs new strategies to stop cyber terrorism

Katie Lange. "DOD's Cyber Strategy: 5 Things to Know." U.S. DEPARTMENT OF DEFENSE, 2 Oct. 2018, https://www.defense.gov/explore/story/Article/1648425/dods-cyber-strategy-5-things-to-know/.

Cyberspace is critical to the way the entire U.S. functions. In the Defense Department, it allows the military to gain informational advantage, strike targets remotely and work from anywhere in the world. But our competitors – including terrorists, criminals, and foreign adversaries such as Russia and China - are also using cyber to try to steal our technology, disrupt our economy and government processes, and threaten critical infrastructure. That means a thorough strategy is needed to preserve U.S. cyberspace superiority and stop cyberattacks before they hit our networks. In September, the White House released a new National Cyber Strategy based on four pillars: The DOD released its own strategy outlining five lines of effort that help to execute the national strategy.

Warrant: Offensive operations allow us to gather information to stop terrorism

Murat Dogrul,. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. Turkish War College, 2011.https://ccdcoe.org/uploads/2018/10/DevelopingAnInternationalCooperation-Dogrul-Aslan-Celik.pdf

Collecting intelligence is the starting point and the key part of building an international cooperation. Afterwards defensive and offensive (deterrence) collaborative actions should be set out. Counter information and cautions to the related public opinion and parties must be provided by the international organizations as defense strategies. The collection of electronic evidence whenever it relates to terrorism is crucial for the nations who desire to cooperate. An "Intelligence pool"

should be created in order to collect and share the intelligence simultaneously among the nations. This intelligence pool should not only monitor and gather information from terrorist websites, but should also collect electronic evidence for the potential cyber attacks Knop, offers an “open source intelligent system” on this issue. Instead of a hierarchical organization, there should be a network, and knowledge should be pooled. There should be committee management, and a credit point system. **Governments should be allowed to use the resource only to the extent that they contribute good quality information and analysis [1]. The collective open source idea is a well thought-out response to the challenge of organizing international cooperation regarding terrorist contents on the Internet.**

Impact: A cyber attack could be as bad as a nuclear attack

Straub, Jeremy. “Hackers Could Kill More People Than a Nuclear Weapon.” Livescience.Com, 2019, https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html.

With the U.S. and Russia pulling out of a key nuclear weapons pact — and beginning to develop new nuclear weapons — plus Iran tensions and North Korea again test-launching missiles, the global threat to civilization is high. Some fear a new nuclear arms race. That threat is serious — but another could be as serious, and is less visible to the public. So far, most of the well-known hacking incidents, even those with foreign government backing, have done little more than steal data. Unfortunately, there are signs that hackers have placed malicious software inside U.S. power and water systems, where it's lying in wait, ready to be triggered. The U.S. military has also reportedly penetrated the computers that control Russian electrical systems. **As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination**

of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.

Analysis: This is a good argument because the impact of a cyberterrorist attack could potentially be larger than any other sort of attack because cyberterrorists have a lot less to lose than countries do in attacking the US. This could embolden them to attack us as hard as they can, which makes this the biggest impact in the round.

A/2: Offensive cyber operations stop cyber terrorism

Answer: Deterrence does not work on terrorists

Warrant: Deterrence goes against American values

Fisher, Uri. "Deterrence, Terrorism, and American Values." Homeland Security Affairs 3, Article 4 (February 2007). https://www.hsaj.org/articles/152

This article explores the practical obstacles to applying deterrence to United States counterterrorism policy. Many commentators still discuss deterrence as a tool for U.S. policymakers to use to prevent future terrorist attacks on the U.S. homeland or its interests abroad. **This paper argues that, while theoretically deterrence may be a viable approach to defending against terrorism, the actual policy choices that will be required of the U.S. to deter terrorism are morally and politically problematic. To effectively deter elements of a terrorist organization the U.S. would be forced to pursue policies that come into direct conflict with American core values.** This paper aims to identify a number of the actual policy choices the U.S. must consider in order to deter the elements that comprise a terrorist organization and assess the compatibility of those choices with democratic values.

Warrant: The United States cannot instill fear that they can harm terrorists

Fisher, Uri. "Deterrence, Terrorism, and American Values." Homeland Security Affairs 3, Article 4 (February 2007). https://www.hsaj.org/articles/152

Most examinations of deterrence and U.S. counterterrorism policy make the common argument that the U.S. will have to communicate a clear message of punishment

against terrorist elements, without actually considering toward whom and where these threats should be directed. Moreover, in those instances where authors consider targets of retaliation, potential threats of punishment rarely strike at what terrorists truly hold dear. Frequently, policy recommendations represent little more than establishing obstacles to terrorist networks, not meaningful attempts to change the decision-calculus of terrorist elements. The targets the U.S. will be forced to retaliate against and the manner in which these targets will have to be engaged may render the moral price of establishing a real deterrent mechanism too high. **Deterrence is impossible against terrorists, not because it is theoretically inapplicable, but because the U.S. is too concerned with maintaining its moral authority in the world. The aspiration of the U.S. to take the "moral high road" will signal to terrorists that the things they value most are actually not in grave danger. When attempting to deter terrorists the "ethical and necessary" ultimately will collide.**

Analysis: This is a good response because even if conventional deterrence arguments may be true in cyber warfare for state actors, it does not apply to non-state actors like terrorists. This is critical because it means that the link chain of the pro's argument falls apart. This makes it very easy to win the debate because without a link, the pro has no impact.

Answer: Terrorists can elude our strategies

Warrant: Cyber terrorists are increasingly difficult to investigate

Christopher Wray. "Keeping America Secure in the New Age of Terror." Federal Bureau of Investigation, 30 Nov. 2017, https://www.fbi.gov/news/testimony/keeping-america-secure-in-the-new-age-of-terror.

Cyber threats are not only increasing in scope and scale, they are also becoming increasingly difficult to investigate. Cyber criminals often operate through online

forums, selling illicit goods and services, including tools that can be used to facilitate cyber attacks. These criminals have also increased the sophistication of their schemes, which are more difficult to detect and more resilient. Additionally, many cyber actors are based abroad or obfuscate their identities by using foreign infrastructure, making coordination with international law enforcement partners essential. The FBI is engaged in a myriad of efforts to combat cyber threats, from improving threat identification and information sharing inside and outside of government, to developing and retaining new talent, to examining the way we operate to disrupt and defeat these threats. We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Warrant: The US offensive tactics alone are insufficient

Symantec Writer. How Do Cybercriminals Get Caught? 2019, https://us.norton.com/internetsecurity-emerging-threats-how-do-cybercriminals-get-caught.html.

On the surface, cybercrime seems like it would be a fairly open and shut case-a cybercriminal commits a crime, law enforcement steps in, catches the bad guy and then the is case closed. **However, due to the sophisticated tactics these criminals use, it makes it extremely difficult for law enforcement alone to collect evidence, capture the suspect and prosecute them. It Takes a Village To Catch A Cybercriminal Since the method of how they commit these crimes is so complicated, law enforcement usually has to coordinate with government agencies, international partners, and private corporations.** Oftentimes, cybercriminals use secure software to remain anonymous which are proxy servers that hide their location and route their communications through multiple countries in order to evade direct detection, and commit the crimes in other countries where they cannot be prosecuted. In addition to these partnerships,

they use a combination of traditional investigative and complicated digital forensics tactics.

Analysis: This is a good response because it indicates that the pro's tactic of using offensive cyber operations is insufficient to stop cyber terrorism. Cyber terrorists are hard to track and thus hard to attack, and also this means that even if offensive operations could help us gather information, it would be impossible to act upon this information without aid from other countries. This is crucial because it adds another condition the pro needs to meet to access their impact, which is that the US would be able to cooperate with other actors.

PRO: Offensive cyber operation stop attacks on US power grids

Argument: Signaling the US's willingness to attack offensively will deter other countries from attacking our power grids with cyber attacks of their own.

Warrant: Attacks have already been made on our power grid

Ranosa, Ted. "First-Of-Its-Kind Cyberattack Hits US Power Grid: Report." Tech Times, 8 Sept. 2019, https://www.techtimes.com/articles/245271/20190908/first-of-its-kind-cyberattack-hits-us-power-grid-report.htm.

Cyberterrorists reportedly launched an attack on the U.S. power grid, creating vulnerabilities in its control center and several power-generation sites across the country. The North American Electric Reliability Corporation or NERC revealed on Thursday that the U.S. grid suffered an unprecedented cyberattack this spring, though it did cause any blackouts in affected areas in the western United States. In its "Lesson Learned" report, the NERC said the March 5 attack caused signal outages at the grid's "low-impact" control center, but they did not last longer than five minutes. The energy watchdog presented its findings to the Department of Energy on what it considers the first disruptive "cyber event" to have victimized the U.S. power grid. **The cyberattack on the U.S. grid shows just how vulnerable power utilities in the country are, as they become more reliant to digitalization and interconnectivity, according to energy news website E&E News.** The NERC itself urged organizations to use "as few internet-facing devices as possible" to avoid becoming exposed to hackers.

Warrant: Trump is increasing offensive attacks to show willingness to strike back

Liptak, Andrew. "US Cyber Command Has Reportedly Been Aggressively Targeting Russia's Electrical Grid." The Verge, 15 June 2019, https://www.theverge.com/2019/6/15/18680445/us-cyber-command-russian-electrical-grid-cyberattack-deterrent-report.

The newly-revealed actions parallel those that Cyber Command undertook in November 2018 to take down state-linked troll operations like the Internet Research Agency before the midterm elections. **Those operations reportedly took the group offline and unable to access the internet, and it was one of the most aggressive actions made public after the Department of Defense authorized the Command to make more offensive campaigns in June. The efforts appear to be part of a move by the Trump Administration deter potential attacks by demonstrating that the US is willing to delivering a cyber attack.** At a conference earlier this week, National Security Advisor John Bolton said that the US made the response against election meddling their "highest priority last year," and that they were ready to impose heavy costs on anyone who tried until they "[got] the point."

Warrant: Offensive cyber attacks deter malicious attacks on the US

Sanger, David E., and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." The New York Times, 15 June 2019. NYTimes.com, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

But the action inside the Russian electric grid appears to have been conducted under little-noticed new legal authorities, slipped into the military authorization bill passed by Congress last summer. **The measure approved the routine conduct of "clandestine military activity" in cyberspace, to "deter, safeguard or defend against attacks or malicious cyberactivities against the United States."** Under the law, those actions can now be authorized by the defense secretary without special presidential approval. **"It**

has gotten far, far more aggressive over the past year," one senior intelligence official said, speaking on the condition of anonymity but declining to discuss any specific classified programs. "We are doing things at a scale that we never contemplated a few years ago." The critical question — impossible to know without access to the classified details of the operation — is how deep into the Russian grid the United States has bored. Only then will it be clear whether it would be possible to plunge Russia into darkness or cripple its military — a question that may not be answerable until the code is activated.

Impact: Attacks on the power grid could stop medical services from being delivered

Christofaro, Beatrise. How the US Would Struggle If Hit by Massive Cyberattack - Business Insider. 23 May 2019, https://www.businessinsider.com/cyber-attack-us-struggle-taken-offline-power-grid-2019-4.

It forced Taiwan Semiconductor Manufacturing Co., the world's biggest contract chipmaker, to shut down production for three days. In the UK, 200,000 computers used by the National Health System were compromised, halting medical treatment and costing nearly $120 million. The US government said North Korean hackers were behind the ransomware. North Korean hackers were also blamed for the 2015 attack that leaked personal information from thousands of Sony employees to prevent the release of "The Dictator," a fictional comedy about Kim Jong Un. These isolated events were middling to major news events when they happened. But they occur against a backdrop of lesser activity that rarely makes the news. The reason we don't hear about more attacks like this isn't because nobody is trying — governments regularly tell us they are fending off constant attacks from adversaries.

Analysis: This is a good argument because the impact is very far reaching and thus easy to weigh. If an adversary is able to make a significant dent in the US's power grid, this could not only harm our economy but also make it difficult to do things like provide medical services to people who need it.

A/2: Offensive cyber operations stop attacks on US power grids

Answer: Offensive cyber operations will create a cyber war

Warrant: US offensive operations have created unprecedented tit for tat

Cheravitch, Joe. "Cyber Threats from the US and Russia Are Now Focusing on Civilian Infrastructure." TechCrunch, 22 July 2019, http://social.techcrunch.com/2019/07/22/cyber-threats-from-the-u-s-and-russia-are-now-focusing-on-civilian-infrastructure/.

The report drew skepticism from some experts and a denial from the administration, but the revelation led Moscow to warn that such activity presented a "direct challenge" that demanded a response. WIRED magazine the same day published an article detailing growing cyber-reconnaissance on U.S. grids by sophisticated malware emanating from a Russian research institution, the same malware that abruptly halted operations at a Saudi Arabian oil refinery in 2017 during what WIRED called "one of the most reckless cyberattacks in history." **Although both sides have been targeting each other's infrastructure since at least 2012, according to the Times article, the aggression and scope of these operations now seems unprecedented.** Washington and Moscow share several similarities related to cyber-deterrence. **Both, for instance, view the other as a highly capable adversary.** U.S. officials fret about Moscow's ability to wield its authoritarian power to corral Russian academia, the private sector, and criminal networks to boost its cyber-capacity while insulating state-backed hackers from direct attribution.

Warrant: The US has more to lose

Greenberg, Andy. “How Not To Prevent a Cyberwar With Russia.” Wired, June 2019. www.wired.com, https://www.wired.com/story/russia-cyberwar-escalation-power-grid/.

Bossert points out that in many respects the US economy and infrastructure is far more reliant on digitization and automation than Russia's, giving the Kremlin an inherent advantage in any future no-holds-barred cyberwar. He paraphrases former secretary of defense Ash Carter: "**If you're doused in gasoline, don't start a match-throwing contest.”** Bossert didn't confirm or deny the facts of the Times' grid-hacking report, but criticized current Trump officials for not doing enough to deter cyberattacks from adversaries like Russia with other, more traditional means, such as diplomacy or economic incentives and punishments. While the Trump administration imposed new sanctions on Russia for grid-hacking and its unprecedented NotPetya cyberattack during Bossert's term, it's not clear what if any similar measures the White House or State Department has pursued since. **"I do not think they’re sufficiently thinking through our other levers of national power, to explain what’s unacceptable and then to start threatening or imposing consequences or inducements—carrots or sticks—to change [Russia's] behavior."** says Bossert, who has since taken a position at an as yet unnamed cybersecurity startup. "I don’t mind escalatory bravado to some degree. But I’d be furious if that’s all we did."

Analysis: This is a good argument because it turns the pro’s argument and makes it a reason to vote for the con. Even if it is likely that an enemy of the US may attack US electrical grids, it still hasn’t happened yet to an extreme degree. If we get into a cyber war, we can guarantee harms will occur at a very large scale.

Answer: Offensive operations make our enemies more retaliatory

Warrant: Offensive operations make adversaries scared and worried

Slayton, Rebecca. "Why Cyber Operations Do Not Always Favor the Offense." Belfer Center for Science and International Affairs, Feb. 2017, https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense.

Organizational skill can shift the costliness of cyber operations toward the defense. Further, whereas breaching information systems is easy and can be done at relatively low cost, achieving physical effects is far more difficult and costly. **Meanwhile, the benefits of cyber operations are highly situational and subjective. Thus, claims that all of cyberspace is offense dominant obscure crucial differences between distinctive kinds of operations and the ways they are valued; such claims should be avoided**. It only makes sense to discuss the offense-defense balance of specific cyber operations with specific goals, between specific adversaries with distinctive capabilities. **Prioritizing offensive operations can increase adversaries' fears, suspicions, and readiness to take offensive action.**

Warrant: Offensive operations reveal our weaknesses

Slayton, Rebecca. "Why Cyber Operations Do Not Always Favor the Offense." Belfer Center for Science and International Affairs, Feb. 2017, https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense.

Cyber offenses include cyber exploitation (intelligence gathering) and cyberattack (disrupting, destroying, or subverting an adversary's computer systems). An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, not technical operation. The difficulty of distinguishing

between offensive and defensive tactics makes mistrustful adversaries more reactive, and repeatedly conducting offensive cyber operations only increases distrust. **A focus on offensive operations can also increase vulnerabilities; for example, secretly stockpiling information about vulnerabilities in computers for later exploitation, rather than publicizing and helping civil society to mitigate those vulnerabilities, leaves critical infrastructure vulnerable to attack.**The skills and organizational capabilities for offense and defense are very similar.

Analysis: This is a good response because the pro's argument is trying to prove that cyber operations will stop future attacks. This response proves that actually the opposite occurs. Offensive operations will make our adversaries weary of our ability to attack them and thus will encourage offensive attacks against us for the same reasons we are attacking them.

PRO: Offensive cyber operations reduce military action

Argument: Offensive cyber operations allow us to act against adversaries and protect our nation without using conventional military action.

Warrant: Trump is escalating offensive cyber tactics

Ken, Dilanian. “Under Trump, U.S. Ramps up Cyber Offense against Other Countries.” NBC News, 23 June 2019, https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281.

Empowered with new legal authority from both Congress and President Donald Trump, the military's elite cyber force has conducted more operations in the first two years of the Trump administration than it did in eight years under Obama, officials say — including against Russia, despite Trump's well-documented affinity for Vladimir Putin. The general in charge of the push, Paul Nakasone, has spoken about the new policy in cryptic terms such as **"persistent engagement," and "defending forward,"** without explaining what that means. Multiple current and former American officials briefed on the matter say military hackers are breaking into foreign networks, striking at enemy hackers and planting cyber bombs that would disable infrastructure in the event of a conflict. The officials declined to confirm or deny a New York Times report that an element of these classified operations included hacking into Russia's power grid, but they said that such a move would be a standard response to similar behavior by Russia and China. U.S. officials have said that those countries have for years planted malware that could turn out the lights in parts of the U.S.

Warrant: the US is using cyber warfare in response to physical warfare

Sussman, Bruce. Cyber War vs. Traditional War: The Difference Is Fading. 24 June 2019, https://www.secureworldexpo.com/industry-news/cyber-war-vs-traditional-war.

Shooting this drone down, a physical act, was expected by many to lead to a physical military response by the United States. Instead, President Trump told the world that he had called off a physical military response shortly before it was to happen and he would increase sanctions, instead. What he did not tell the world is what The Washington Post revealed two days later. The President gave U.S. Cyber Command the green light to launch a cyber attack against Iran, and the U.S. hit Iranian computer systems that control missile and rocket launches. **In other words, an act of physical warfare (shooting down the drone) led to an act of cyber warfare (a cyber attack) in response. During 2018, the U.S. dramatically shifted the way it talks about cyber warfare and cyber attacks.** We were there as former Secretary of Homeland Security Kirstjen Nielsen issued a warning at an annual cybersecurity conference:

Warrant: Cyber warfare could make conventional tactics obsolete

Mary O'Neill. "Cyber Warfare: The New Front | Bush Center." Cyber Warfare: The New Front | Bush Center, 2017, http://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html.

As history has shown, military strategy must adapt to new domains. **Cyber space is that next domain.** While traditional warfare will continue to exist, technology and cyber operations will aid its methods. **Cyber warfare could make conventional warfare systems that employ computers and electronics operationally ineffective or obsolete. A traditional system that cannot respond in "digital time" to a multi-pronged threat or that cannot provide protection while attacking others may be of little use in the future.** It would be the equivalent of the Polish Army attempting to use their horse

cavalry team against the German armored brigades at the beginning of World War II. Society and warfare have evolved from horses against metal to metal against the matrix.

Impact: Cyber warfare costs fewer lives than traditional warfare

Maurer, Tim. "The Case for Cyberwarfare." Foreign Policy, 19 Oct. 2011, https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/.

According to an intriguing story in this week's New York Times, the Obama administration decided not to use cyberwarfare against Libya, opting instead for a conventional attack on Muammar al-Qaddafi's defense installations. Officials feared that it would set a precedent and invite other countries (think: China, Russia) to use similar means of attack in the future. As James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, succinctly put it, "We don't want to be the ones who break the glass on this new kind of warfare." **Senior officials such as Secretary of Defense Leon Panetta warn that the "next Pearl Harbor we confront could very well be a cyber attack." But what if cyberwarfare is not such a bad thing after all, though? What if it saves lives? The evidence so far actually suggests that cyberwarfare costs fewer lives compared with traditional types of warfare**.

Analysis: This is a good argument because while all the other impacts in the round may be bigger in magnitude, this is likely to outweigh on probability. The odds that Russia or China was ever planning to launch a major cyber attack on the US or that they will now because of offensive operations are very low because it would hurt their international legitimacy a lot. However, shifting away from conventional military tactics provides a surefire way to save lives.

A/2: Offensive cyber operations reduce military action

Answer: Cyber warfare is not less dangerous than conventional war

Warrant: Cyber warfare can cause damage to infrastructure like conventional war

Christofaro, Beatrice. "Cyberattacks Are the Newest Frontier of War and Can Strike Harder than a Natural Disaster. Here's Why the US Could Struggle to Cope If It Got Hit." Business Insider, 23 May 2019, https://www.businessinsider.com/cyber-attack-us-struggle-taken-offline-power-grid-2019-4.

The lights are out, there is no running water, you have no phone signal, no internet, no heating or air conditioning. Food starts rotting in your fridge, hospitals struggle to save their patients, trains and planes are stuck. There are none of the collapsed buildings or torn-up trees that accompany a hurricane, and no floodwater. But, all the same, the world you take for granted has collapsed. **This is what it would look like if hackers decided to take your country offline.** Business Insider has researched the state of cyberwarfare, and spoken with experts in cyberdefense, to piece together what a large-scale attack on a country like the US could look like. **Nowadays nations have the ability to cause warlike damage to their enemy's vital infrastructure without launching a military strike, helped along by both new offensive technology and the inexorable drive to connect more and more systems to the internet.**

Warrant: Cyber warfare can be worse than a nuclear weapon

Hauser, Kristin. "Scientist: Major Cyberattack Could Be as Bad as Nuclear War." Futurism, 20 Aug. 2019, https://futurism.com/the-byte/major-cyberattack-nuclear-war.

We already know what kind of damage a nuclear weapon attack can do — and according to a computer science expert, a cyberattack could now be just as devastating. "As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact… could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon," Jeremy Straub, an assistant professor of computer science at North Dakota State University, wrote in a newly published post in The Conversation. **In the post, Straub cites numerous examples of hackers targeting water treatment plants, power grids, and even nuclear facilities as examples of the form a nuclear weapon-level cyberattack might take**.

Analysis: This is a good response because it takes out the underlying premise that the argument relies upon, which is that cyber warfare is less deadly than conventional warfare. In fact, this is not true because cyber attacks can be just as damning if not more damning than conventional warfare. This means that the impact is either mitigated or turned for the negative.

Answer: Cyber warfare has less mutually assured destruction than conventional warfare

Warrant: Cyber weapons are cheap and easy to attain

Halpern, Sue. How Cyber Weapons Are Changing the Landscape of Modern Warfare. July 2019. www.newyorker.com, https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.

The cyberattack was done below the level of war. It did not harm civilians. It was an off-ramp to war." But Zegart cautioned, "What most people don't think about, and what the national-security people are really alarmed by, is that we could stumble into a war that neither side wants because of the feeling that you have to retaliate." She added, "We don't understand escalation in cyberspace." **In the past, the threat of mutually assured destruction was the way that nuclear powers kept one another's lethal capabilities in check. Cyber weapons may offer some of the same assurances, but only to a point. Unlike nuclear weapons, which are expensive and stockpiled by a small number of states, cyber weapons are cheap and widely available, not just to nation-states but to criminals and malign actors. (According to a new study from the University of Maryland, American computers are attacked every thirty-nine seconds.)**

Warrant: Cyber weapons are harder to trace

Halpern, Sue. How Cyber Weapons Are Changing the Landscape of Modern Warfare. July 2019. www.newyorker.com, https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.

And unlike conventional weapons, whose trajectories are easily traced, cyber weapons, which move through fibre-optic cables that crisscross the globe, lend themselves to plausible deniability. How do you levy a threat when it's not clear where an attack is coming from or who is responsible? The impact of a cyber attack can prove similarly elusive. As Lin, the scholar of cyber policy and security at Stanford, pointed out, "we don't know what it means that we took the Iranian cruise missiles and its command and control systems down. **Maybe it means we took them offline for a few days. Maybe it was more serious. We just don't know."** We do know that on July 11th, three weeks after the cyberattack, three Iranian boats tried to block a British tanker carrying oil through the Strait of Hormuz. In the weeks since the American

cyberattack, the U.S. has imposed further economic sanctions, and Iranian hackers have continued their assault on American businesses.

Analysis: This is a good response because the underlying weighing behind why a big cyber attack is unlikely is that there is mutually assured destruction. However, this response says that MAD is rendered ineffective in an arena of war dominated by cyber tactics, thus taking out the weighing. This makes retaliation arguments on the con much easier to weigh.

PRO: Offensive cyber operations deter cyber attacks on the US

Argument: If the US shows that it is willing to launch offensive cyber attacks against other countries, they will fear retaliation if they attack us and thus never attack to begin with.

Warrant: Current offensive operations are meant to deter attacks from adversaries

Ellen, Nakashima. "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries." Washington Post, 20 Sept. 2019, https%3A%2F%2Fwww.washingtonpost.com%2Fworld%2Fnational-security%2Ftrump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says%2F2018%2F09%2F20%2Fb5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

The Trump administration is focused on foreign governments' attempts to target U.S. networks and interfere in November's election. The strategy incorporates a new classified presidential directive that replaced one from the Obama administration, Bolton said. **It allows the military and other agencies to undertake cyber operations intended to protect their systems and the nation's critical networks**. **Bolton's remarks are consistent with the Trump administration's posture toward cyber deterrence, which is considered to be more aggressive in comparison to former administrations' positions. He cast the latest move as part of an effort to "create structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear."**

Warrant: Offensive operations let adversaries know we can strike back

Lopez, Todd. “Deterrence in Cyberspace Requires Multifaceted Approach.” U.S. DEPARTMENT OF DEFENSE, 11 Sept. 2019, https://www.defense.gov/explore/story/Article/1957874/deterrence-in-cyberspace-requires-multifaceted-approach/.

Deterrence also includes letting adversaries know the United States has the ability to strike back, Wilson told lawmakers. "We look very hard at the ability, if called upon, to deliver consequences, not just kinetically or in all the other domains of operations the department has, but also in the domain of cyberspace," he said. Congressional involvement has enhanced the department's ability to deter, specifically with clarity on the authorities DOD has to act when needed, Wilson said. **Additionally, National Security Presidential Memorandum 13 also focuses on the decision process for either offensive or defensive cyber-effects operations, he said.**

Warrant: Cyber attacks allow us to threaten other countries without putting lives at risk

Ellen, Nakashima. “White House Authorizes ‘Offensive Cyber Operations’ to Deter Foreign Adversaries.” Washington Post, 20 Sept. 2019, https%3A%2F%2Fwww.washingtonpost.com%2Fworld%2Fnational-security%2Ftrump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says%2F2018%2F09%2F20%2Fb5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

In general, the president’s directive — called National Security Presidential Memorandum 13, or NSPM 13 — frees the military to engage, without a lengthy approval process, in actions that fall below the “use of force” or a level that would cause death, destruction or significant economic impacts, said individuals familiar with the policy who spoke on the condition of anonymity to discuss nonpublic information. “As a policy matter, Bolton’s remarks likely mean the administration is willing to take

more risks than previous administrations, but the proof will be in the results," said Michael Daniel, who was cyber coordinator for the Obama Administration.

Impact: A cyber attack on the US could cause destruction on par with a nuclear attack

Straub, Jeremy. "A Cyberattack Could Wreak Destruction Comparable to a Nuclear Weapon." Public Radio International, 16 Aug. 2019, https://www.pri.org/stories/2019-08-16/cyberattack-could-wreak-destruction-comparable-nuclear-weapon.

With the US and Russia pulling out of a key nuclear weapons pact — and beginning to develop new nuclear weapons – plus Iran tensions and North Korea again test-launching missiles, the global threat to civilization is high. Some fear a new nuclear arms race. **That threat is serious — but another could be as serious, and is less visible to the public**. So far, most of the well-known hacking incidents, even those with foreign government backing, have done little more than steal data. Unfortunately, there are signs that hackers have placed malicious software inside US power and water systems, where it's lying in wait, ready to be triggered. The US military has also reportedly penetrated the computers that control Russian electrical systems. Many intrusions already **As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.**

Analysis: This is a good argument because it provides an easy link into all the other arguments in the round. Since all con arguments will likely have something to do with other countries attacking the US with cyber warfare in some way or another, this argument turns or at least mitigates all of those impacts by proving that all types of cyber warfare will go down when the US shows its power to act offensively.

A/2: Offensive cyber operations deter cyber attacks on the US

Answer: Offensive cyber operations can bring unpredictable consequences

Warrant: Using offensive cyber operations once encourages officials to just keep going

Groll, Elias. "The U.S.-Iran Standoff Is Militarizing Cyberspace." Foreign Policy, 27 Sept. 2019, https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/.

Ahead of the 2018 midterm elections, Cyber Command knocked the main Russian troll operation offline. A joint task force set up to target the Islamic State is continuing to go after the group online after it was largely militarily defeated in Iraq and Syria. **And earlier this summer, after Trump scotched plans for a military strike, American hackers struck Iranian computer systems instead.** Like drone strikes, which became an integral part of the U.S. arsenal a little over a decade ago, cyberweapons seemingly offer a standoffish, bloodless way to target enemies—with the risk that they become an automatic fallback, not just for the United States, but for everyone else as well. **"It's increasingly part of the arsenal that states are using against each other," said Sergio Caltagirone, the vice president of threat intelligence at the industrial cybersecurity firm Dragos. "The issue in the long term is that the United States using cyber consistently leads to the idea that it can be used any time."**

Warrant: Offensive operations can create far reaching consequences that are hard to predict

Groll, Elias. "The U.S.-Iran Standoff Is Militarizing Cyberspace." Foreign Policy, 27 Sept. 2019, https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/.

> **The growing use of cyberweapons has a host of unpredictable consequences. Caltagirone, a former senior intelligence analyst at the NSA, likens it to prying open Pandora's box a bit further with each attack. The consequences of breaking into a computer system or launching a cyberattack can be highly unpredictable. When Russian intelligence unleashed the NotPetya ransomware in Ukraine in 2017, for example, it probably did not expect that it would eventually shut down the Danish shipping giant Maersk and even British hospitals. The United States is no stranger to the unexpected consequences of digital weapons, either.** Its landmark cyberattack on Iran's nuclear infrastructure was only discovered in 2010 after the Stuxnet malware spread to other computer systems that it never intended to target. Indeed, Stuxnet was a pioneering weapon in the history of cyberwarfare, illustrating the possibilities of digital weapons to covertly attack key targets—and to use cyberweapons to cause physical havoc in the real world.

Analysis: This is a good response because it means that even if offensive operations are successful in deterring future attacks upon the US, it can create unintended harmful externalities that outweigh the benefits of deterring future attacks. The magnitude of this impact is also very weighable because it is so hard to predict, which means that it could be infinitely large.

Answer: Cyber attacks could increase retaliation against the US

Warrant: Offensive cyber attacks encourage countries to increase their cyber arsenals

Guest Blogger for Net Politics. "Global Consequences of Escalating U.S.-Russia Cyber Conflict." Council on Foreign Relations, 2 Apr. 2019, https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict.

The number of potential cyber conflict participants continues to increase, with dozens of countries globally building military cyber capabilities. In conventional military operations, armed forces in close proximity are often at an increased risk of escalatory events, like Russian involvement in Eastern Ukraine or the recent events on the Indian and Pakistani border. The concept of borders and distance does not really exist in cyberspace; dozens of armed forces are constantly within the virtual arm's length, creating a constant possibility of interaction and escalation. Additionally, despite the meticulous preparation and execution of cyber operations, the situation can quickly spin out of control in a manner difficult to predict. The further militarization of the internet might lead to an increased escalation risk. While today's cyber tug-of-war happens well below the threshold of armed conflict, engaging in discussions about norms at the UN within the First Committee and the Group of Government Expert process, adopting the restraint-inducing principles enshrined by international humanitarian law and increasing the doctrinal transparency are absolutely necessary going forward.

Warrant: Peace is unviable because cyber space is unpredictable

Chachak, Elias. "Is the Threat of Escalation Viable Cyber Deterrence?" CyberDB, 12 July 2018, https://www.cyberdb.co/threat-escalation-viable-cyber-deterrence/.

The question that governments ask is how to deter hostile acts in cyberspace? And while an important question to raise, perhaps the reality is that there is no viable answer. There is a reason why international efforts continually fail when trying to gain consensus on cyber norms, **Internet governance, and the legalities and criteria of hacking back – there is lack of a fundamental desire to actually find a solution. Governments willing to agree to the standards and principles of any of these issues are stating their willingness to abide by them, and while that may fit the current**

situation, the dynamism of cyberspace has proven unpredictable. Being cuffed to such an agreement that no longer has relevance while other governments operate without constraints is not an ideal situation. Therefore, without an agreement in place, the status quo remains.

Analysis: This is a good response because it turns the argument and makes it a reason to vote for the con. Even if the pro can prove that offensive cyber attacks make the US seem scarier and stronger in terms of its cyber capabilities, this does not necessarily mean that other countries will back down as a result. Instead, they might increase their cyber power and offensive operations to protect themselves from an increasingly aggressive US.

PRO: Offensive cyber operations can stop economic attacks

Argument: With offensive cyber attacks, the US is able to find out crucial intelligence information otherwise unavailable.

Warrant: Russia and China could both potentially launch cyber attacks that hurt our economy

Ranger, Steve. "Cyberattacks: China and Russia Can Disrupt US Power Networks Warns Intelligence Report." ZDNet, https://www.zdnet.com/article/cyber-attacks-china-and-russia-can-disrupt-us-power-networks-warns-intelligence-report/. Accessed 4 Oct. 2019.

Both China and Russia now have the capabilities to launch cyberattacks that could at least temporarily disrupt US critical infrastructure such as gas pipelines or power networks, according to intelligence officials. The Worldwide Threat Assessment of the US Intelligence Community is a document published each year, which itemises the significant threats to the US and its allies. **It said that currently China and Russia pose the greatest espionage and cyberattack threats to the US but also warned that other adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence US policies. It warned that rivals to the US have experimented with growing capabilities to "shape and alter the information and systems" that the country relies on.** "As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information," the document said.

Warrant: The US has started offensive cyber operations to prevent economic interference

Vavra, Shannon. "U.S. Ramping up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says." CyberScoop, 11 June 2019, https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/.

"We're now looking at — beyond the electoral context — a whole range of other activities to prevent this other kind of cyber interference … in the economic space, as well," Bolton said while speaking at The Wall Street Journal's CFO Network annual meeting. **The U.S. faces many digital economic threats, including a particularly aggressive salvo from Beijing**, **which continues to steal intellectual property and conduct other cyber-espionage activities**, according to the latest Pentagon assessment on Chinese military operations. **The U.S. government traditionally has carried out offensive cyber-operations in the electoral context, such as a 2018 Cyber Command operation that interrupted the internet access of a Russian organization that spread political disinformation on social media. Now, according to Bolton, American focus is expanding to deter the theft of IP.**

Warrant: Offensive cyber attacks signal the US's cyber strength

Ken, Dilanian. "Under Trump, U.S. Ramps up Cyber Offense against Other Countries." NBC News, 23 June 2019, https://www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281.

The new approach was empowered by language Congress inserted last year in a defense bill, which provided new authorities for offensive military cyber operations. Last August, Trump last year signed a classified order known as National Security Presidential Memorandum 13, which officials say authorized Cyber Command to take action abroad without specific presidential approval. "Between strategy, policy and authorities there has been a tremendous change over the past 18 months," Nakasone

said in April. The army general made clear that the offensive hacking is being done "below the level of armed conflict." **He frequently draws an analogy to other branches of the military. "Our air force doesn't stay in hangars on the ground and never take off and fly in the air," he said. "They're flying every single day. They're flying missions to provide us warning…they provide a show of force sometimes. Its's the same concept in cyber space…We don't wait for something to happen to us."**

Impact: Cyber attacks cost the economy billions of dollars

US Federal Government (CEA). The Cost of Malicious Cyber Activity to the U.S. Economy. Feb. 2018. https://www.hsdl.org › view

Using the information provided in this document, as well as estimates from Ponemon (2017) on the probability of a material data breach, we estimate that malicious cyber activity costs the U.S. economy between $57 billion and $109 billion in 2016, which represents between 0.31 percent and 0.58 percent of that year's GDP (please the Computational Appendix for the details). For comparison, based on an extrapolation exercise that used a variety of datasets on adverse cyber events from several countries, the Center for Strategic and International Studies (2014) estimates that the cost of malicious cyber activity directed at U.S. entities was $107 billion in 2013, which represented 0.64 percent of GDP

Analysis: This is a good argument because the impact is very easy to weigh. With one cyber attack, Russia or China could potentially deliver an irrevocable amount of damage on the US economy, pushing millions of people into poverty. This is an impact that is almost certainly going to be the biggest in the round given the number of people potentially affected and the severely high magnitude to which they are hurt.

A/2: Offensive cyber operations can stop economic attacks

Answer: Offensive cyber attacks could backfire

Warrant: The US would lose in a cyber war

Greenberg, Andy. “How Not To Prevent a Cyberwar With Russia.” Wired, June 2019. www.wired.com, https://www.wired.com/story/russia-cyberwar-escalation-power-grid/.

But former White House cybersecurity officials caution against that cyberwar hawkishness. **"The idea that we can use cyber offense capabilities to impose sabotage-like effects, and to do so in increasingly large scale and costly ways until they get it through their head that they can’t win, I don’t think that's going to work," says Tom Bossert, who served as White House homeland security advisor and the president's most senior cybersecurity-focused official until April of last year. "I want to make sure we don’t end up in an escalatory cyber exchange where we lose more than they do.” Bossert points out that in many respects the US economy and infrastructure is far more reliant on digitization and automation than Russia's, giving the Kremlin an inherent advantage in any future no-holds-barred cyberwar.** He paraphrases former secretary of defense Ash Carter: "If you're doused in gasoline, don't start a match-throwing contest."

Warrant: Russia might retaliate on a previously unseen scale

Guest Blogger for Net Politics. “Global Consequences of Escalating U.S.-Russia Cyber Conflict.” Council on Foreign Relations, 2 Apr. 2019,

https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict.

Domestically, Russia is currently already in the process of isolating its networks from the outside internet. Russia's official justification for the action is to lower the risk of external cyberattacks; however, in reality the goal is to increase control over the networks, including strict traffic filtering, reminiscent of the China's Great Firewall. **While Russia's narrative rings hollow, U.S. reports of cyberattacks on Russia may be exploited internally to justify the changes. There is also the danger of a retaliation. While Russia could simply limit its response to a diplomatic message, the standard previously followed by the United States, escalation in response to the November action might follow, potentially on a previously unseen scale**. Intensifying cyber conflict would not only seriously impact national security, but also increase geopolitical risk for businesses. Today, most cyber attacks focus on espionage or data theft. Offensive activity elevated to the disruption of civilian systems - for example, causing utility service interruptions - would result in serious ramifications; the 2017 NotPetya wiper worm served as a pointed demonstration of potential consequences. This issue would be made more severe by the constantly evolving theater.

Analysis: This is a good response because it turns the pro's argument and makes it a reason to vote for the con. If offensive attacks only increase retaliation toward the US, then it is likely they do more harm than good. Even if some attacks are stopped or preempted by offensive operations, this is outweighed by the increase in retaliatory attacks that offensive operations bring with them.

Answer: Offensive operations under Trump are ineffective

Warrant: Trump's offensive cyber attacks only increase escalation

Valeriano, Branden. "The Myth of the Cyber Offense: The Case for Restraint." Cato Institute, 15 Jan. 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.

We demonstrate that, while cyber operations to date have not been escalatory or particularly effective in achieving decisive outcomes, **recent policy changes and strategy pronouncements by the Trump administration increase the risk of escalation while doing nothing to make cyber operations more effective. These changes revolve around a dangerous myth: offense is an effective and easy way to stop rival states from hacking America. New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game.** Cyberspace to date has been a domain of political warfare and coercive diplomacy. An offensively postured cyber policy is dangerous, counterproductive, and undermines norms in cyberspace. Many have promoted the idea of a coming "Cyber Pearl Harbor," but instead the domain is littered with covert operations meant to manage escalation and deter future attacks. Cyber strategy and policy must start from an accurate understanding of the domain, not imagined realities.

Warrant: Offensive cyber attacks under Trump could put innocents at risk

Farrell, Michael B., et al. "Trump Is Rattling Sabers in Cyberspace — but Is the U.S. Ready?" POLITICO, 13 July 2019, https://politi.co/2jJjsVz.

The Trump administration is sending aggressive messages about the United States' willingness to hack its adversaries — alarming lawmakers and experts who fear the president is provoking a global cyberconflict that the U.S. may not be prepared to face. A U.S. cyberattack on Iranian military and intelligence targets last month was one of the most prominent signs of the new approach, which comes after a reported effort to implant hostile computer code in Russia's electrical grid and a temporary takedown

of a notorious Kremlin-backed troll operation last fall. To supporters, the tactics are a sign the U.S. may finally be getting out of its defensive crouch in cyberspace — as advocated by hawks such as national security adviser John Bolton. **But the moves also lay the potential groundwork for a tit for tat of cyberattacks that could inflict significant damage on bystanders. Targets such as banks, hospitals, oil companies and electric utilities in the U.S**. and elsewhere have already proved vulnerable, as seen in recent criminal hacks that paralyzed entities such as Baltimore's city government.

Analysis: This is a good response because even if it is true that offensive cyber attacks could be good in a vacuum or under most circumstances, they have recently taken a turn for the worse. This means that this is likely the trajectory cyber attacks will continue on, which makes the response easy to weigh by saying its impact is more long term than any con argument.

PRO: Offensive cyber operations help stop nuclear proliferation

Argument: The United States can use cyber attacks to prevent adversaries from acquiring nuclear weapons technology.

Warrant: Cyber attacks can be used in a variety of ways to attack enemy governments

Marco Roscini, Cyber Operations as Nuclear Counterproliferation Measures, Journal of Conflict and Security Law, Volume 19, Issue 1, April 2014, Pages 133–157

Cyber operations conducted by States include both cyber attacks and cyber exploitation.11 **Cyber attacks could be standalone operations or be used in conjunction with a subsequent kinetic attack, and could occur in peacetime as well as in time of armed conflict.12 A cyber attack may go from relatively innocuous operations such as website defacement to acts that cause havoc in military campaigns by generating misinformation, or acts resulting in major disruption of services and even physical damage to property, loss of lives and bodily injury.** In all cases, a cyber attack involves an action, either in offence or in defence, delivered in or through cyberspace, that targets either information systems or infrastructure control systems.13 The former contain information but do not operate physical infrastructures, hence an attack on them causes loss, alteration or corruption of data but does not directly result in loss of functionality or material damage. The latter, **of which a common type is Supervisory Control and Data Acquisition (SCADA) systems, operate infrastructures: if corrupted, the consequence may be malfunction or even physical damage.**

Warrant: These tactics could be leveraged against an adversary to stop them from nuclear proliferation

Marco Roscini, Cyber Operations as Nuclear Counterproliferation Measures, Journal of Conflict and Security Law, Volume 19, Issue 1, April 2014, Pages 133–157

Both cyber attacks and cyber exploitation could be employed as counterproliferation tools in alternative to, or together with, more traditional means. **Cyber attacks, for instance, could be used to incapacitate the air defence networks of the proliferator State in support of aerial monitoring of compliance with non-proliferation agreements.19 Cyber attacks could also be used to enable a subsequent kinetic attack for counterproliferation purposes, as in the case of Israel's bombing of a Syrian nuclear facility in 2007,** which was preceded by a cyber attack that neutralized ground radars and anti-aircraft batteries.20 **Finally, States could conduct cyber attacks to directly damage or disrupt the facilities where nuclear weapons are being manufactured or, if the State in question has already acquired nuclear weapons, to attack other infrastructures in order to persuade it to disarm.** Stuxnet was allegedly designed to slow down Iran's nuclear programme by affecting the gas centrifuges at the Natanz uranium enrichment facility.

Warrant: Cyber espionage could give the United States early warning of nuclear proliferation

Marco Roscini, Cyber Operations as Nuclear Counterproliferation Measures, Journal of Conflict and Security Law, Volume 19, Issue 1, April 2014, Pages 133–157

Cyber exploitation could also be used to collect information about the nuclear programme of the suspected proliferator. **The US Foreign Intelligence Surveillance (FISA) Amendments Act of 2008,** for instance**, allows the FISA Court to authorize 'the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information',**28 where 'foreign intelligence' includes

'information that relates to … the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power'

Impact: The Stuxnet cyber attack set Iran back 2 years

Straub, Jeremy. "A Cyberattack Could Wreak Destruction Comparable to a Nuclear Weapon." Public Radio International, 16 Aug. 2019, https://www.pri.org/stories/2019-08-16/cyberattack-could-wreak-destruction-comparable-nuclear-weapon.

The Stuxnet virus, which has attacked Iran's nuclear facilities and which Israel is suspected of creating, has set back the Islamic Republic's nuclear program by two years, a top German computer consultant who was one of the first experts to analyze the program's code told The Jerusalem Post on Tuesday. **"It will take two years for Iran to get back on track," Langer said in a telephone interview from his office in Hamburg, Germany. "This was nearly as effective as a military strike, but even better since there are no fatalities and no full-blown war. From a military perspective, this was a huge success."**

Warrant: Iran would have to start from scratch for much of its program

Katz, Yaakov "Stuxnet set back Iran by two years" December 15, 2010 JPOST. https://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years

According to Langer**, Iran's best move would be to throw out all of the computers that have been infected by the worm, which he said was the most "advanced and aggressive malware in history." But, he said, even once all of the computers were thrown out, Iran would have to ensure that computers used by outside contractors**

were also clean of Stuxnet. "It is extremely difficult to clean up installations from Stuxnet, and we know that Iran is no good in IT [information technology] security, and they are just beginning to learn what this all means," he said. "Just to get their systems running again they have to get rid of the virus, and this will take time, and then they need to replace the equipment, and they have to rebuild the centrifuges at Natanz and possibly buy a new turbine for Bushehr."

Analysis: This argument demonstrates how cyber operations could be useful to achieving a major American foreign policy goal. This point is strong because the threat of Iranian nuclear proliferation carries emotional resonance and will be persuasive to judges.

A/2: Offensive cyber operations help stop nuclear proliferation

Answer: Offensive cyber operations will not stop nuclear proliferation

Warrant: Cyber weapons lead to a dangerous escalation mentality

Groll, Elias. "The U.S.-Iran Standoff Is Militarizing Cyberspace." Foreign Policy, 27 Sept. 2019, https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/.

A joint task force set up to target the Islamic State is continuing to go after the group online after it was largely militarily defeated in Iraq and Syria**.** And earlier this summer, after Trump scotched plans for a military strike, American hackers struck Iranian computer systems instead. **Like drone strikes, which became an integral part of the U.S. arsenal a little over a decade ago, cyberweapons seemingly offer a standoffish, bloodless way to target enemies—with the risk that they become an automatic fallback, not just for the United States, but for everyone else as well.** "It's increasingly part of the arsenal that states are using against each other," said Sergio Caltagirone, the vice president of threat intelligence at the industrial cybersecurity firm Dragos. "**The issue in the long term is that the United States using cyber consistently leads to the idea that it can be used any time."**

Warrant: The consequences of escalation could be extreme

Groll, Elias. "The U.S.-Iran Standoff Is Militarizing Cyberspace." Foreign Policy, 27 Sept. 2019, https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/.

The consequences of breaking into a computer system or launching a cyberattack can be highly unpredictable. When Russian intelligence unleashed the NotPetya ransomware in Ukraine in 2017, for example, it probably did not expect that it would eventually shut down the Danish shipping giant Maersk and even British hospitals. The United States is no stranger to the unexpected consequences of digital weapons, either. Its landmark cyberattack on Iran's nuclear infrastructure was only discovered in 2010 after the Stuxnet malware spread to other computer systems that it never intended to target. Indeed, Stuxnet was a pioneering weapon in the history of cyberwarfare, illustrating the possibilities of digital weapons to covertly attack key targets—and to use cyberweapons to cause physical havoc in the real world. **But U.S. use of cyberweapons has generally been more restrained than that of its adversaries. Unlike Russia, for example, the United States has refrained from using cyberweapons to target civilian infrastructure, at least as far as is publicly known.**

Analysis: This response is good because it shows how so little is known about cyber weapons and there is so much potential for harm. Use this to appeal to your judge's sense of caution and urge them to exercise restraint.

Answer: Cyber attacks could increase retaliation against the US

Warrant: Offensive cyber attacks encourage countries to increase their cyber attacks

Guest Blogger for Net Politics. "Global Consequences of Escalating U.S.-Russia Cyber Conflict." Council on Foreign Relations, 2 Apr. 2019, https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict.

More worryingly, with a more offensive posture, it will be increasingly difficult for states to differentiate between cyber espionage and more damaging degradation

operations. What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, "in the [aggressor] state's own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective." **The new strategy risks producing a "forever cyber war" prone to inadvertent escalation because it implies all cyber operations should be interpreted as escalatory by adversaries**.

Warrant: Peace will become impossible because cyber space is unpredictable

Chachak, Elias. "Is the Threat of Escalation Viable Cyber Deterrence?" CyberDB, 12 July 2018, https://www.cyberdb.co/threat-escalation-viable-cyber-deterrence/.

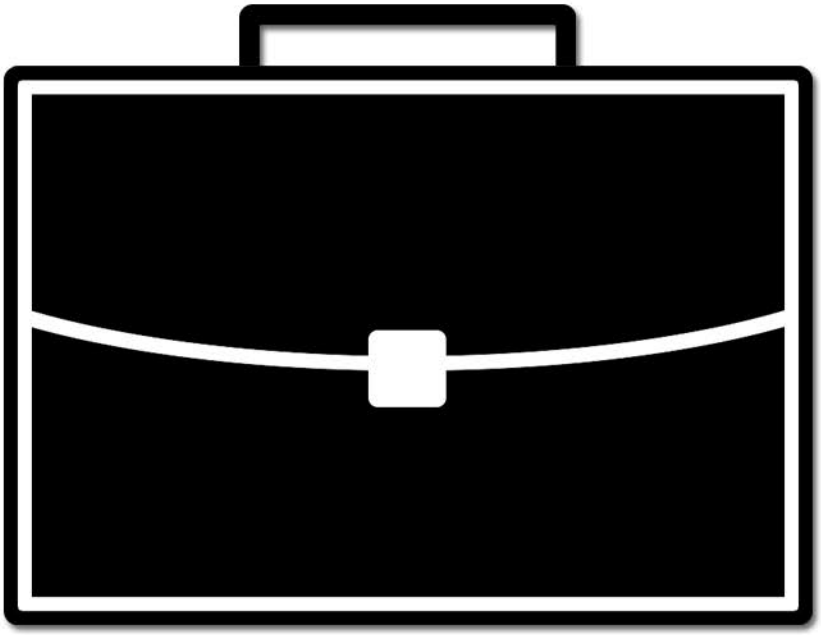
Yet the search for decisive battle is often an elusive, if not dangerous, temptation for military planners and policymakers. **In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that "often, war results in something clouded, neither triumph nor defeat. It is an arena of grey outcomes, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place."**60 Decisive victories in any one battle are rare. Adversaries can refuse to fight.61 They can even signal resolve through demonstrating their ability to endure pain.

Analysis: This argument shows that cyber weapons can create long running intractable conflicts. These conflicts might have lower magnitude than nuclear weapons, but the probability of peace trends towards zero. Nuclear weapons have never been used, while cyber weapons will cause persistent pain.

Champion Briefs

Nov/Dec 2019

Public Forum Brief



Con Arguments with Pro Responses

CON: Offensive operations hurt civilians

Claim: US engaged in cyberattacks on Russia

Klar, Rebecca. "Russia: Reported US cyberattack on power grid possible." The Hill. 6/17/19. https://thehill.com/policy/national-security/448847-russia-reported-us-cyberattack-on-power-grid-possible

The Kremlin on Monday reportedly said it is possible the U.S. put implants into Russian power grids.

The New York Times first reported the U.S. allegedly gearing up for a cyberattack last week, citing unnamed officials describing the types of actions that had been taken toward Russian power grids.

Kremlin spokesman Dmitry Peskov told Reuters, "Undoubtedly this information shows the hypothetical possibility ... all signs of cyber war and military cyber action against the Russian Federation."

The Hill has reached out to the Kremlin for comment.

Peskov told Reuters that Russian authorities are working to keep its economy safe after unnamed strategic parts had endured foreign cyberattacks.

According to the New York Times report, probes in control systems have been in place since at least 2012 but now the strategy is shifting toward offense.

Officials told the Times the U.S. had deployed computer code within Russia's grid to combat Russian disinformation and hacking in 2018 elections.

Warrant: Cyberattacks on Russia could take out grid

Liptak, Andrew. "US Cyber Command has reportedly been aggressively targeting Russia's electrical grid." The Verge. 6/15/19.

https://www.theverge.com/2019/6/15/18680445/us-cyber-command-russian-electrical-grid-cyberattack-deterrent-report

Officials tell the Times that the US has been probing the country's electrical grid since 2012, and that those efforts have stepped up significantly in recent months, sending "potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before."

US officials have spoken about the need to be able to launch a cyberattack against the Russian government if the need arises. The Times says that Cyber Command didn't outline what actions it had specifically undertaken with its newfound authorization. It also notes that the agency can undertake operations with authorization from the Secretary of Defense, without the approval of the President.

The newly-revealed actions parallel those that Cyber Command undertook in November 2018 to take down state-linked troll operations like the Internet Research Agency before the midterm elections. Those operations reportedly took the group offline and unable to access the internet, and it was one of the most aggressive actions made public after the Department of Defense authorized the Command to make more offensive campaigns in June.

The efforts appear to be part of a move by the Trump Administration deter potential attacks by demonstrating that the US is willing to delivering a cyber attack. At a conference earlier this week, National Security Advisor John Bolton said that the US made the response against election meddling their "highest priority last year," and that they were ready to impose heavy costs on anyone who tried until they "[got] the point."

Warrant: Taking out the grid would be devastating

Bogost, Ian. "Revenge of the Power Grid." The Atlantic. 7/15/19. https://www.theatlantic.com/technology/archive/2019/07/manhattan-blackout-reveals-infrastructure-risk/594025/

Failure, fire, and flood aren't the only dangers that can befall transformer substations. Power infrastructure can be an appealing target for terrorism because the sites are poorly protected and the economic impact of a successful attack can be high—particularly in a city like New York. Cyberattacks are also possible. This March, a denial of service attack affected electrical systems in Los Angeles and Salt Lake City, two major population centers. Intelligence suggests that the risk of similar foreign attacks is currently elevated. A House Energy and Commerce subcommittee discussed those risks in a hearing the day before the Midtown Manhattan blackout.

One way to mitigate these dangers is to make utility infrastructure less susceptible to single points of failure. Underground distribution tends to make it easier to reach electrical customers via multiple paths. Regulatory agencies such as the New York State Reliability Council also impose requirements on utility service. Con Edison, which powers almost all of New York City, is expected to design its network to operate even if some of its components fail or are lost to disaster. But new risks associated with climate change, cyberwarfare, and other factors haven't necessarily been accounted for in the design and operation of utility infrastructure.

Impact: Civilian lives are at risk

Plumer, Brad. "It's way too easy to cause a massive blackout in the US." Vox. 4/14/14. https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability

Back in 2012, the National Research Council worried that a well-coordinated attack on the grid "could deny large regions of the country access to bulk system power for weeks or even months. … If such large extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold."

How would that work? It's worth walking through the mechanics of how a truly massive blackout — like the 2003 Northeast blackout that left 50 million people without power — can happen.

Power grids are, by their nature, extremely complex. It's hard to store electricity for any extended period. That means that the output from power plants has to be equal to the use of electricity at all times. Otherwise, power lines can get overloaded or generators underloaded, causing damage to the equipment.

Usually, the grid has protective devices that switch off a piece of equipment if there's a problem. So if, say, a sagging power line hits a tree — causing it to overheat — that line will get disconnected. The problem is that all the other lines now have to carry excess current. If they start overheating and have to switch off, you can get … cascading failures.

So power grid operators have to constantly monitor the system to make sure that power generation and power use are matched up and that a single fault can't cause the entire grid to fail. They're usually very good at this. But it's a difficult task — and if, the grid is already running at capacity or a major piece of equipment falters, it can be hard to prevent "cascading failures." The National Research Council was worried about an attack causing this sort of cascading effect.

Analysis: Cyberattacks on critical infrastructure have already been planned by the United States. The recent cyberattacks on Russia’s electrical grid demonstrate that the U.S is willing to target infrastructure that is essential to survival. Infrastructure is very vulnerable to cyberattacks, and restoring the power is not always an easy task. These attacks on infrastructure can put tens if not thousands of civilian lives at risk, making these cyber operations very costly in terms of human life.

A/2: Offensive operations hurt civilians

Answer: The attack did no damage

"US and Russia clash over power grid hack attacks." BBC. 6/18/19. https://www.bbc.com/news/technology-48675203

In its report the newspaper said American "code" had been deployed inside many elements of Russia's power network.
The Times said this was an escalation of other work the US was doing to combat Russian disinformation and hacking campaigns.
Mr Peskov said President Trump had dismissed the allegations made in the Times, calling them "fake news".
The Kremlin spokesman added: "If one assumes that some government agencies do this without informing the head of state, then of course this may indicate that cyber-war against Russia might be a hypothetical possibility."
He said "vital areas" of Russia's economy were under continuous attack, but it had managed to counter the intrusions so they did no damage.

Answer: The US cant shut down the whole grid

"Russia thwarts U.S. cyber attacks on its infrastructure: new agencies." Reuters. 6/17/19. https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCN1TI1U0

Russia has uncovered and thwarted attempts by the United States to carry out cyber attacks on the control systems of Russian infrastructure, Russian news agencies cited an unnamed security source as saying on Monday.

The disclosure was made on Russia's RIA and TASS news agencies days after the New York Times cited unnamed government sources as saying that the United States had inserted potentially disruptive computer code into Russia's power grid as part of a more aggressive deployment of its cyber tools.

The newspaper suggested President Donald Trump had not been informed of the intrusions. Trump, without providing evidence, said on Twitter that the article was not true.

The Kremlin had said earlier on Monday that the U.S. newspaper report was worrying and showed that a cyber war was, in theory, possible.

"We see and note such attempts," the Russian security source was quoted as saying in response to the report. "However, we manage to neutralize these actions."

Foreign intelligence services have stepped up cyber attacks against Russia in recent years and are targeting mainly transport, banking and energy infrastructure, the source told TASS and RIA.

Answer: Russia would retaliate

Fullmer, Hannah. "DHS and FBI Say Russia Hacked the U.S. Electric Grid." Electrical Contractor. 4/18. https://www.ecmag.com/section/systems/dhs-and-fbi-say-russia-hacked-us-electric-grid

Amid coverage of Russia's involvement in the 2016 presidential election, more news of nefarious Russian cyber activity has come to light. This time, a Russian campaign to infiltrate U.S. power and infrastructure sectors gained access to and observed these organizations for an undetermined amount of time.

In a joint technical alert released on March 15, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) revealed that, since at least March 2016, Russian government hackers attacked U.S. government entities and critical

infrastructure organizations in the energy, nuclear, commercial facilities, water, aviation and manufacturing sectors.

The report does not list the companies attacked. In press releases, they are allowed to remain anonymous so that companies can share and access reports of hacking with others without fear of public knowledge alarming investors or customers.

According to the report, the attacks were not random. To gain access to their victims' networks, hackers employed well-known techniques in multistep attacks, going after smaller companies' networks en route to their primary targets—American power plant computers and networks.

Analysis: Russia acknowledged the United States' intrusion into its electrical grid, but it also noted that it was able to neutralize the U.S' efforts. Russia claims that these attacks did virtually no damage, so it's plausible that the U.S isn't capable of disabling their systems. Furthermore, the U.S knows not to attack Russia's electrical grid, as Russia has already proven that it can hack into the U.S' system as well.

CON: Offensive operations lead to retaliation on U.S grid

Claim: Cyberattacks lead to retaliation

Marks, Joseph. "The Cybersecurity 202: U.S. businesses are preparing for Iranian hacks after American cyberattack." The Washington Post. 6/24/19. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/06/24/the-cybersecurity-202-u-s-businesses-are-preparing-for-iranian-hacks-after-american-cyber-attack/5d1007a81ad2e552a21d507f/

U.S. businesses should get ready for a barrage of digital retaliation from Iran after the Trump administration launched a cyberattack against the Islamic Republic's rocket and missile launching systems, current and former U.S. government officials said this weekend.

Iranian hackers are already targeting U.S. companies with specialized malicious software designed to wipe the contents of their computer networks rather than to simply steal their data, Chris Krebs, director of the Homeland Security Department's cybersecurity division, warned in a Saturday email.

And cybersecurity companies — which were already clocking a dramatic increase in Iranian hacking during the past few weeks — began warning this weekend that the nation could increase its attacks and make them far more destructive.

Warrant: The US Grid is very vulnerable

"A Cyberattack on the U.S. Power Grid." Council on Foreign Relations." 4/3/17. https://www.cfr.org/report/cyberattack-us-power-grid

Carrying out a cyberattack that successfully disrupts grid operations would be extremely difficult but not impossible. Such an attack would require months of planning, significant resources, and a team with a broad range of expertise. Although cyberattacks by terrorist and criminal organizations cannot be ruled out, the capabilities necessary to mount a major operation against the U.S. power grid make potential state adversaries the principal threat.

Attacks on power grids are no longer a theoretical concern. In 2015, an attacker took down parts of a power grid in Ukraine. Although attribution was not definitive, geopolitical circumstances and forensic evidence suggest Russian involvement. A year later, Russian hackers targeted a transmission level substation, blacking out part of Kiev. In 2014, Admiral Michael Rogers, director of the National Security Agency, testified before the U.S. Congress that China and a few other countries likely had the capability to shut down the U.S. power grid. Iran, as an emergent cyber actor, could acquire such capability. Rapid digitization combined with low levels of investment in cybersecurity and a weak regulatory regime suggest that the U.S. power system is as vulnerable—if not more vulnerable—to a cyberattack as systems in other parts of the world.

An adversary with the capability to exploit vulnerabilities within the U.S. power grid might be motivated to carry out such an attack under a variety of circumstances. An attack on the power grid could be part of a coordinated military action, intended as a signaling mechanism during a crisis, or as a punitive measure in response to U.S. actions in some other arena. In each case, the United States should consider not only the potential damage and disruption caused by a cyberattack but also its broader effects on U.S. actions at the time it occurs. With respect to the former, a cyberattack could cause power losses in large portions of the United States that could last days in most places and up to several weeks in others. The economic costs would be substantial. As for the latter concern, the U.S. response or non-response could harm U.S. interests. Thus, the United States should take measures to prevent a cyberattack on its power grid and mitigate the potential harm should preventive efforts fail.

Impact: Taking out the grid would be devastating

Bogost, Ian. “Revenge of the Power Grid.” The Atlantic. 7/15/19.
https://www.theatlantic.com/technology/archive/2019/07/manhattan-blackout-reveals-infrastructure-risk/594025/

Failure, fire, and flood aren’t the only dangers that can befall transformer substations. Power infrastructure can be an appealing target for terrorism because the sites are poorly protected and the economic impact of a successful attack can be high—particularly in a city like New York. Cyberattacks are also possible. This March, a denial of service attack affected electrical systems in Los Angeles and Salt Lake City, two major population centers. Intelligence suggests that the risk of similar foreign attacks is currently elevated. A House Energy and Commerce subcommittee discussed those risks in a hearing the day before the Midtown Manhattan blackout.
One way to mitigate these dangers is to make utility infrastructure less susceptible to single points of failure. Underground distribution tends to make it easier to reach electrical customers via multiple paths. Regulatory agencies such as the New York State Reliability Council also impose requirements on utility service. Con Edison, which powers almost all of New York City, is expected to design its network to operate even if some of its components fail or are lost to disaster. But new risks associated with climate change, cyberwarfare, and other factors haven’t necessarily been accounted for in the design and operation of utility infrastructure.

Impact: Civilians may die

Plumer, Brad. “It’s way too easy to cause a massive blackout in the US.” Vox. 4/14/14.
https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability

Back in 2012, the National Research Council worried that a well-coordinated attack on the grid "could deny large regions of the country access to bulk system power for weeks

> or even months. … If such large extended outages were to occur during times of extreme weather, they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold."
>
> How would that work? It's worth walking through the mechanics of how a truly massive blackout — like the 2003 Northeast blackout that left 50 million people without power — can happen.
>
> Power grids are, by their nature, extremely complex. It's hard to store electricity for any extended period. That means that the output from power plants has to be equal to the use of electricity at all times. Otherwise, power lines can get overloaded or generators underloaded, causing damage to the equipment.
>
> Usually, the grid has protective devices that switch off a piece of equipment if there's a problem. So if, say, a sagging power line hits a tree — causing it to overheat — that line will get disconnected. The problem is that all the other lines now have to carry excess current. If they start overheating and have to switch off, you can get … cascading failures.
>
> So power grid operators have to constantly monitor the system to make sure that power generation and power use are matched up and that a single fault can't cause the entire grid to fail. They're usually very good at this. But it's a difficult task — and if, the grid is already running at capacity or a major piece of equipment falters, it can be hard to prevent "cascading failures." The National Research Council was worried about an attack causing this sort of cascading effect.

Analysis: Cyberwarfare is an easy tool to deploy because it doesn’t have an inherent human cost, which makes retaliation against U.S cyberattacks more likely. However, when cyberwarfare targets vulnerable targets, however, it can put many lives in danger. The Untied States’ power grid is very weak and defenseless, meaning a cyberattack could easily turn off the power for thousands if not millions of Americans. If the United States continues aggressive cyber operations, it could prompt such a retaliation which would put countless lives at risk.

A/2: Offensive operations lead to retaliation on U.S grid

Answer: The U.S grid is well defended

Warrant: The U.S grid is difficult to hit with an attack.

Newman, Lily Hay, “Russian Hackers Haven’t Stopped Probing the US Power Grid.” Wired. 11/28/18. https://www.wired.com/story/russian-hackers-us-power-grid-attacks/

In recent years, hacks against the power grid have gone from a mostly theoretical risk to a real-world problem. Two large-scale blackouts in Ukraine caused by Russian cyberattacks in 2015 and 2016 showed just how feasible it is. But grid hacking comes in less dramatic forms as well—which makes Russia's continued probing of US critical infrastructure all the more alarming.

At the CyberwarCon forum in Washington, DC on Wednesday, researchers from threat intelligence firm FireEye noted that while the US grid is relatively well-defended, and difficult to hit with a full-scale cyberattack, Russian actors have nonetheless continued to benefit from their ongoing vetting campaign.

"There’s still a concentrated Russian cyber espionage campaign targeting the bulk of the US electrical grid," says FireEye analyst Alex Orleans says. "The grid is still getting hit."

FireEye calls the Russia-linked hacking group that has been targeting the US grid "TEMP.Isotope." It's also known as Dragonfly 2.0, or Energetic Bear. The group mostly uses generic hacking tools and techniques created by other actors—a strategy known as "living off the land"—to minimize development time and costs, while also making it harder to identify and track its movements. But TEMP.Isotope has also created at least one custom system backdoor, and often uses spearphishing and infected websites to compromise targets. And the group has brought these tools to bear against the US grid in a patient and methodical way.

Warrant: The US is securing its grid

O'Flaherty, Kate. "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks." Forbes. 7/3/19. https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#14f22ecf3191

The U.S. Government has announced a surprising move to secure power grids by using "retro" technologies. It comes after numerous attempts by foreign actors to launch cyberattacks on so-called critical national infrastructure (CNI).
Nations have been trying to secure the industrial control systems that power CNI for years. The challenge lies in the fact that these systems were not built with security in mind, because they were not originally meant to be connected to the internet.
It is with this in mind that the U.S. has responded with a new strategy: rather than bringing in new technology and skills, it will use analog and manual technology to isolate the grid's most important control systems. This, the government says, will limit the reach of a catastrophic outage.

Warrant: The US is investing in protection

O'Flaherty, Kate. "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks." Forbes. 7/3/19. https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#14f22ecf3191

If that happens and it's approved, a two-year pilot would be set up with the National Laboratories to study power grid operators and identify new vulnerabilities. It would also aim to develop new analog devices with the ability to isolate critical systems from

cyber-attacks. At the same time, a working group would be set up to test these analog devices.

According to Senators King and Risch, SEIA was inspired by the 2015 Russian attack on Ukraine's power grid which left the country without power. "The attack could have been worse if not for the fact that Ukraine relies on manual technology to operate its grid," they said.

Analysis: The United States' electrical grid is not as vulnerable as many would lead you to believe. The grid is well defended and difficult to hit with a catastrophic blow. Furthermore, the United States has recognized the risk of retaliation on its grid by investing in further protection for this piece of critical infrastructure in the future.

CON: Offensive operations lead to war

Claim: Cyberattacks lead to escalation and war.

Warrant: Cyber conflicts are heating up.

> "Global Consequences of Escalating U.S.-Russia Cyber Conflict." Council on Foreign Relations. 4/2/19. https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict

Cyber conflicts involving state actors are quickly becoming a geopolitical reality. Perhaps the most cited example, the alleged Russian interference in the 2016 U.S. election, is a continued source of conflict in U.S.-Russia relations. The story took another turn last October when the U.S. Cyber Command conducted an offensive cyber operation against the Internet Research Agency (IRA), the "Russian troll factory" linked to using disinformation campaigns during the 2016 elections, and onwards. While the operation has yet to be confirmed by the U.S. government, media reports and U.S. officials' commentary taken together suggest the event occurred. The U.S. action, which took place during the 2018 midterm elections, has been portrayed as a defensive warning against Russia and other U.S. adversaries online. But the result of the offensive operation may, however, in the end benefit Russia and possibly contribute to escalation in the cyber domain globally.

Somewhat unexpectedly, the operation was confirmed by the apparent target. In a public announcement, the Russian Federal News Agency (FNA), which is reportedly tied to the IRA, describes a cyberattack that supposedly caused storage system malfunction, specifically destructively targeting the RAID controller and causing hard drives being

formatted. While FNA's credibility is low, the report's claim that the offensive cyber operation resulted in a significant disruption seems undeniable.

Warrant: Escalation leads to retaliation

Greenberg, Andy. "How Not To Prevent a Cyberwar With Russia." Wired. 6/18/19. https://www.wired.com/story/russia-cyberwar-escalation-power-grid/

In the short span of years in which the threat of cyberwar has loomed, no one has quite figured out how to prevent one. As state-sponsored hackers find new ways to inflict disruption and paralysis on one another, that arms race has proven far easier to accelerate than to slow down. But security wonks tend to agree, at least, that there's one way not to prevent a cyberwar: launching a preemptive or disproportionate cyberattack on an opponent's civilian infrastructure. As the Trump administration increasingly beats its cyberwar drum, some former national security officials and analysts warn that even threatening that sort of attack could do far more to escalate a coming cyberwar than to deter it.

Over the past weekend, The New York Times reported that US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. But judging by Russia's response, news of the grid-hacking campaign may have already had the immediate opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries, even as it claimed that Russia's grid was immune from such threats.

Warrant: Cyberattacks lave led to conflict (Israel)

Fazzini, Kate. "Israel says it bombed Hamas compound that committed cyberattacks." CNBC. 5/6/19. https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyberattack-will-lead-to-a-shift.html

The Israel Defense Forces said Sunday it responded to a cyberattack from a Hamas-controlled compound in Gaza with an airstrike, a rare mix of physical and cyber conflict on the world stage.

The cyberattacks emanating from the Gaza facility were aimed at harming Israeli civilians and was thwarted online before the strike, the IDF said, though they did not immediately release further details about the cyberattack.

In Gaza, Hamas militants have launched 600 rockets into Israel, while the country has retaliated with hundreds of strikes on military targets there.

International organizations and militaries have long debated how or when countries should use military force to respond to cyberattacks that could harm citizens.

The incident is certain to spark further debate on how cyberattacks and live conflict should mix. It's an important distinction as countries including the United States grow increasingly concerned at the possibility a cyberattack on the electric grid, water supply or other infrastructure could lead to loss of human life, and create norms for how they will respond to those threats, either immediately or preemptively.

Impact: Retaliatory strikes kill.

Cohen, Kelly. "Violence continues as Israel and Hamas exchange fire over 2 days of fighting." Vox. 5/5/19. https://www.vox.com/world/2019/5/4/18529287/israel-rocket-attack-hamas-450-rockets-idf-airstrikes-tel-aviv

Executing the prime minister's directive, the IDF said Sunday it has conducted attacks on more than 260 military targets in Gaza, including an assault on what the Israeli military described as a "building where Hamas cyber operatives work" and a targeted attack

against a Palestinian militant commander it says funneled money to "terror organizations operating within the Gaza Strip."

The successful targeted attack against that commander, Hamed Ahmed Al-Khodary, was the first targeted killing Israel has conducted since 2014. Targeted attacks had been suspended as an olive branch; in previous conflicts, Palestinian critics have called the attacks assassinations.

Three other Palestinians are believed to have been wounded in the attack on Al-Khodary. All told, officials in Gaza say 20 people, including eight civilians, have been killed throughout the weekend.

Who is responsible for some of those deaths is disputed.

For instance, officials in Gaza said that Palestinian civilians Falastine Abu Arar, a 37-year-old pregnant mother, and her 14-month-old niece Siba, were killed by Israeli forces Saturday. However, the IDF has denied this, claiming the woman and child died due to a misfiring of a Hamas rocket.

At least four Israeli citizens have been killed.

Analysis: As cyberattacks increase in frequency across the globe, the risk of escalation and violence has risen as well. The recent strike by Israel demonstrates that cyberattacks can lead to real world conflict and loss of life. The United States has yet to face a similar attack, but the risk is there if it continues to act aggressively in cyberspace.

A/2: Offensive operations lead to war

Answer: Cyberattacks will not cause conflict.

Warrant: Cyberattacks less likely to escalate

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

However, cyberattacks are less likely to deter adversaries for the same reasons they are less likely to lead to escalation. Deterrence is all about sending signals to other countries that there will be consequences if they behave badly.

[How cyber operations can help manage crisis escalation with Iran]

As other scholars have noted, the best deterrence signals are ones that are costly, visible and credible. Here's why cyber-operations often fail this test: They may be hard to detect, hard to attribute to their source and hard to turn into a credible threat, because they may rely on vulnerabilities that are easy to plug if the target knows about them. This all makes cyber-operations less escalatory, but also harder to use to send clear signals.

Moreover, as Sanger and Barnes note, the United States is in a particularly vulnerable position when it uses cyberattacks, because the U.S. way of life is more dependent on digitally dependent technologies than Iranian society. So if Iran retaliates to a cyberattack with another cyberattack, the United States may come off worse. Furthermore, the United States depends more on the global communications infrastructure than Iran does, generating further vulnerabilities that might deter America from using cyberattacks.

Warrant: Cyberattacks make people less likely to respond with violence

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

Recent work by myself and Sarah Kreps finds that the American public is less likely to support retaliation against cyberattacks than against an airstrike, even when they create similar effects. U.S. government security decision-makers seem to feel the same way. Research by Brandon Valeriano and Benjamin Jensen, as well as evaluation of strategic war games, finds that players are less likely to respond to a crisis by escalating when they are given cyber-tools — and less likely to respond with violent escalation when the adversary conducts a cyberattack.

These researchers looked at responses from people in the United States for the most part. However, statistical analysis of international cyber-incidents reaches mostly similar conclusions, as does research on battlefield operations in Ukraine. The emerging consensus among researchers is that cyberattacks aren't unusually escalatory. If anything, the opposite is true.

Analysis: Cyberattacks aren't as visible or easily understood as conventional warfare, meaning it's less likely to prompt retaliation and escalation. Recent studies have shown voters are less likely to support retaliation of the cause is a cyberattack. Escalation, therefore, is less likely with offensive cyber operations than with conventional military strategies.

CON: The U.S shares its offensive arsenal leading to conflict

Claim: The United States shares its tech with allies who use it for bad ends.

Warrant: US develops advanced cyberweapons

Vinik, Danny. "America's secret arsenal." Politico. 12/9/15.
https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331

The growth has been snowballing. Last year, the secretary of the Army created a new branch for cyber—the first new Army branch since Special Forces was created in 1987. By October of this year, there were 32 teams, coordinated out of a new joint force headquarters for cyber opened last year in Fort Gordon, Georgia. By next summer, the Army expects to have 41.

What's going on? The growth points to one of the most cutting-edge, but also obscure, realms of American military activity: its cyber strategy, and especially its strategy for cyber offense. The United States already has, most observers believe, the most powerful cyberattack capabilities in the world. Much less clear is just what its capacities actually are—and when the Department of Defense believes it should use them.

In conventional war, weapons and strategies are fairly well-understood; the international community has developed rules of the road for armed conflict. Even tactics wrapped in secrecy, such as covert military raids, are governed by some standards about when and how we use them.

That's not the case with cyber. It's widely acknowledged that offensive cyberattacks will be a necessary component of any future military campaign, and the weapons are being developed now. In April, the DOD released a 32-page document that laid out specific strategic goals for U.S. cyber offense for the first time. But critics say that document still

leaves many questions unanswered about how, when and where the government will use these capabilities.

Warrant: US shares tech with allies

"US to offer cyberwar capabilities to NATO allies." CNBC. 10/3/18. https://www.cnbc.com/2018/10/03/us-to-offer-cyberwar-capabilities-to-nato-allies.html

Acting to counter Russia's aggressive use of cyberattacks across Europe and around the world, the U.S. is expected to announce that, if asked, it will use its formidable cyberwarfare capabilities on NATO's behalf, according to a senior U.S. official.
The announcement is expected in the coming days as U.S. Defense Secretary Jim Mattis attends a meeting of NATO defense ministers on Wednesday and Thursday.
Katie Wheelbarger, the principal deputy assistant defense secretary for international security affairs, said the U.S. is committing to use offensive and defensive cyber operations for NATO allies, but America will maintain control over its own personnel and capabilities.
The decision comes on the heels of the NATO summit in July, when members agreed to allow the alliance to use cyber capabilities that are provided voluntarily by allies to protect networks and respond to cyberattacks. It reflects growing concerns by the U.S. and its allies over Moscow's use of cyber operations to influence elections in America and elsewhere.
"Russia is constantly pushing its cyber and information operations," said Wheelbarger, adding that this is a way for the U.S. to show its continued commitment to NATO.

Warrant: Israel gets US tech

Johnson, Derek B. “Bill boosting cyber R&D between U.S. and Israel passes house.” FCW. 7/24/19. https://fcw.com/articles/2019/07/24/house-bill-us-israel-cyber-research.aspx

The House quietly passed legislation on July 23 that would expand cybersecurity research and development partnerships between several federal agencies and the government of Israel.

The bill, introduced in March by Reps. Ted Deutch (D-Fla.) and Joe Wilson (R-S.C.), covers a broad set of cooperative issues between the two countries but contains several provisions related to cybersecurity. Most notably, it would create a new grant program at the Department of Homeland Security to support cybersecurity R&D as well as the demonstration and commercialization of cybersecurity technology with the Israeli government.

Applicants would be eligible for funding under the program if their project represents a joint venture between a U.S.-based third-party organization and an Israeli one, including the U.S. and Israeli governments, and addresses “a requirement in the area of cybersecurity research or … technology, as determined by the secretary.

Impact: Israel’s cyber operations escalated and led to conflict.

Makuch, Ben. “Israel Bombing ‘Cyber Operatives Isn’t Cyber War, It’s Just War.” 5/6/19. https://www.vice.com/en_us/article/gy4vn3/israel-bombing-cyber-operatives-gaza-palestine

On Sunday, amidst Israel’s deadly bombing campaign in Gaza, the Israeli Defense Forces announced it had taken out a building housing “Hamas cyber operatives” after thwarting a “cyber offensive” from the group.

> The IDF announced the strike in a tweet that included a nerdy, macabre joke. The apparent novelty of targeting hackers with bombs, and the way the announcement was made set off a flurry of reactions on infosec Twitter.
>
> For some, the strike heralded a new moment in cyberwarfare. Hackers had just been bombed, apparently for their hacking efforts. Mikko Hypponen, a well-known security researcher who's tracked malware for more than 20 years, said in a Tweet that "we just crossed a line we haven't crossed before."
>
> But according to other experts, the reality is that this may not be an escalation in so-called "cyberwar" but just a continuation of aerial bombing campaigns. And it's not the first time that hackers have been targeted by a major military power.

Analysis: The United States has developed very powerful cyber weapons over the years. Whether or not the government chooses to use them with restraint, they have chosen to share those technologies with allies who may not be as cautious. In particular, the U.S. shares cyber weapons with Israel, who was recently involved in a cyber conflict that led to a conventional strike and a several days long confrontation.

A/2: The U.S shares its offensive arsenal leading to conflict

Answer: Sharing weapons builds alliances.

Warrant: The U.S. has built alliances with cyber technology.

"US to offer Cyber Warfare Technology to NATO" VOA News. 10/6/18. https://learningenglish.voanews.com/a/us-to-offer-cyber-warfare-technology-to-nato/4601212.html

A United States official says the U.S. military is offering its cyber warfare technology, including computer software tools, to the North Atlantic Treaty Organization (NATO). The move is meant to help the 69-year-old alliance better deal with cyber threats from Russia and China.

The Associated Press says an announcement is expected soon.

Katie Wheelbarger is a deputy assistant defense secretary for the United States Department of Defense. She said the U.S. is prepared to use defensive and offensive cyber operations for NATO allies. One condition, however, is that the U.S. will keep control of its own personnel and operations.

Warrant: The US is bolstering cyberalliances

Herr, Trey. "Sharing is Caring: The United States' New Cyber Commitment for NATO." 10/10/18. https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato

The new commitment is notable given how cybersecurity has long been treated as an exceptional domain of operations, and cyber capabilities reserved as strategic national

assets to be shared with only the closest of allies. With this announcement, the Pentagon is suggesting that cyber capabilities might be used alongside conventional weapons with allies and indeed, equal weight appears to be given to offensive and defensive operations. Perhaps most significantly, the announcement moves NATO partners closer to what has been a tight coterie of U.S.-favored signals intelligence partners such as the United Kingdom, New Zealand, Australia, and Canada.

The DoD announcement is a sign of the continued, if nascent, normalization of cybersecurity under the current administration and in Europe. Even where offensive cyber operations may not rise to the level of war, they provide decision-makers with options to influence the geopolitical environment. This aligns with recent trends in the U.S. military to integrate cyber capabilities into maneuver units and large exercises, and reflects the shift towards more risk acceptant and offensive measures to counter cyberattacks found in the 2018 DoD Cyber Strategy.

Moving cyber capabilities into the same strategic frame as conventional weapons, especially with NATO, reflects a shift in institutional cyber arrangements within the United States and the growing power of the military relative to the intelligence community. For the United States, cyber capabilities have always had a complicated relationship with the intelligence community, in particular the National Security Agency (NSA). When Cyber Command stood up in 2010 as a sub-unified combatant command within the Department of Defense, it moved into the NSA's headquarters, staffed its management ranks with longtime NSA employees, borrowed networks and technical capabilities, and to this day shares a dual-hatted commander. In the immediate years after the command was created, it was logical that the structure of partnerships with allies looked more like the special signals intelligence relationships formed around the NSA rather than traditional alliance networks in NATO and Asia. The recent announcement aligns cyber operations more closely with Department of Defense missions, which are more likely to posture capabilities for deterrent effects, than intelligence missions, which view capabilities as assets to be carefully husbanded.

Impact: Cyberalliances are key

Herr, Trey. "Sharing is Caring: The United States' New Cyber Commitment for NATO." 10/10/18. https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato

Treating cybersecurity capabilities more like conventional arms and less like national assets also helps drive the integration of cyber operations into the planning and execution of a broader array of conventional military missions. Early cyber operations were largely conventional espionage and surveillance activities supercharged by the spread of computing and the internet. In the United States, this led to the creation of large and complex software tools, carefully guarded by the intelligence community as national assets (sometimes unsuccessfully). The DoD's announcement indicates a move towards treating at least some of these capabilities, along with their supporting infrastructure, more like conventional armaments and making them available for broader use; a model closer to Central or Special Operations Command and less like the National Security Agency.

The Pentagon's new commitment also reflects changes in how Europe talks about cybersecurity and characterizes the Russian threat. The last two years have seen a trend toward more open discussion of offensive cyber operations and the possibility of the alliance adopting more assertive postures to counter cyber operations against its members. After years of devastating ransomware attacks and cyber-enabled information attacks, NATO members are more willing to explore cyber triggers to Article 5. They have also been more willing to articulate the cyber threat against the alliance. In addition to last week's denunciation by Dutch, UK, and U.S. authorities, Russian state actors are widely suggested to be responsible for an increasingly brazen series of operations, including targeting German government ministries, French and British TV stations, and more.

> Sharing offensive cyber capabilities raises the question of whether cyber operations can extend effective deterrence to NATO partners. There seems to be little focus on using these operations to deter conventional or nuclear attacks on NATO countries, but this may evolve. The United States seems to want NATO to use cyber operations to deter other cyber operations, particularly those falling under the threshold of armed conflict. Cyber operations have all sorts of problems for deterrence: signaling is difficult, they can be perceived as a cheap threat, and their effects are largely uncertain. By contrast, moving new military forces in Eastern Europe or conducting ground exercises are credible signals of extended deterrence, but are costly and time consuming. Cyber capabilities aren't free, nor are they necessarily cheap, but the promise to use them can add new credibility to a deterrent threat without the same investment and delay as conventional alternatives. Sharing cyber capabilities may be a cheaper way to signal alliance commitment than other options and might signal a further maturation, and acceptance, of cybersecurity into geopolitics.

Analysis: The United States sharing its technology may run the risk of it being used, but it also allows for alliances to be created. By bolstering its cyberalliance with NATO countries, the United States is more prepared for cyberattacks in the future.

CON: Offensive operations lead to escalation of tensions with Russia

Claim: Offensive operations will escalate tensions with Russia.

Warrant: Tensions with Russia are high.

Dorell, Oren. "Another Cold War? Tensions between U.S. may be higher now." USA Today. 3/29/18. https://www.usatoday.com/story/news/world/2018/03/29/united-states-russia-cold-war-putin-trump/467806002/

Is a second Cold War brewing? Not so fast.

President Trump's expulsion this week of 60 Russian diplomats over the poisoning of a Russian double agent in Britain eclipsed the 55 diplomats then-President Ronald Reagan expelled in 1986 during the height of the Cold War.

Measures to remove Russian diplomats by Western countries, and Moscow's retaliatory expulsions of the same number on Thursday, were a throwback. But much has changed since the collapse of the Soviet Union. The Russians have new tools at their disposal.

The rules of engagement for both countries are less clear. And the United States and its allies are much stronger now.

The differences make the tensions between Russia and the U.S. possibly more volatile, but they also create opportunities for the West. Here are a few ways what's happening now is not like the Cold War:

Warrant: The U.S attacked Russia's grid.

Klar, Rebecca. “Russia: Reported US cyberattack on power grid possible.” The Hill. 6/17/19. https://thehill.com/policy/national-security/448847-russia-reported-us-cyberattack-on-power-grid-possible

The Kremlin on Monday reportedly said it is possible the U.S. put implants into Russian power grids.

The New York Times first reported the U.S. allegedly gearing up for a cyberattack last week, citing unnamed officials describing the types of actions that had been taken toward Russian power grids.

Kremlin spokesman Dmitry Peskov told Reuters, “Undoubtedly this information shows the hypothetical possibility ... all signs of cyber war and military cyber action against the Russian Federation.”

The Hill has reached out to the Kremlin for comment.

Peskov told Reuters that Russian authorities are working to keep its economy safe after unnamed strategic parts had endured foreign cyberattacks.

According to the New York Times report, probes in control systems have been in place since at least 2012 but now the strategy is shifting toward offense.

Officials told the Times the U.S. had deployed computer code within Russia's grid to combat Russian disinformation and hacking in 2018 elections.

Warrant: The recent cyberattack runs risk of retaliation

Greenberg, Andy. “How Not To Prevent a Cyberwar With Russia.” Wired. 6/18/19. https://www.wired.com/story/russia-cyberwar-escalation-power-grid/

In the short span of years in which the threat of cyberwar has loomed, no one has quite figured out how to prevent one. As state-sponsored hackers find new ways to inflict disruption and paralysis on one another, that arms race has proven far easier to accelerate than to slow down. But security wonks tend to agree, at least, that there's

one way not to prevent a cyberwar: launching a preemptive or disproportionate cyberattack on an opponent's civilian infrastructure. As the Trump administration increasingly beats its cyberwar drum, some former national security officials and analysts warn that even threatening that sort of attack could do far more to escalate a coming cyberwar than to deter it.

Over the past weekend, The New York Times reported that US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. But judging by Russia's response, news of the grid-hacking campaign may have already had the immediate opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries, even as it claimed that Russia's grid was immune from such threats.

Impact: Russia may respond

Goud, Naveen. “Russia to retaliate to cyber threats from United States.” Cybersecurity Insiders. https://www.cybersecurity-insiders.com/russia-to-retaliate-to-cyber-threats-from-the-united-states/

Reacting to the news published the New York Times (NYT) about the intrusions into the Russian national infrastructure, the government officials of Russian Federation have released a press statement yesterday saying it knows on how to retaliate to such threats from adversaries and have successfully thwarted them till date.

Announcing the same through RIA and TASS News agencies the government sources working under the regime of President Vladimir Putin have suggested that the cyber attacks were being carried out by Pentagon keeping the US president Donald Trump under sheer ignorance.

Trump, however, reacted to the news published on Saturday in NYT by saying the article is baseless and the news resource was working towards bringing political instability in the region.

Kremlin released a press statement on Monday saying that the news report was completely true as cyber attacks from the US on National Infrastructure of Russia were escalating on a weekly note- all as a part of cyberwarfare triggering World War 3.

"We have managed to neutralize such actions and have enough potential to thwart them with severity", says Konstantin Yurivich Noskov, the Minister of Digital Development, Communications and Mass Media of Russia.

Analysis: Pursuing a more aggressive cyber-strategy with Russia could escalate what is already a very tense and hostile relationship between the two countries. Russia has already threatened to respond after the United States was able to breach the security of Russia's electrical grid. More offensive cyber operations could push this détente over the brink.

A/2: Offensive operations lead to escalation of tensions with Russia

Answer: Cyberattacks will not escalate tensions.

Warrant: Russia can stop the U.S' cyberattacks

"Russia thwarts U.S. cyber attacks on its infrastructure: new agencies." Reuters. 6/17/19. https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCN1TI1U0

Russia has uncovered and thwarted attempts by the United States to carry out cyber attacks on the control systems of Russian infrastructure, Russian news agencies cited an unnamed security source as saying on Monday.

The disclosure was made on Russia's RIA and TASS news agencies days after the New York Times cited unnamed government sources as saying that the United States had inserted potentially disruptive computer code into Russia's power grid as part of a more aggressive deployment of its cyber tools.

The newspaper suggested President Donald Trump had not been informed of the intrusions. Trump, without providing evidence, said on Twitter that the article was not true.

The Kremlin had said earlier on Monday that the U.S. newspaper report was worrying and showed that a cyber war was, in theory, possible.

"We see and note such attempts," the Russian security source was quoted as saying in response to the report. "However, we manage to neutralize these actions."

Foreign intelligence services have stepped up cyber attacks against Russia in recent years and are targeting mainly transport, banking and energy infrastructure, the source told TASS and RIA.

Warrant: Cyberattacks are less likely to escalate

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

However, cyberattacks are less likely to deter adversaries for the same reasons they are less likely to lead to escalation. Deterrence is all about sending signals to other countries that there will be consequences if they behave badly.

[How cyber operations can help manage crisis escalation with Iran]

As other scholars have noted, the best deterrence signals are ones that are costly, visible and credible. Here's why cyber-operations often fail this test: They may be hard to detect, hard to attribute to their source and hard to turn into a credible threat, because they may rely on vulnerabilities that are easy to plug if the target knows about them. This all makes cyber-operations less escalatory, but also harder to use to send clear signals.

Moreover, as Sanger and Barnes note, the United States is in a particularly vulnerable position when it uses cyberattacks, because the U.S. way of life is more dependent on digitally dependent technologies than Iranian society. So if Iran retaliates to a cyberattack with another cyberattack, the United States may come off worse. Furthermore, the United States depends more on the global communications infrastructure than Iran does, generating further vulnerabilities that might deter America from using cyberattacks.

Warrant: Cyberattacks make people less likely to respond with violence

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

Recent work by myself and Sarah Kreps finds that the American public is less likely to support retaliation against cyberattacks than against an airstrike, even when they create similar effects. U.S. government security decision-makers seem to feel the same way. Research by Brandon Valeriano and Benjamin Jensen, as well as evaluation of strategic war games, finds that players are less likely to respond to a crisis by escalating when they are given cyber-tools — and less likely to respond with violent escalation when the adversary conducts a cyberattack.

These researchers looked at responses from people in the United States for the most part. However, statistical analysis of international cyber-incidents reaches mostly similar conclusions, as does research on battlefield operations in Ukraine. The emerging consensus among researchers is that cyberattacks aren't unusually escalatory. If anything, the opposite is true.

Analysis: Cyberwarfare is far less likely to escalate the relationship between the U.S. and Russia than other issues because voters and politicians are less likely to treat it as a credible threat. Furthermore, Russia is able to disable most of the attacks launched by the United States, including the recent attacks on its grid, meaning there's little reason to believe Russia feels it needs to build up its capabilities and respond.

CON: Offensive operations lead to escalation of tensions with China

Claim: Offensive operations will increase the stakes of the ongoing cyberwar with Russia.

Warrant: Tensions with China are rising

Shapiro, Ari and Daly, Robert. "Rising Tensions Between The U.S. And China Go Beyond Trade Dispute." NPR. 8/6/19. https://www.npr.org/2019/08/06/748810969/rising-tensions-between-the-u-s-and-china-go-beyond-trade-dispute

DALY: What we really see now is long-term contentious relations between the United States and China. This is a major development that is going to be worked out most likely over the course of decades. China is now, essentially, a peer competitor to the United States...

SHAPIRO: Meaning it has a comparably sized economy.

DALY: It means it has a comparably sized economy. It is narrowing the gap - military gap - especially in the Western Pacific, where it is using asymmetric tactics that can offset things like our aircraft carriers. China is also an education leader. It is becoming a technological leader. And it's the world's biggest trading nation.

So China is on the move all over the world. And the U.S.-China relationship is not anymore just Beijing to Washington. It's being measured in Africa, in South America, at both poles, in cyberspace and outer space.

SHAPIRO: And is it becoming a more adversarial relationship now because of China's growth, because it suddenly is big enough to really challenge the United States?

DALY: Well, there's a big argument in the United States about this. There's one group of folks who think that engagement policy failed. We engaged with China from 1979 until

about 2013 when Xi Jinping came into power. And the idea of engagement was that coevolution was in the American interest as well as in China's interest. And you could bring China along to be a responsible player to some degree.

Many hardliners in the United States government - and outside and including in the expert community - now claim that engagement was a sucker's game and that we have raised up a tiger which could now devour us. But there are different schools of thought about this, and many of us think that we still need to engage with China, albeit more strategically.

SHAPIRO: That image of raising a tiger that will devour us is very dramatic. Is that what we're talking about here? I mean, like, one or the other will triumph?

DALY: I don't think so. I'm actually borrowing from a Chinese phrase - (speaking Chinese) - you don't want to raise up a baby tiger because it grows up. But again, there are people like Steve Bannon and the Committee for the Present Danger: China, which now claim that China is an existential threat to the United States. And they're also claiming that the United States cannot coexist with the Chinese Communist Party, despite the fact that we've been doing so at least since 1949.

Warrant: China and US already engaged in cyberwarfare

Doffman, Zak. “Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities.” Forbes. 8/3/19. https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#2fac32716758

The notorious Chinese state-sponsored hacking group APT10, which is believed to act for the country's Ministry of State Security, is the most likely culprit behind a cyber campaign targeting U.S. utility companies in July. The disclosure on August 1 was made by researchers at Proofpoint, who warned that "persistent targeting of any entity that

provides critical infrastructure should be considered an acute risk—the profile of this campaign is indicative of specific risk to U.S.-based entities in the utilities sector."

The spear-phishing campaign targeted company employees with emails purporting to be from the National Council of Examiners for Engineering and Surveying (NCEES), emails that claimed to be delivering professional examination results but which were actually delivering "malicious" Microsoft Word attachments. Threat researchers at Proofpoint broke the news and dubbed the command and control malware "LookBack."

According to Proofpoint's Michael Raggi and Dennis Schwarz, once the emailed Microsoft Word attachment is opened, a malicious VBA macro drops files onto the host computer which then provide the malware with the command and control framework needed to access data on the machine. The malware can attack and mimic a wide range of processes on an infected machine—primarily, though, the objective is to steal data files and take operational screenshots.

Warrant: The US has started to respond

Gertz, Bill. “U.S. hits back against Chinese cyberattacks.” Washington Times. 3/6/19. https://www.washingtontimes.com/news/2019/mar/6/us-counters-china-cyberattacks/

American intelligence and military cyberwarriors have begun conducting counter-cyberattacks against Chinese intelligence and military targets, according to a U.S. official.

The counterattacks are part of a new Trump administration policy designed to retaliate for rampant cybertheft of American technology by the Chinese that has caused estimated losses ranging from $200 billion to $600 billion a year. Details of the U.S. cyberoperations were not disclosed, and the activities remain classified.

The hacking is likely to include theft of Chinese advanced military know-how, such as hypersonic missile technology — an area of military research where China is believed to

be ahead of the United States. Another possible target would be technology related to China's anti-ship ballistic missile technology like that deployed in the DF-21D ship-killing missile. Such technology requires maneuvering warheads and special guidance.
One recent reported U.S. operation involved cyberattacks on a Russian troll farm in St. Petersburg on the day of the November midterm elections, The Washington Post reported. The troll farm was linked to the Moscow influence operation against the 2016 presidential election.

Impact: China is escalating, building alliances

Doffman, Zak. "Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S." Forbes. 7/6/19. https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#42ec1b2c42eb

"The Islamic Republic of Iran and China are standing in a united front," claimed Iran's ICT Minister Mohammad Javad Azari Jahromi last week, "to confront U.S. unilateralism and hegemony in the field of IT." For confront read "offensive actions," and for IT read "cyber."
Jahromi followed this with similar comments in Beijing a few days later, when he met his opposite number Miao Wei. The ministers discussed "common challenges" in the face of "U.S. unilateralism," of which Jahromi said, "we are facing similar challenges, so we need to find common solutions." The Iranian minister accused the U.S. of "spreading its hegemony on new strategic technologies such as artificial intelligence," and criticized Washington's actions against Huawei and ZTE.
Miao Wei reportedly stressed that cooperation between the two countries would help tackle "such threats and pressures."

Analysis: China has historically been the more aggressive of the two countries when it comes to targeted cyberattacks. The United States has started going on the offensive more often, and China has certainly taken notice. In response, they've begun forming alliances in cyberspace that could form a threat to the United States in the long term.

A/2: Offensive operations lead to escalation of tensions with China

Answer: China is already engaged in cyberwarfare.

Warrant: China has been engaging in cyberattacks for years

Wagner, Daniel. "China's head start in cyberwarfare leaves others playing catch-up." South China Morning Post. 3/7/19. https://www.scmp.com/comment/insight-opinion/united-states/article/2188873/chinas-head-start-cyberwarfare-leaves-us-and

Buyers apparently included the Pentagon and a host of other US federal agencies. A subsequent report by the FBI concluded that the routers could be used by foreign intelligence agencies to take down networks and weaken cryptographic systems.
Armed with knowledge of the flaws in Microsoft's and Cisco's software and hardware, China's hackers had the ability to stop most of the world's networks from operating.
Chinese networks would also have been vulnerable but, as part of its deal with Microsoft, the Chinese modified the version of Microsoft software sold in China to include a secure component using their own encryption, according to the book.
They also developed their own operating system (Kylin) and secure microprocessors for use on servers and Huawei routers.
By 2003, the Chinese government had created cyberwarfare units with defensive and offensive capabilities with weapons that had never been seen before, according to Cyber War.
Why US cybertheft demands are so painful for China
These capabilities include the ability to plant information mines, conduct information reconnaissance, change network data, release information bombs, dump information

garbage, disseminate propaganda, apply information deception, release clone information, and establish network spy stations.

By 2007, China was said to be penetrating US and European networks, successfully copying and exporting huge volumes of data. China has since developed its cyberwarfare capabilities into a finely tuned and largely unrivalled machine.

Also by 2007, Chinese hackers were able to carry out the "Byzantine Hades" cyberattacks with little more than a peep of condemnation from US officials.

Warrant: Cyberattacks are less likely to escalate

Schneider, Jacquelyn. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran? The Washington Post. 10/1/19. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

However, cyberattacks are less likely to deter adversaries for the same reasons they are less likely to lead to escalation. Deterrence is all about sending signals to other countries that there will be consequences if they behave badly.

[How cyber operations can help manage crisis escalation with Iran]

As other scholars have noted, the best deterrence signals are ones that are costly, visible and credible. Here's why cyber-operations often fail this test: They may be hard to detect, hard to attribute to their source and hard to turn into a credible threat, because they may rely on vulnerabilities that are easy to plug if the target knows about them. This all makes cyber-operations less escalatory, but also harder to use to send clear signals.

Moreover, as Sanger and Barnes note, the United States is in a particularly vulnerable position when it uses cyberattacks, because the U.S. way of life is more dependent on digitally dependent technologies than Iranian society. So if Iran retaliates to a cyberattack with another cyberattack, the United States may come off worse.

Furthermore, the United States depends more on the global communications infrastructure than Iran does, generating further vulnerabilities that might deter America from using cyberattacks.

Analysis: Given that China has been engaging in coordinated cyberattacks on the United States for years, it's hard to believe that the United State's offensive operations are shifting the tides. China will continue to do so regardless of what the United States does on the offensive, especially because cyberattacks are less likely to escalate the relationship between two nations.

CON: Offensive operations lead to escalation of tensions with Iran

Claim: Offensive operations with Iran have escalated tensions.

Warrant: Tensions with Iran rising

Haltiwanger, John. “Trump and Iran may be on the brink of a war that would likely be devastating to both sides.” Business Insider. 9/19/19. https://www.businessinsider.com/trump-iran-near-brink-of-a-war-that-would-likely-devastate-both-sides-2019-5

In May, the US deployed military assets to the Middle East to counter threats from Iran. This was around the same time US sanctions meant to choke out Iran's oil revenue went into full effect.

Within weeks, oil tankers in the region were attacked, which the US blamed on Iran. The US said Iran used naval mines to sabotage the tankers. Iran also seized oil tankers, which further increased tensions.

In late June, Iran shot down a US Navy drone, which nearly prompted a military response from President Donald Trump. Trump called off the retaliatory strike at the last minute, however, stating it would not have been proportionate to the downing of an unmanned aircraft.

Warrant: The US and Iran engaged in cyber conflict

McKay, Hollie. “Iran prepares for cyberwar amid rising tensions, boasts thousands of cyberbatallions.” Fox News. 10/4/19. https://www.foxnews.com/tech/iran-cyberwar-rising-tensions

In the aftermath of last month's Saudi oil field attacks, believed to have been carried out by Iran, cybersecurity experts have detected an uptick in Iranian movement — and they contend it aims to both guard their nation against retaliation and to launch its own attacks in the shadowy arena of cyberspace.

“Both the U.S. and Iran are maneuvering in this space right now, and we will see ongoing attacks from both sides. The key question is how far will they go and how much the situation escalates,” David Kennedy, founder and CEO of TrustedSec and a former U.S. military intelligence analyst told Fox News. “Iran has been aggressive over the past several years when it comes to cyberattacks. Its back is against the wall, and it has less to lose from a cyberwar with the United States.”

President Trump has long expressed his hesitation for the Islamic Republic of Iran. The country has remained at the forefront of his foreign policy decisions, subject to both economic and military threats. Nonetheless, Trump has also advocated for getting the U.S out of the Middle East and becoming further embroiled in protracted conflicts – making cyberattacks and digital warfare effective and clean-handed methods to cripple Tehran further and demonstrate American strength.

“Iran is currently preparing for an attack and seems to be slowing their current attacks as a matter of readiness,” said Jeff Bardin, chief intelligence officer at cybersecurity firm Treadstone 71. “All critical infrastructures are moving to higher readiness levels.”

Impact: Iran is forming alliances

Doffman, Zak. “Cyber Warfare Threat Rises As Iran And China Agree ‘United Front’ Against U.S.” Forbes. 7/6/19.

https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#42ec1b2c42eb

"The Islamic Republic of Iran and China are standing in a united front," claimed Iran's ICT Minister Mohammad Javad Azari Jahromi last week, "to confront U.S. unilateralism and hegemony in the field of IT." For confront read "offensive actions," and for IT read "cyber."

Jahromi followed this with similar comments in Beijing a few days later, when he met his opposite number Miao Wei. The ministers discussed "common challenges" in the face of "U.S. unilateralism," of which Jahromi said, "we are facing similar challenges, so we need to find common solutions." The Iranian minister accused the U.S. of "spreading its hegemony on new strategic technologies such as artificial intelligence," and criticized Washington's actions against Huawei and ZTE.

Miao Wei reportedly stressed that cooperation between the two countries would help tackle "such threats and pressures."

Impact: Iran could wage cyberwarfare

Kennedy, David. "How Iran Would Wage Cyber War Against The United States." National Interest. 10/5/19. https://nationalinterest.org/blog/buzz/how-iran-would-wage-cyber-war-against-united-states-85841

The Center for Strategic & International Studies (CSIS) offers this assessment of Iran: "Iranian [cyber] attacks are likely to be retaliatory, intending to make the point that the United States is not invulnerable but without going too far." It goes on to say that, "Attacking major targets in the American homeland would be escalatory, something Iran wishes to avoid."

This is a fair assessment of Iran, but there is a lot of wiggle room in terms of what is considered "retaliatory"—as well as what Iran deems to be instigative and the

timeframe for a response—and what constitutes "major targets" in the United States. Remember, Iran has already shown itself to be brazen in its attacks on U.S. homeland targets—and some describe the early 2010s cyber skirmishes with Iran as America's first known cyberwar.

Iran is likely to carry out the bulk of any attacks on Gulf state rivals, with a particular focus on the royals, government assets and oil and gas industry infrastructure. But we should not underestimate its ability or willingness to attack important targets within the United States. Whether it limits these attacks to soft targets, like media companies, think tanks, outspoken critics of Iran, etc., or instead goes after hard targets like the U.S. financial system, energy industry and government assets depends entirely on how escalatory the regime considers U.S. actions to be.

What Trump calls "maximum pressure," the Iranians view as "economic terrorism." To Iran's leaders, any cyber offensive action taken at any time during the current standoff and destabilizing economic sanctions may be deemed justified as a retaliatory measure.

Analysis: Tensions with Iran have already been on the rise, but there has been a recent spike that can be attributed to unilateral cyberattacks on behalf of the United States. Iran specifically cited these attacks when announcing they've formed an alliance with China as an attempt to push back against the United States, which could be a problem for the United States in the long term.

A/2: Offensive operations lead to escalation of tensions with Iran

Answer: The US can stop an Iranian cyberoffensive.

Warrant: US Cyberattacks can disable Iran

Miller, Maggie. "US cyberattack took out Iran's ability to target oil tankers: report." The Hill. 8/28/29. https://thehill.com/policy/cybersecurity/459199-us-cyberattack-took-out-irans-ability-to-target-oil-tankers-report

A cyberattack carried out by U.S. Cyber Command against Iran in June severely impacted a database used by Iran to target oil tankers, The New York Times reported Wednesday.
Government officials told The New York Times that the secret cyberattack temporarily hurt Iran's ability to target shipping traffic in the Persian Gulf.
The officials discussed the consequences of the cyberattack in order to "quell doubts within the Trump administration" as to whether the attack was worth the loss of access to key intelligence sources in Iran, the Times reported.
U.S. Cyber Command targeted a network run by Iran's Revolutionary Guard Corps, Iran's paramilitary forces, that U.S. intelligence reported was involved in an attack on American oil tankers earlier this year.
Iran is still working to get all its systems back online and recover data that was lost during the June cyberattack, according to the Times.
The cyberattack took place the same day President Trump called off planned military strikes on Iran in retaliation for shooting down an unarmed U.S. surveillance drone. Iran claimed the drone was in its airspace, while U.S. officials said it was in international airspace.

Warrant: US is prepared to retaliate if Iran attacks

Baldor, Lolita. "US prepared to strike back against cyberattacks amid report of naval systems breaches." Military Times. 3/14/19. https://www.militarytimes.com/news/pentagon-congress/2019/03/14/us-prepared-to-strike-back-against-cyberattacks-amid-report-of-naval-systems-breaches/

Members of Congress peppered Nakasone and Kenneth Rapuano, the assistant defense secretary for homeland defense, with questions about what the military is doing to respond to cyber breaches and deter countries like Russia and China.

Rapuano acknowledged that for years the U.S. did not sufficiently respond to cyberattacks by other nations, particularly as the breaches did not rise to the level of a conventional military response. He said deterrence is about imposing consequences and, "historically we have not done that."

He said that strategy is changing but officials also have a deliberate approval process for offensive cyber operations, including some that require presidential approval.

He also said that the Pentagon will soon issue a memo outlining how National Guard will be able use department networks and systems in the states to help foil cyberattacks on the homeland.

The proposed budget released on Tuesday calls for a 10 percent increase in Pentagon spending on cyber operations, for a total of $9.6 billion.

Analysis: The United States has the capability to secretly take out Iran's resources through cyberwarfare, which renders them unable to act offensively. Doing so can deescalate tensions, much like it did this summer when the U.S. stopped Iran's attempts to bomb oil tankers. If Iran were to respond, they know that the United States has shifted its strategy toward retaliation, meaning they're unlikely to attack the United States.

CON: Trump's new offensive strategy is too aggressive

Claim: Trump's new strategy is too aggressive.

Warrant: Trump is going on the offensive.

Farrell, Michael. "Trump is rattling sabers in cyberspace – but is the U.S. ready? Politico. 7/13/19. https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650

A U.S. cyberattack on Iranian military and intelligence targets last month was one of the most prominent signs of the new approach, which comes after a reported effort to implant hostile computer code in Russia's electrical grid and a temporary takedown of a notorious Kremlin-backed troll operation last fall.

To supporters, the tactics are a sign the U.S. may finally be getting out of its defensive crouch in cyberspace — as advocated by hawks such as national security adviser John Bolton.

But the moves also lay the potential groundwork for a tit for tat of cyberattacks that could inflict significant damage on bystanders. Targets such as banks, hospitals, oil companies and electric utilities in the U.S. and elsewhere have already proved vulnerable, as seen in recent criminal hacks that paralyzed entities such as Baltimore's city government.

Now, both Republican and Democratic members of Congress are pressing the White House for details about its offensive cyber strategies, worried that unchecked operations could be dangerously destabilizing for the U.S.

"It's essential that Congress have its ability to conduct proper oversight. It's our constitutional responsibility," Rep. Jim Langevin (D-R.I.) told POLITICO. "I support the administration's plan to be more forward-leaning in cyberspace, on balance. But with

that comes the responsibility to make sure we're not undermining stability in cyberspace."

Langevin added an amendment to the National Defense Authorization Act, which the House passed Friday, to compel the White House to provide details of its new cyber strategy to the House Armed Services Committee. Despite repeated requests from the committee, the administration has not shared a secret presidential directive, National Security Presidential Memorandum 13, that President Donald Trump signed last year to give U.S. Cyber Command more authority to carry out digital attacks.

Warrant: Trump's strategy is overly optimistic

Zegart, Amy. "America's Misbegotten Cyber Strategy." The Atlantic. 2/2/19. https://www.theatlantic.com/ideas/archive/2019/02/trumps-national-cyber-strategy-overly-optimistic/581839/

The DNI's answer: Nuh-uh. In his prepared testimony, Director of National Intelligence Dan Coats made it clear that U.S. intelligence agencies had concluded the U.S. was already losing its edge in emerging technologies, and we'd better get used to it. He even provided a devastating chart with the title "Researchers Worldwide Citing More Foreign and Less US Research," which showed a steeply rising line for Chinese research citations around the world over the past 10 years and a precipitous decline for American citations. The evidence didn't lie. "For 2019 and beyond," Coats wrote, "the innovations that drive military and economic competitiveness will increasingly originate outside the United States, as the overall U.S. lead in science and technology shrinks; the capability gap between commercial and military technologies evaporates; and foreign actors increase their efforts to acquire top talent, companies, data, and intelligence property via licit and illicit means."

The National Cyber Strategy also declared that the U.S. would "preserve peace through strength" in cyberspace by, among other things, encouraging adherence to global cyber

norms. Here, too, this week's DNI testimony put the kibosh on all that hopey-changey talk, making clear that cyber norms have been very much contested by China, Russia, and their autocratic buddies who believe that every country should repress free expression within their own borders and free enterprise from outside them. Not only that, but Team Autocrat seems to be winning through a devious strategy of populating international organizations like the UN with their own countrymen to push their own views of "global norms." In case you missed it, China is now the second-largest contributor to the United Nations budget. "[China] is successfully lobbying for its nationals to obtain senior posts in the UN Secretariat and associated organizations," notes the intelligence threat assessment, "and it is using its influence to press the UN and member states to acquiesce in China's preferences on issues such as human rights and Taiwan."

Warrant: Trump's cyberoffensive is reckless

Wolff, Josephine. "Trump's Reckless Cybersecurity Strategy." The New York Times. 10/2/18. https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html

The Trump administration's shift to an offensive approach is designed to escalate cyber conflicts, and that escalation could be dangerous. Not only will it detract resources and attention from the more pressing issues of defense and risk management, but it will also encourage the government to act recklessly in directing cyberattacks at targets before they can be certain of who those targets are and what they are doing.

One of the advantages of the slow, unwieldy approval processes put into place by previous administrations is that they gave the government ample time to ascertain who was behind a cyberattack. That is not always easy to do: Many adversaries route cyberattacks through compromised third-party machines in other countries, such as university computer systems. Rushing to retaliate may make it more likely that the

United States will lash out at the wrong target, which may invite new attacks rather than deter them.

It could also lead to more attacks from existing adversaries like Russia and North Korea, from whom we already face substantial online threats. These countries have demonstrated their considerable online capabilities in cyberattacks directed at hospitals and power companies. If the United States pre-emptively attacks their servers and online infrastructure, it will only provoke greater and more damaging shows of force. And what these countries are capable of will be every bit as terrifying and harmful as what we can do.

There is no evidence that pre-emptive cyberattacks will serve as effective deterrents to our adversaries in cyberspace. In fact, every time a country has initiated an unprompted cyberattack, it has invariably led to more conflict and has encouraged retaliatory breaches rather than deterring them. Nearly every major publicly known online intrusion that Russia or North Korea has perpetrated against the United States has had significant and unpleasant consequences.

Impact: Trump's strategy leads to escalation

"Global Consequences of Escalating U.S.-Russia Cyber Conflict." Council on Foreign Relations. 4/2/19. https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict

Cyber conflicts involving state actors are quickly becoming a geopolitical reality. Perhaps the most cited example, the alleged Russian interference in the 2016 U.S. election, is a continued source of conflict in U.S.-Russia relations. The story took another turn last October when the U.S. Cyber Command conducted an offensive cyber operation against the Internet Research Agency (IRA), the "Russian troll factory" linked to using disinformation campaigns during the 2016 elections, and onwards. While the operation has yet to be confirmed by the U.S. government, media reports and U.S. officials'

commentary taken together suggest the event occurred. The U.S. action, which took place during the 2018 midterm elections, has been portrayed as a defensive warning against Russia and other U.S. adversaries online. But the result of the offensive operation may, however, in the end benefit Russia and possibly contribute to escalation in the cyber domain globally.

Somewhat unexpectedly, the operation was confirmed by the apparent target. In a public announcement, the Russian Federal News Agency (FNA), which is reportedly tied to the IRA, describes a cyberattack that supposedly caused storage system malfunction, specifically destructively targeting the RAID controller and causing hard drives being formatted. While FNA's credibility is low, the report's claim that the offensive cyber operation resulted in a significant disruption seems undeniable.

Analysis: The United States has entered a new era of cyberwarfare as the Trump administration has announced they're more willing to retaliate and act offensively online. Allowing the Trump administration more control over cyberwarfare has led to concerns that escalation may accelerate, and other countries may respond. President Trump has not been known for his restraint thus far in his term, there's reason to believe he may start some sort of conflict.

A/2: Trump's new offensive strategy is too aggressive

Answer: Trump's strategy creates deterrence

Warrant: Trump is willing to retaliate

"Trump boosting offensive capabilities in cyber strategy." APNews. 9/20/18. https://www.apnews.com/f309d407b5354a6e9104a715911499d7

The White House is warning foreign adversaries that the U.S. is preparing to step up its offensive cyber capabilities as part of a new government-wide strategy.
President Donald Trump on Tuesday is signing a National Cyber Strategy that furthers his lifting of Obama-era constraints on offensive actions.
National Security Adviser John Bolton says, "We're going to do a lot of things offensively," adding, "Our adversaries need to know that."
Bolton says the reason for the new strategy is that "Americans and our allies are under attack every day in cyberspace."
The strategy directs federal agencies to work with state and local governments to shore up government systems, and to coordinate with private-sector companies to address threats.
Bolton says the U.S. is aiming "to create the structures of deterrence" in cyberspace.

Warrant: Trump's strategy makes it easier to respond

Fazzini, Kate. "Trump's new strategy means the U.S. could get more aggressive with Russia and China over hacking." CNBC. 10/21/18. https://www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html

The strategy codifies the ability of agencies aligned with the Department of Defense, like the NSA and military branches, to conduct offensive actions in cyberspace.

This means these agencies will be able to go after the overseas sources of attacks more proactively. These activities can be risky, as cybercriminals may position their attacks from a neutral third party or a non-hostile country, making it more complicated for the U.S. to engage in cyber battles. These back-and-forth attacks can also cause damage to the infrastructure that supports the internet, particularly telecommunications providers.

But NSA leaders have long sought a clear green light to conduct operations meant to counter the scale of those launched by nations like Russia against voting infrastructure and financial institutions; or China, against private corporations and government contractors, targeting intellectual property.

This strategy gets the agency and law enforcement partners closer than ever to being allowed to make these offensive bids, which could include dismantling “botnets” — which are collections of compromised computers and devices used to attack corporate or government targets — underground cyber black markets, or other sources of cyberattacks.

Analysis: Trump’s new cyber strategy is a first step toward creating cyber deterrence. Acting offensively and retaliating against our enemies in cyberspace will dissuade countries like Russia and China who otherwise might choose to attack the US online.

CON: Offensive capabilities have been weaponized against the U.S

Claim: U.S developed weapons have been used against the country.

Warrant: The US develops new technologies

Nakashima, Ellen. "U.S. accelerating cyberweapon research." Washington Post. 3/18/12. https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html

The Pentagon is accelerating efforts to develop a new generation of cyberweapons capable of disrupting enemy military networks even when those networks are not connected to the Internet, according to current and former U.S. officials.

The possibility of a confrontation with Iran or Syria has highlighted for American military planners the value of cyberweapons that can be used against an enemy whose most important targets, such as air defense systems, do not rely on Internet-based networks. But adapting such cyberweapons can take months or even years of arduous technical work.

When U.S. military planners were looking for ways to disable Libya's air defense system before NATO's aerial attacks last year, they discussed using cybertechnology. But the idea was quickly dismissed because no effective option was available, said current and former U.S. officials.

Warrant: Other countries steal our tech

Baker, Sinead. "The US says China is stealing technology to modernize its military, and that could erode American dominance." Business Insider. 5/3/19.

https://www.businessinsider.com/us-accuses-china-steal-military-technology-2019-5

A new Pentagon report said that China uses "cyber theft" and other methods to bolster its military, which the report claims will continue to grow rapidly.
"China uses a variety of methods to acquire foreign military and dual-use technologies, including targeted foreign direct investment, cyber theft, and exploitation of private Chinese nationals' access to these technologies, as well as harnessing its intelligence services, computer intrusions, and other illicit approaches," it said.
One example outlined in the report is from 2018, when China used "dynamic random access memory, aviation technologies, and anti-submarine warfare technologies'" to acquire "sensitive, dual-use, or military grade equipment."

Impact: Stolen tech is used against us

Brewster, Thomas. “Chinese Hacker Crew Stole NSA Cyber Weapons In 2016 – A Year Before They Were Leaked Online.” Forbes. 5/7/19. https://www.forbes.com/sites/thomasbrewster/2019/05/07/chinese-hacker-crew-stole-nsa-cyber-weapons-in-2016--a-year-before-they-were-leaked-online/#6fb3a742237b

A Chinese group of hackers managed to get hold of cyber weapons from the U.S. National Security Agency's arsenal of digital weapons and were using them as far back as 2016.
Researchers at American cybersecurity giant Symantec claimed in a report released Tuesday that a group dubbed Buckeye had used a pair of tools called "Bemstour" and "DoublePulsar," which exploited weaknesses in Microsoft Windows, back in March 2016. Symantec didn't name Buckeye as a Chinese espionage unit, but U.S. government and private industry have previously tied the group to China's intelligence apparatus.

A year later, a group calling itself the Shadow Brokers started releasing versions of tools from a cyber-espionage operator called the Equation Group, which was swiftly revealed to be the NSA. The identity and provenance of the Shadow Brokers remains a mystery.

The researchers were unable to say just how Buckeye stole from the NSA a year before the public Shadow Brokers leak. It could be that the hackers witnessed an NSA attack on a network and put the "artefacts" left on infected computers back together to re-create the American intelligence agency's tools. "Other less supported scenarios, given the technical evidence available, include Buckeye obtaining the tools by gaining access to an unsecured or poorly secured Equation Group server, or that a rogue Equation group member or associate leaked the tools to Buckeye," Symantec wrote.

Impact: China's use of NSA tools hurts the US

Zilbermints, Regina. "Hacking tool responsible for attacks on Baltimore, other cities developed by NSA: report." The Hill. 5/26/19. https://thehill.com/policy/cybersecurity/445612-hacking-tool-responsible-for-attack-on-baltimore-other-cities-developed

A key component of malware used by hackers to disrupt U.S. cities, paralyzing local governments and frustrating residents, was developed by the National Security Agency (NSA), The New York Times reported.

The NSA reportedly lost control of the tool, called EternalBlue, in 2017.

After that, it was used across the globe by hackers in Russia, China and North Korea, according to the Times, which added that it has affected hospitals, airports, shipping operators, ATMs and factories.

More recently, it has been used against a number of U.S. cities, including the recent high-profile ransomware attack on Baltimore in which computers were frozen

and water bills, health alerts, real estate sales and other services were disrupted, the newspaper reports.

On May 7, city workers' screens suddenly locked and a message demanded $100,000 to free the city's files. Baltimore has not paid and almost three weeks later remains affected.

According to the Times, damage from these attacks would be less vast without EternalBlue.

The NSA and FBI declined to comment to the Times, which reported that the NSA still hasn't acknowledged the theft of the cyberweapon or know whether the group responsible, which calls itself the Shadow Brokers, is made up of foreign spies or disgruntled federal employees.

Analysis: The United States is already focused on developing new cyberweapons, but as they create new ones, they're being stolen by nefarious actors. China, for instance, was able to gain access to an NSA tool that spreads malware. The tool was then used against several U.S. cities, including Baltimore and a few others. Developing new weapons without the ability to secure those weapons risks those weapons being used against us once more.

A/2: Offensive capabilities have been weaponized against the U.S

Answer: The U.S. can defend against its own technologies.

Warrant: The US has good cyberdefenses

> "U.S. prepared to strike back against cyberattacks, Pentagon warns." Marketwatch. 3/13/19. https://www.marketwatch.com/story/us-prepared-to-strike-back-against-cyberattacks-pentagon-warns-2019-03-13
>
> Cyberattacks from Russia, China, North Korea and Iran are increasingly sophisticated and, until recently, were done with little concern for the consequences, the top Pentagon cyber leaders told a congressional committee on Wednesday.
> Army Gen. Paul Nakasone, head of U.S. Cyber Command, laid out the escalating threats, following a Navy review released this week that described significant breaches of naval systems and concluded that the service is losing the cyber war.
> Speaking during a subcommittee hearing, Nakasone said the U.S. is now prepared to use cyber operations more aggressively to strike back, as the nation faces growing cyberattacks and threats of interference in the 2020 presidential elections.
> He said the military learned a lot working with other government agencies to thwart Russian interference in the 2018 midterm elections, and the focus now has turned to the next election cycle.
> The Navy report underscored long-known cyber threats from Russia and China that have plagued the U.S. government and its contractors for more than a decade. It said there were "several significant" breaches of classified Navy systems and that "massive amounts" of national security data have been stolen. The report laid out a number of

recommendations to reduce cyber vulnerabilities across the Navy and make cybersecurity a higher priority.

Data has been stolen from key defense contractors and their suppliers, the report said, adding that "critical supply chains have been compromised in ways and to an extent yet to be fully understood." The report, ordered by Navy Secretary Richard Spencer, concluded that while the Navy is prepared to win at conventional warfare, that's not the case for the current cyber war.

Warrant: The US is using a new strategy of deterrence

"Trump boosting offensive capabilities in cyber strategy." APNews. 9/20/18. https://www.apnews.com/f309d407b5354a6e9104a715911499d7

The White House is warning foreign adversaries that the U.S. is preparing to step up its offensive cyber capabilities as part of a new government-wide strategy.

President Donald Trump on Tuesday is signing a National Cyber Strategy that furthers his lifting of Obama-era constraints on offensive actions.

National Security Adviser John Bolton says, "We're going to do a lot of things offensively," adding, "Our adversaries need to know that."

Bolton says the reason for the new strategy is that "Americans and our allies are under attack every day in cyberspace."

The strategy directs federal agencies to work with state and local governments to shore up government systems, and to coordinate with private-sector companies to address threats.

Bolton says the U.S. is aiming "to create the structures of deterrence" in cyberspace.

Analysis: Countries will need to think twice about stealing U.S technology in the future now that Trump's cyber strategy has come into effect. The fear of retaliation on behalf of the United States is enough to deter actors like China from taking U.S cyberweapons in the future.

CON: Offensive capabilities are less important than defensive capabilities

Claim: The U.S should prioritize defensive cyber capabilities instead.

Warrant: The US is unprepared for cyber war.

Sellin, Lawrence. "The US is unprepared for space cyberwarfare." Military Times. 10/4/19. https://www.militarytimes.com/opinion/commentary/2019/09/04/the-us-is-unprepared-for-space-cyberwarfare/

Virtually every aspect of American national security, including the detection of threats, the use of weapons, the deployment of forces and their resupply, is now dependent on the integrity of critical space-based capabilities.

In defense parlance, those systems are known as command, control, communications, computing, intelligence, surveillance and reconnaissance (C4ISR) and integral and expeditionary logistics.

Both our major adversaries, China and Russia, have placed a high priority on developing superiority within the electromagnetic battlespace with already demonstrable capabilities in electronic and cyber warfare.

Cyberattacks on space-based systems can produce data loss, service disruptions, sensor interference or the permanent loss of satellite capabilities. An adversary could potentially seize control of a satellite through a cyberattack on its command-and-control system, subtly corrupt the data it provides, or even redirect its orbit, essentially transforming it into a kinetic weapon against other space infrastructure.

Warrant: Cyber defense is distinct from offense

Slayton, Rebecca. "Why Cyber Operations Do Not Always Favor the Offense." Belfer Center. 2/17. https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense

The assumption that cyberspace favors the offense is widespread among policymakers and analysts, many of whom use this assumption as an argument for prioritizing offensive cyber operations. Faith in offense dominance is understandable: breaches of information systems are common, ranging from everyday identity theft to well-publicized hacks on the Democratic National Committee. A focus on offense, however, increases international tensions and states' readiness to launch a counter-offensive after a cyberattack, and it often heightens cyber vulnerabilities. Meanwhile, belief in cyber offense dominance is not based on a clear conception or empirical measurement of the offense-defense balance.

One useful conception of the cyber offense-defense balance is based on cost-benefit analysis: What is the benefit of offense less the cost of offense, relative to the benefit of defense less the cost of defense? The technological complexity of cyberspace does tend to increase the costs of defense, but the costs of offense and defense are ultimately shaped by the complexity of the goals of offense and defense and organizations' capabilities in managing this complexity. Organizational skill can shift the costliness of cyber operations toward the defense. Further, whereas breaching information systems is easy and can be done at relatively low cost, achieving physical effects is far more difficult and costly. Meanwhile, the benefits of cyber operations are highly situational and subjective. Thus, claims that all of cyberspace is offense dominant obscure crucial differences between distinctive kinds of operations and the ways they are valued; such claims should be avoided. It only makes sense to discuss the offense-defense balance of specific cyber operations with specific goals, between specific adversaries with distinctive capabilities.

Warrant: Defensive focus more strategic

Valeriano, Brandon and Jensen, Benjamin. "The Myth of the Cyber Offense: The Case for Restraint." CATO Institute. 1/15/19. https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

Rather than going on the offensive, the United States should develop a cyber posture that signals restraint and builds an active defense network. This network should adopt key tenets of Julian Corbett's concept of a "fleet-in-being." For Corbett, writing in 1911, the operative strategic problem for the British Empire was securing global interests. Regional adversaries could overwhelm local defenses and achieve fait accompli victories, and the British could not be everywhere at once. They had to adopt a fleet-in-being, a distributed network of cruisers (mobility) and fortified ports (strong points) that increased the costs of adversary aggression, buying time for diplomacy and, should it fail, for mobilizing sufficient forces for a counterattack. This dispersed network signaled resolve and generated options by disputing who could command the seas. A fleet-in-being "endeavor[ed] by active defensive operations to prevent the enemy either securing or exercising control for the objects he has in view." This strategy thus advocated "avoiding decisive action by strategical or tactical activity, so as to keep our fleet-in-being till the situation develops in our favor."67

In cyber operations, the United States requires a global network organized around active defenses rather than offensive actions designed to preempt other great powers. This network requires intelligence sharing and target hardening with partners, including industry, to reduce adversaries' expected benefits of cyber operations. Just as new technologies enabled new theories of victory for Corbett, digital connectivity puts a premium on deception and active defense in cyberspace.

Analysis: Emphasizing offensive operations at a time when the United States is woefully underprepared to defend itself in cyberspace is a poor choice. Offensive and defensive cyber

operations are completely distinct, and if the U.S. has to choose one focus, it should clearly be defense. Adopting a defensive mindset will allow the U.S to defend itself on a global scale through alliances and preemption.

A/2: Offensive capabilities are less important than defensive capabilities

Answer: The best defense is good offense.

Warrant: Trump is planning new retaliation strategies.

Thomsen, Jacqueline. "Trump's new cyber approach: The best defense is a good offense." The Hill. 9/23/18. https://thehill.com/policy/cybersecurity/407861-trumps-new-cyber-approach-the-best-defense-is-a-good-offense

The Trump administration's new cyber strategy is raising questions about the U.S. role in offensive cyberattacks.

The document itself, unveiled Thursday, largely consists of existing practices and policies dealing with defensive measures. But national security adviser John Bolton told reporters that the U.S. will now act more aggressively in cyberspace, a move that could both deter cyberattacks and expose the country to new vulnerabilities, according to some cyber experts.

Bolton on Thursday confirmed reports that Trump had rescinded Obama-era guidance on how to handle cyberattacks by signing a replacement policy, one that puts the U.S. on offense.

Cyber experts and Obama-era officials said they agree that a fresh policy is needed, but they also have reservations about the Trump administration putting an emphasis on the offense component.

They warned against the dangers of taking this new approach too far: Federal government actions could set a precedent for what is considered to be acceptable behavior. And while the U.S. already faces cyberattacks on a daily basis, the new

aggressive posture means it could end up the victim of the same kinds of attacks it ends up carrying out.

Warrant: Trump will retaliate against attackers

Thomsen, Jacqueline. "Trump's new cyber approach: The best defense is a good offense." The Hill. 9/23/18. https://thehill.com/policy/cybersecurity/407861-trumps-new-cyber-approach-the-best-defense-is-a-good-offense

The Obama administration often responded to cyberattacks with sanctions against other countries. For example, after the U.S. intelligence community determined that Russia had interfered in the 2016 election, then-President Obama imposed sanctions against the country and expelled Russian diplomats from the U.S.

The administration's new strategy doesn't specify what offensive attacks are fair game; instead, it says "instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States."

The authorized actions are apparently included in a directive signed by the president in recent weeks, the same order that rescinded the Obama-era guidance which required several federal departments and agencies to be consulted before any adversarial actions are carried out. That directive is not public.

Ari Schwartz, who was senior director for cybersecurity in the Obama White House, told The Hill that from his conversations with people familiar with the document, it appears that Trump's approach involves soliciting feedback from federal agencies on potential cyber actions on a case-by-case basis, rather than requiring that specific agencies be involved in each decision.

Analysis: Without the ability to retaliate and go on the offensive, there's no way for the United States to deter its adversaries in cyberspace. The Trump administration's decision to go on the offensive with new technologies will bolster the United State's cyber defenses by dissuading potential attackers before they strike.

CON: Offensive operations will hurt U.S. business

Claim: Offensive operations will lead to retaliatory cyber attacks. Small businesses are likely to be targeted because they can't afford expensive cyber security. These attacks will hurt the economy.

Warrant: Offensive operations will lead to retaliation.

Greenberg, Andy. "How Not To Prevent a Cyberwar With Russia." Wired, WIRED, 18 June 2019, www.wired.com/story/russia-cyberwar-escalation-power-grid/. Accessed 7 Oct. 2019.

After all, Russia's hackers have already demonstrated perhaps the world's most aggressive targeting of foreign electric utility networks, triggering blackouts in Ukraine in 2015 and 2016, and gaining deep access to American utilities' industrial control systems in 2017. **"The idea that we're going to put implants in the Russian grid and they won't do the same to us is silly,"** Daniel says, while emphasizing that, like Bossert, he has no independent knowledge of such activities beyond the Times' story. **Even the notion of trying to deter Russia by hacking their grid to the same degree that they've hacked ours introduces serious potential for unintended consequences.** "If the argument is that we're going to hold each other's grids at risk, and that's inherently more stabilizing, I'm not sure the theory holds entirely. I think the possibility for accidents and miscalculation is high here."

Warrant: Cyber operations are unstable and could hurt U.S. business.

Marks, Joseph. "Analysis | The Cybersecurity 202: Trump Gave the Military Freer Rein for Offensive Hacking. Security Experts Say That's a Good Idea." The Washington

Post, 11 Feb. 2019, www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/11/the-cybersecurity-202-trump-gave-the-military-freer-rein-for-offensive-hacking-security-experts-say-that-s-a-good-idea/5c607a571b326b66eb098678/. Accessed 5 Oct. 2019.

The military acting alone might be unaware of unintended consequences those operations might produce, they warned, such as hurting U.S. businesses or undermining intelligence operations. "Cyber operations are inherently unstable. They are hard to contain and constrain. Their use has implications beyond their immediate effects," said Bruce Schneier, fellow and lecturer at the Harvard Kennedy School. "For this reason, many more equities need to be involved in decisions to use cyberweapons than for ordinary military operations.

Warrant: Every organization is at risk of being hacked.

Manship, Ryan. "The Top 6 Industries At Risk For Cyber..." RedTeam Security, RedTeam Security, 2 Jan. 2019, www.redteamsecure.com/the-top-6-industries-at-risk-for-cyber-attacks/. Accessed 7 Oct. 2019.

Thinking "it won't happen to us" is one of the biggest mistakes a business can make when it comes to cybersecurity. **Every organization is at risk of data breach, systems hack, malware or ransomware attack, or the cybercriminal illicitly accessing their network's processing power.** Yet for the high-target industries we'll talk about below, there's an even higher risk profile and specific types of threats that businesses within these industries need to prepare for and protect against.

Warrant: Small businesses are vulnerable to attacks.

Walker, Ivy. "Cybercriminals Have Your Business In Their Crosshairs And Your Employees Are In Cahoots With Them." Forbes, 28 June 2019, www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#23636bee1953. Accessed 7 Oct. 2019.

The lost revenue due to downtime, the cash spent attempting to remediate the breach and the reputational damage can really add up. **Despite these stark facts, most small business owners aren't prepared to prevent, detect or respond to a cyber attack.** "The threat environment is active and intense," says Cyrus Walker, Managing Principal at Data Defenders, a cybersecurity advisory, response and managed services provider. "**A cybercriminal has a much greater opportunity for success in attacking a small business because small businesses are very weak in their security countermeasures."**

Impact: Cyber attacks force firms to go out of business.

Walker, Ivy. "Cybercriminals Have Your Business In Their Crosshairs And Your Employees Are In Cahoots With Them." Forbes, 28 June 2019, www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#23636bee1953. Accessed 7 Oct. 2019.

A cyber attack can put you out of business because the cost of cleaning up after a breach can be considerable. In fact, according to Malwarebytes, a global provider of malware prevention and remediation solutions, **ransomware attacks caused nearly a quarter of small and medium-sized businesses hit by them in 2017 to completely halt operations. Recent statistics show that around 60% of SMBs forced to suspend operations after a cyber attack never reopen for business.** The lost revenue due to

downtime, the cash spent attempting to remediate the breach and the reputational damage can really add up.

Impact: Cyber attacks damage business' reputations by breaching customer privacy.

dcomisso. "Impact of Cyber Attack on Your Business." Nibusinessinfo.Co.Uk, 7 Mar. 2019, www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business.

Trust is an essential element of customer relationship. **Cyber attacks can damage your business' reputation and erode the trust your customers have for you. This, in turn, could potentially lead to: loss of customers, loss of sales, reduction in profits.** The effect of reputational damage can even impact on your suppliers, or affect relationships you may have with partners, investors and other third parties vested in your business.

Analysis: This argument can be weighed on probability. It's very likely perpetrators of cyber attacks would target small business because of their vulnerabilities, whereas arguments about things like nuclear infrastructure—which have much more heightened security—could be construed as a bit of a stretch.

A/2: Offensive operations will hurt U.S. business

Answer: Offensive operations help combat cyber attacks on business.

Warrant: The Trump administration's cyber strategy is a way to beat back against cyber attacks that hurt the economy.

Vavra, Shannon. "U.S. Ramping up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says." CyberScoop, CyberScoop, 11 June 2019, www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/. Accessed 7 Oct. 2019.

While these kinds of "defending forward" operations continue, according to military cybercommanders, **the administration is also moving to address economic concerns.** The urgency of addressing Chinese hacking is increasing because that activity has expanded to the point that it can "degrade core U.S. operational and technological advantages," according to the Pentagon. **Bolton's remarks Tuesday mark the first time a senior White House official has publicly acknowledged that the authorizations issued last year go beyond just election contexts. He warned adversaries that the U.S. reserves the right to retaliate to economically-motivated cyberattacks**, even outside of the cyber realm.

Warrant: Offensive operations are the most effective approach for organizations to protect themselves.

"The Future of Cybersecurity: The Best Defense Is a Good Offense." Boozallen.Com, 2019, www.boozallen.com/s/insight/blog/future-of-cybersecurity.html. Accessed 7 Oct. 2019.

> In today's unpredictable environment, filled with rapidly evolving threat actors and emerging technologies, **the only way organizations can protect themselves is by unleashing offensive cyber techniques to uncover advanced adversaries on their networks. The most effective approach—Threat hunting—is essential to any organization that wants to stop and prevent attacks in its networks.** Advanced adversaries live in the noise of networks and defeat reactive, rule-based cybersecurity defenses by constantly developing malicious tactics, techniques, and procedures (TTPs). These developments—such as polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and hijacking legitimate operating system functions—all evade traditional defenses.

Analysis: This response can be framed as a turn. Trump's offensive policy may deter attackers rather than emboldeing them. Pro teams can then weigh on risk of solvency, since they are the only team offering a solution to these cyber attacks.

Anwer: Businesses are already being targeted in the status quo.

Warrant: Iranian hackers are targeting U.S. companies.

> Marks, Joseph. "Analysis | The Cybersecurity 202: U.S. Businesses Are Preparing for Iranian Hacks after American Cyberattack." The Washington Post, 24 June 2019, www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/06/24/the-cybersecurity-202-u-s-businesses-are-preparing-for-iranian-hacks-after-american-cyber-attack/5d1007a81ad2e552a21d507f/. Accessed 7 Oct. 2019.

> U.S. businesses should get ready for a barrage of digital retaliation from Iran after the Trump administration launched a cyberattack against the Islamic Republic's rocket and

missile launching systems, current and former U.S. government officials said this weekend. **Iranian hackers are already targeting U.S. companies with specialized malicious software designed to wipe the contents of their computer networks rather than to simply steal their data, Chris Krebs, director of the Homeland Security Department's cybersecurity division, warned in a Saturday email.** And cybersecurity companies — which were already clocking a dramatic increase in Iranian hacking during the past few weeks — began warning this weekend that the nation could increase its attacks and make them far more destructive.

Warrant: 15% more U.S. businesses experienced cyber attacks this year than last year.

"Is Your Business Prepared for a Cyber Attack?" Hiscox, 14 Aug. 2019, www.hiscox.com/blog/your-business-prepared-cyber-attack. Accessed 7 Oct. 2019.

Among U.S. businesses, 53% experienced a cyber attack in the last year, up significantly from the 38% who reported an attack the previous year. Over a quarter (27%) of companies experienced four or more attacks in the past 12 months. The average cost of a single cyber attack in the U.S. is $73,000. The cost for all attacks suffered by the average U.S. business in the past 12 months is $119,000.

Analysis: This response makes the con's argument non unique. It doesn't matter that offensive operations would slightly increase attacks on businesses when this is already the current trend. Clearly other factors, besides this cyber policy, are contributing to an increase in attacks.

CON: Offensive operations lead to retaliation

Argument: Offensive operations are more threatening than defensive operations, which will prompt leaders to retaliate against the U.S. in order to save face. This tit-for-tat mentality can quickly escalate into cyber war.

Warrant: A preemptive or disproportionate attack could easily escalate.

> Greenberg, Andy. "How Not To Prevent a Cyberwar With Russia." Wired, WIRED, 18 June 2019, www.wired.com/story/russia-cyberwar-escalation-power-grid/.
>
> But security wonks tend to agree, at least, that **there's one way not to prevent a cyberwar: launching a preemptive or disproportionate cyberattack on an opponent's civilian infrastructure. As the Trump administration increasingly beats its cyberwar drum, some former national security officials and analysts warn that even threatening that sort of attack could do far more to escalate a coming cyberwar than to deter it.** Over the past weekend, The New York Times reported that US Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. But judging by Russia's response, news of the grid-hacking campaign may have already had the immediate opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries, even as it claimed that Russia's grid was immune from such threats.

Warrant: Russia's threshold to launch escalatory cyber attacks is low because it feeds into government officials' anti-West narrative.

Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare*. Center for Naval Analyses, Sept. 2016. https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf.

While Russian cyber tactics appear to be evolving, the theoretical and doctrinal underpinnings of Russia's approach to cyber warfare have remained more or less constant. **Russian officials are convinced that Moscow is locked in an ongoing, existential struggle with internal and external forces that are seeking to challenge its security in the information realm.** Globalization, along with the free flow of information it engenders, is viewed as both a threat and an opportunity in this regard. Russian information warfare doctrine—which encompasses cyber along with other, more traditional tools for shaping the information space—blurs the separation between peacetime and wartime. **Cyber operations that in a U.S. context might require Title 10 authorizations and authorities are more likely to be employed by the Russians in a pre-conflict scenario or even peacetime when their capacity to affect a strategic outcome is viewed as more advantageous. This suggests that the Kremlin has a relatively low bar for employing cyber in ways that U.S. decisionmakers are likely to view as offensive and escalatory in nature.**

Warrant: U.S. attacks could trigger a response on a previously unseen scale.

Olejnik, Lukasz. "Global Consequences of Escalating U.S.-Russia Cyber Conflict." Council on Foreign Relations, 2019, www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict.

Domestically, Russia is currently already in the process of isolating its networks from the outside internet. Russia's official justification for the action is to lower the risk of external cyberattacks; however, in reality the goal is to increase control over the networks, including strict traffic filtering, reminiscent of the China's Great Firewall.

While Russia's narrative rings hollow, U.S. reports of cyberattacks on Russia may be exploited internally to justify the changes. **There is also the danger of a retaliation. While Russia could simply limit its response to a diplomatic message, the standard previously followed by the United States, escalation in response to the November action might follow, potentially on a previously unseen scale.** Intensifying cyber conflict would not only seriously impact national security, but also increase geopolitical risk for businesses.

Warrant: U.S. infrastructure is far more vulnerable than Russia's.

Greenberg, Andy. "How Not To Prevent a Cyberwar With Russia." Wired, WIRED, 18 June 2019, www.wired.com/story/russia-cyberwar-escalation-power-grid/.

But former White House cybersecurity officials caution against that cyberwar hawkishness. **"The idea that we can use cyber offense capabilities to impose sabotage-like effects, and to do so in increasingly large scale and costly ways until they get it through their head that they can't win, I don't think that's going to work,**" says Tom Bossert, who served as White House homeland security advisor and the president's most senior cybersecurity-focused official until April of last year. "I want to make sure we don't end up in an escalatory cyber exchange where we lose more than they do." **Bossert points out that in many respects the US economy and infrastructure is far more reliant on digitization and automation than Russia's, giving the Kremlin an inherent advantage in any future no-holds-barred cyberwar.** He paraphrases former secretary of defense Ash Carter: "If you're doused in gasoline, don't start a match-throwing contest."

Impact: A cyber attack would put critical infrastructure at risk.

LaFrance, Adrienne. "When Is Cyberwar Just War?" *The Atlantic*, 16 May 2017, www.theatlantic.com/technology/archive/2017/05/cyberwar-is-officially-crossing-over-into-the-real-world/526860/.

The devastating effects of a massive cyberattack are no more confined to a computer network than any other action carried out online. People use the computers and the internet all the time to make things happen in the physical world. **A cyberattack isn't just a cyberattack. It's an attack. Hospitals, pharmacies, and major corporations like FedEx and the Spanish telecommunications giant Telefonica were among the 200,000 victims hobbled by a global ransomware attack on Friday, which locked people's computers and demanded Bitcoin payment in exchange for access. In the United Kingdom, some hospitals canceled procedures and other appointments as a result.** The software security firm Symantec found that people paid ransoms totaling about $54,000 in the attack, though officials strongly caution against paying such ransoms.

Impact: The potential for more destructive cyberwar would lead to tension and fear on par with the Cold War.

Lindsey, Nicole. "The Rise of the Global Cyber War Threat." *CPO Magazine*, 31 July 2019,www.cpomagazine.com/cyber-security/the-rise-of-the-global-cyber-war-threat/.

Stratfor, for example, has described a "hair-trigger" world in which the most powerful cyber nations could unleash war on each other with lightning speed and with no advance warning. A massive attack on one nation's power grid might lead to a tit-for-tat attack on the electrical grid of the other. And, **to avoid this scenario of having to hit back hard after already being hit, a nation like the United States might decide to develop a "first strike" capability. This would be tantamount to being able to let fly hundreds of intercontinental nuclear weapons, all at the same time, in order to**

destroy a nation before it ever has a chance to respond. As a result, the next generation might grow up under the constant risk of a cyber attack taking down the national energy grid, in the same way that generations before lived with the constant risk of nuclear war.

Analysis: Con teams running this argument should provide nuanced warrants about how offensive operations would change our adversaries' propensity for conflict in cyberspace. Pro teams will likely also impact to cyberwar, so strong warranting coupled with link weighing will be necessary to come out on top. For example, con teams can make the analysis that authoritarian leaders like Putin—who derive their legitimacy from rallying around the flag and using the West as a scapegoat—are more likely to retaliate than sit idly by.

A/2: Offensive operations lead to retaliation

Answer: Mutually Assured Destruction in cyberspace will prevent retaliation.

Warrant: Credible U.S. threats would deter adversaries from launching attacks.

Gale, David, et al. "Cybermad: Should the United States Adopt a Mutually Assured Destruction Policy for Cyberspace?" Air University, Apr. 2009.

The nuclear MAD doctrine is credited with preventing the Cold War from turning hot, since neither side could expect to survive a full scale nuclear exchange. Although the loss of cyberspace might not rise to this level, the doctrine still applies. **If the US can credibly vow to destroy cyberspace, thus destroying world economies, the US can deter an adversary from launching an attack.** Critics may correctly argue that CyberMAD's deterrent effect is limited, since it will not deter non-state actors. However, nuclear MAD doctrine never deterred non-state actors. Critics will also argue that the lack of attribution will limit CyberMAD. Although true, it allows us to focus on developing the capability. We should not throw out the doctrine. We should develop the capability.

Warrant: Cyber attacks are inevitable, so the best option is Mutually Assured Destruction.

Crosston, Matthew. World Gone Cyber MAD How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. Strategic Studies Quarterly, 2011.

Most analysts, military specialists, and government officials admit that **life in the twenty-first century will include cyber attacks. There is no vision of a world free from**

such attacks. This simple admission undermines the efficacy of a cyber deterrence system whose reason for being is the prevention of such attacks. This article is not so contrarian as to argue anarchically for abandonment of the effort to achieve real cyber security. Rather it asks that certain structural realities finally be given equal intellectual space at the discussion table and allow that space to entertain new options and possibilities. There are two structural realities in particular that should be emphasized. First, in the cyber realm offense always dominates and always will. It is structural and axiomatic. Second, the capabilities, technology, and talent already exist to institute this system within the United States.What is needed is a change in mind-set and encouraging new ideas and policies—transparently. Not easy by any means, but still achievable. **The imposition of a cyber-MAD policy could prove more effective, even though it may make the United States uncomfortable politically and diplomatically.** The debate continues and the argument remains: greater cyber security can be achieved by mutually assured debilitation for all.

Analysis: With this response, pro teams can cast severe doubt on the idea that our adversaries would be so easily willing to retaliate against the most powerful country in the world. This response is strategic because it can act as terminal defense, taking out the con's argument at the top of their link chain.

Answer: The threat of cyberwar is heavily overblown.

Warrant: Security companies over exaggerate the threat of cyberwar to increase profits.

WIRED Staff. "Cyberwar Hype Intended to Destroy the Open Internet." *WIRED*, Mar. 2010, www.wired.com/2010/03/cyber-war-hype/.

Security companies have long relied on creating fear in internet users by hyping the latest threat, whether that be Conficker or the latest PDF flaw. And now they are

reaping billions of dollars in security contracts from the federal government for their PR efforts. But the industry and its most influential voices need to take a hard look at the consequences of that strategy and start talking truth to power's claims that we are losing some non-existent cyberwar.

Warrant: Warnings and threats have been empty in the past.

WIRED Staff. “Is the Hacking Threat to National Security Overblown?” *WIRED*, 3 June 2009, www.wired.com/2009/06/cyberthreat/.

Poulsen called the threat of cyber-terrorism "preposterous," citing the long-standing warnings that hackers would attack the power grid — despite the fact that it has never happened. And he argued that calling such intrusions national security threats means information about attacks gets classified unnecessarily. If we can't publicly share info that the attackers already have — since it's about them — then we are doing far more harm than good," Poulsen said, arguing that classification makes it impossible for the security community at large to analyze or prepare defenses for such attacks.

Analysis: By casting the the threat of cyberwar as unrealistic fear mongering, pro can severely mitigate the con’s impacts. Just be careful not to contradict yourself; this response relies on the pro running an argument that doesn’t also impact to cyber war.

CON: Offensive operations put nuclear infrastructure at risk

Argument: U.S. offensive operations normalize similar attacks, increasing the likelihood that nuclear infrastructure becomes targeted.

Warrant: Offensive operations normalize the militarization of cyberspace.

Groll, Elias. "The U.S.-Iran Standoff Is Militarizing Cyberspace." Foreign Policy, 27 Sept. 2019, foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/.

But experts in cyberwarfare worry that **the administration's apparent eagerness to rely on digital weapons to strike back against Tehran for a missile and drone attack that briefly ground Saudi oil output to a halt carries with it a great risk: normalizing the militarization of cyberspace. The risk is twofold. The United States and its massive digital economy would be exposed to attack—with more vulnerabilities than most other countries. And Washington would be lowering the bar for engaging in a new domain of warfare, exposing the broader digital economy to new types of threats. With the United States making cyberweapons a larger part of its military arsenal, such attacks are becoming a routine feature of the ways that countries interact with one another in cyberspace.** And that has even veterans of U.S. hacking units worried. "The normalization of destructive attacks is what concerns me," said Jake Williams, the founder of the cybersecurity firm Rendition Infosec and a veteran of the U.S. National Security Agency's elite hacking corps.

Warrant: Nuclear facilities are vulnerable to a cyber attack.

Sadam, Syed, and Hussain Shah. *Offensive Cyber Operations and Nuclear Weapons*. Center for Strategic and International Studies, Mar. 2019. https://csis-

prod.s3.amazonaws.com/s3fs-public/190313_Shah_OffensiveCyber_pageproofs2.pdf. Accessed 6 Oct. 2019.

Nuclear and military organizations rely heavily on computers, making themselves vulnerable to a cyber-attack. Nuclear Command and Control (NC2) plays a critical role in ensuring that weapons are readily available when needed by the national leadership but are not used inadvertently or accidentally. **But what if these systems are compromised? How would decisionmakers communicate? What if weapons are launched in an unauthorized fashion? And what if hackers reveal the sensitive information related to individuals working on nuclear matters or the nuclear facilities command and control locations and so on? These are the threats to nuclear systems posed by offensive cyber operations (OCOs).** Max Smeets defined OCOs as "computer activities to disrupt, degrade, and or destroy."

Warrant: Even small vulnerabilities in the system can lead to catastrophic consequences.

Sadam, Syed, and Hussain Shah. *Offensive Cyber Operations and Nuclear Weapons*. Center for Strategic and International Studies, Mar. 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/190313_Shah_OffensiveCyber_pageproofs2.pdf. Accessed 6 Oct. 2019.

System-level access in an air-gapped network at a nuclear facility could allow a hacker to cause a radiological accident or crash the reactor process by raising or lowering pressure, resulting in mass causalities and loss of the facility. Nuclear organizations require thousands of computers for their operations, and even a single vulnerability can lead to severe consequences. Missile guidance systems, communications systems, nuclear submarines, and many other critical C3 systems are connected to computers and thus vulnerable to cyberattack, which may result in an inadvertent escalation.

Warrant: Almost half of countries with nuclear facilities don't have regulations for cyber security.

Stoutland, Page. "Cyberattacks on Nuclear Power Plants: How Worried Should We Be? | NTI." *Nti.Org*, 2 Oct. 2019, www.nti.org/analysis/atomic-pulse/cyberattacks-nuclear-power-plants-how-worried-should-we-be/. Accessed 7 Oct. 2019.

The good news is that the safety and security of nuclear facilities is taken very seriously. In the United States, cyber security at nuclear facilities is receiving increased attention from regulators, plant operators and technical experts. In addition, as the United States has an aging nuclear infrastructure, many of the plants are still operating mostly with analog controls and/or safety systems, meaning they are less vulnerable to cyberattacks. **Unfortunately, this attention to the cyber threat does not exist everywhere. A 2016 NTI study found that nearly half of the countries with relevant nuclear facilities had no regulations for cyber security at those facilities.** Looking forward, there are a number of concerning signs. As recent attacks have confirmed, cyberattacks are getting increasingly sophisticated. Complex attacks are no longer just the purview of nations but can now be conducted by smaller groups. Furthermore, systems which may have been analog at one time are increasingly digital and increasingly complex. The growing Internet-of-Things will present additional challenges.

Impact: An attack could damage a nuclear reactor and release radiation.

Stoutland, Page. "Cyberattacks on Nuclear Power Plants: How Worried Should We Be? | NTI." *Nti.Org*, 2 Oct. 2019, www.nti.org/analysis/atomic-pulse/cyberattacks-nuclear-power-plants-how-worried-should-we-be/. Accessed 7 Oct. 2019.

The New York Times reported last week on a U.S. government report accusing Russia of conducting a series of cyberattacks aimed at U.S. and European nuclear power plants and water and electric systems from 2015 through 2017. In addition to attacks on water

and electric plants, publicly available evidence suggests that Russia infiltrated the business systems of the Burlington, Kan., Wolf Creek nuclear plant but not the plant's control systems. It was not clear whether the goal of the attack was to conduct reconnaissance or, more seriously, some type of sabotage. **Needless to say, any type of attack on a nuclear plant is very concerning. An attack that allows hackers to manipulate the systems that control a nuclear reactor, while very difficult, could have very serious consequences, including potentially nuclear reactor core damage and off-site release of radiation.** This is not the first time that nuclear facilities have been attacked. The most well-known example is the Stuxnet attack on Iran's uranium enrichment facility, generally attributed to the U.S. and Israel (for a summary of attacks on nuclear facilities, click here. Very recently, a new piece of dangerous malware, TRISIS, which specifically targets the industrial controllers used for safety critical applications, including in nuclear plants, has been found in the Middle East.

Impact: Radiation released from nuclear accidents is lethal.

"What Does Radiation from a Nuclear Disaster Actually Do to Our Bodies?" ABC News, 22 Apr. 2016, www.abc.net.au/news/science/2016-04-22/what-nuclear-radiation-does-to-your-body/7346324. Accessed 7 Oct. 2019.

So long-term exposure to low doses of radiation increase the odds of getting cancer, while a single high dose will quickly cause immediate damage to cells and tissues — a process used effectively to kill tumour cells in radiation therapy. **Very high doses like those experienced by workers at the site of nuclear accidents (several thousand times higher than the background radiation level) cause extensive damage, resulting in a range of symptoms known collectively as radiation sickness. Extremely high doses can kill in days or weeks.**

Analysis: This argument can be weighed on magnitude. A successful cyber attack on a nuclear plant would cause far more harm than other types of attacks. It also has a high probability because even a small attack on a nuclear plant could cause destruction on a mass scale through the release of radiation.

A/2: Offensive operations put nuclear infrastructure at risk

Answer: Nuclear plants are well-protected from cyber attacks.

Warrant: Safety and control systems for nuclear reactors aren't connected to the internet.

Conca, James. "Russia Hacks Into U.S. Power Plants, But Nuclear Reactors Should Be Impervious." Forbes, 17 Mar. 2018, www.forbes.com/sites/jamesconca/2018/03/16/russia-hacks-into-u-s-nuclear-power-plants/#59e47a1d57b9. Accessed 7 Oct. 2019.

As we've discussed before, a recent joint report from the DHS and the FBI says, 'There is no indication of a threat to public safety [from hacking of our nuclear plants] as any potential impact appears to be limited to administrative and business networks.' **America's nuclear plants are one of the best protected of all systems from possible cyber threats. The safety and control systems for our nuclear reactors and other vital plant components are not connected to business networks or the Internet. We learned a lot from Stuxnet, the malicious computer worm that substantially damaged Iran's nuclear program.** John Keeley of the Nuclear Energy Institute says no reactors operating in the United States have been affected by this hacking.

Warrant: It's more difficult to attack nuclear control systems than those of other industrial facilities.

Greenberg, Andy. "Hackers Targeted a US Nuclear Plant (But Don't Panic Yet)." Wired, WIRED, 7 July 2017, www.wired.com/story/hack-brief-us-nuclear-power-breach/. Accessed 7 Oct. 2019.

But the attacks are a long way from the ones actually used to turn out the lights in Ukraine, says Lee. The Times and Bloomberg reports go so far as to consider the possibility that heat-dispersing nuclear safety equipment could be disabled or that equipment could be permanently destroyed. **But the threat of a nuclear disaster caused by the hackers shouldn't be overblown, Lee says. Based on years of security assessments of critical infrastructure utilities, he admits that the notion of an "air gap"—a separation between sensitive systems and internet-connected ones—is often illusory. In nuclear plants, by contrast, he says that disconnection is far stricter. "In nuclear environments, they have an air gap," says Lee. That means that to jump from the corporate network, which these hackers reportedly probed, to the critical control systems would be far more difficult than in other industrial facilities.** None of that changes the fact that attacks on US power facilities represent a dangerous harbinger. But Lee argues the recent incidents are still too far from actual harm to infrastructure to warrant panic or overreaction. The hacker blackouts in Ukraine may show what's on the horizon for the US. But that future hasn't arrived just yet.

Analysis: This response severely mitigates the probability of the con's link. Policymakers recognize that the impact of a nuclear cyber attack would be catastrophic—and because of this have put the appropriate cautionary measures in place to prevent such an attack from occurring.

Answer: Before offensive attacks by the U.S. were on the table, hackers still targeted nuclear facilities.

Warrant: Cyber nuclear espionage has grown considerably over the last two decades.

Futter, Andrew. Hacking the Bomb: Nuclear Weapons in the Cyber Age. University of Leicester, 2015. https://www2.le.ac.uk/departments/politics/people/afutter/copy_of_AFutterHackingtheBombISAPaper2015.pdf. Accessed 6 Oct. 2019.

Cyber nuclear espionage is a significant problem that has grown considerably over the past two decades and clearly has implications not just for proliferation of nuclear knowhow, but also for the efficacy of systems (nuclear and non-nuclear) in any future crisis scenario. Given the enormous amounts of data involved, it is most likely that this problem can really only be managed rather than eradicated.

Warrant: In 2017 hackers penetrated networks that operate nuclear facilities.

Perlroth, Nicole. "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say." The New York Times, 6 July 2017, www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html. Accessed 7 Oct. 2019.

Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

Analysis: This response makes the con's argument non unique. Pro teams should argue that offensive operations will not be the action that leads to the targeting of nuclear facilities when such hacking already happens in the status quo.

CON: Offensive operations increase chance of miscalculation

Argument: Offensive operations are more likely than defensive operations to be perceived as an all-out attack. This increases the chance that signals are misinterpreted and conflicts unintentionally escalate.

Warrant: The Trump administration has been vague about their offensive operations, which increases the chance for miscalculation.

> "The Pentagon's New Cyber Strategy: Defend Forward." Lawfare, 2 Oct. 2018, www.lawfareblog.com/pentagons-new-cyber-strategy-defend-forward.
>
> At this point **defend forward remains a vague concept**, but suffice it to say that the administration is—purposely or not—provoking a strategic dialogue on digital sovereignty and nations' right to self defense in cyberspace. **The United States must not lose sight, however, of the ultimate goal: deterrence. In this respect, ambiguity only increases the prospect for miscalculation and misunderstanding. Transparency, on the other hand, breeds credibility.**

Warrant: Similar miscalculation that occurred during the Cold War could happen with a cyber attack.

> Straub, Jeremy. "Hackers Could Kill More People Than a Nuclear Weapon." Livescience.Com, Live Science, 27 Aug. 2019, www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html.
>
> In another situation, a nation or a terrorist organization could unleash a massively destructive cyberattack — targeting several electricity utilities, water treatment facilities or industrial plants at once, or in combination with each other to compound the

damage. **Perhaps the most concerning possibility, though, is that it might happen by mistake. On several occasions, human and mechanical errors very nearly destroyed the world during the Cold War; something analogous could happen in the software and hardware of the digital realm.**

Warrant: Noncyber responses establish stability; cyber responses can lead to miscalculation.

Healey, Jason. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” Journal of Cybersecurity, vol. 5, no. 1, 1 Jan. 2019, academic.oup.com/cybersecurity/article/5/1/tyz008/5554878/, 10.1093/cybsec/tyz008.

There may be great advantages to the USA in following a strategy of persistent presence. **But there are also opportunities for mistake, misperception, and miscalculation. 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, the USA may only be able to establish stability through noncyber 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.

Warrant: Russia could misinterpret U.S. actions as preparing to cause a Russian blackout.

Greenberg, Andy. “How Not To Prevent a Cyberwar With Russia.” Wired, WIRED, 18 June 2019, www.wired.com/story/russia-cyberwar-escalation-power-grid/.

"The idea that we’re going to put implants in the Russian grid and they won't do the same to us is silly," Daniel says, while emphasizing that, like Bossert, he has no independent knowledge of such activities beyond the Times' story. **Even the notion of**

trying to deter Russia by hacking their grid to the same degree that they've hacked ours introduces serious potential for unintended consequences. "If the argument is that we're going to hold each other's grids at risk, and that's inherently more stabilizing, I'm not sure the theory holds entirely. I think the possibility for accidents and miscalculation is high here." One very plausible miscalculation would be if US Cyber Command were to penetrate Russian grid networks only to "prepare the battlefield," building the capability to cause a blackout in Russia with no immediate intention to do so, but Russians misinterpreted the intrusion as an immediate threat. Georgetown University professor Ben Buchanan calls this dangerous ambiguity "the cybersecurity dilemma" in his book by the same name.

Impact: Miscalculation can lead to targeting of critical infrastructure and deaths.

Palmer, Danny. "Cyberwar: What Happens When a Nation-State Cyber Attack Kills?" ZDNet, ZDNet, 19 Jan. 2019, www.zdnet.com/article/cyberwar-what-happens-when-a-nation-state-issued-cyber-attack-kills/.

"The problem is **the risk of miscalculation is huge," he said, speaking at a security conference in London last month. "If you start to tamper with industrial control systems, if you start to tamper with health systems and networks, it feels like it's only a matter of time before somebody gets hurt and somebody is ultimately killed.**" The mention of health systems is a reminder perhaps of last year's WannaCry ransomware outbreak, which crippled large parts of the UK's National Health Service. **Thousands of appointments were cancelled, causing disruption and inconvenience for patients around the country**. No critical systems were hit, but given the nature of WannaCry -- which the US, UK, and others have blamed on North Korea -- that was likely due to luck rather than planning. **With attacks against hospitals, transport, power plants, or other critical national infrastructure, attackers are playing a dangerous game** -- but that hasn't stopped clandestine, targeted campaigns against infrastructure.

Impact: A cyber attack on the military would be disastrous.

> Donnelly, John M, et al. "America Is Woefully Unprepared for Cyber-Warfare." Roll Call, 11 July 2019, www.rollcall.com/news/u-s-is-woefully-unprepared-for-cyber-warfare.
>
> The Defense Science Board, meanwhile, has delivered a similar message, recommending in 2017 that a second U.S. military that is truly cyber-secure be created as soon as possible, because the one America has will not necessarily work. **A cyberattack on the military, the science board said, "might result in U.S. guns, missiles, and bombs failing to fire or detonate or being directed against our own troops; or food, water, ammo, and fuel not arriving when or where needed; or the loss of position/navigation ability or other critical warfighter enablers."** The report chillingly warned that doubts about U.S. defense capabilities due to cyber vulnerabilities could cause a president to more quickly turn to nuclear weapons in a conflict.

Analysis: This argument can be weighed on magnitude. Conflict caused by miscalculation would likely be on a larger scale and have greater casualties than the strategic benefit that the U.S. gets from using offensive operations. It also interacts well with the argument about deterrence on pro; countries would more likely misinterpret U.S. offensive operations as aggression than get the signal that they're only meant to be deterred.

A/2: Offensive operations increase chance of miscalculation

Answer: Non unique—Trump's presidential style makes the chance of miscalculation high in the status quo.

Warrant: Trump has a 'doctrine' of unpredictability.

Fuchs, Michael. Trump's Doctrine of Unpredictability. "Trump's Doctrine of Unpredictability." Democracy Journal, 10 Feb. 2017, democracyjournal.org/arguments/trumps-doctrine-of-unpredictability/.

Maybe Trump is a realist; or maybe he wants to dismantle the U.S.-led international order. Perhaps he is purely a dealmaker. **Whatever the approach, one theme is consistent in Mr. Trump's actions and words: his desire to make U.S. foreign policy appear as unpredictable as possible. As Trump so succinctly summarized it himself during a foreign policy speech in April 2016: "We have to be unpredictable." Call it a "doctrine of unpredictability," if you like.** Donald Trump believes that the United States should pursue the foreign policy of a gambler, shedding the more "predictable" aspects of U.S. foreign policy that have, until now, helped keep the world somewhat stable. As gambler-in-chief, Trump's perceived unpredictability will supposedly give him leverage to negotiate anything with anyone at anytime.

Warrant: U.S. adversaries don't know where bluster ends and reality begins with Trump.

Seib, Gerald F. "Where Donald Trump's Unpredictability Could Hurt Him." WSJ, Wall Street Journal, 23 Oct. 2017, www.wsj.com/articles/where-donald-trumps-unpredictability-could-hurt-him-1508772460?ns=prod/accounts-wsj.

> Domestically, the danger is that lawmakers start to simply ignore what Mr. Trump says because they don't think they can count on it in the end. **Internationally, the danger is that opponents miscalculate because they don't know where bluster ends and bottom-line reality begins.** That seems a real danger right now in the tensions with North Korea. President Barack Obama learned the price of unpredictability in foreign policy in at least one important case. He warned publicly that Syria's use of chemical weapons in its civil war would cross a red line for him, prompting retaliation. When that red line was crossed, Mr. Obama failed to act, creating doubts about American reliability that lingered through his presidency.

Analysis: Offensive operations probably aren't the brightline that lead to miscalculation. By explaining that Trump's style itself makes the risk of miscalculation high, pro teams can mitigate the con's impact scenario—because it's not all that different from the status quo.

Answer: Effective cyber diplomacy prevents countries from misinterpreting each other's actions.
Warrant: The Trump administration has triggered a discussion about creating more effective cyber diplomacy.

Fidler, David. "Year in Review: The Trump Administration Disrupts U.S. Cyber Diplomacy." Council on Foreign Relations, 2017, www.cfr.org/blog/year-review-trump-administration-disrupts-us-cyber-diplomacy.

The Trump administration's actions triggered wide-ranging discussion about cyber diplomacy and what was needed to make it a more effective part of U.S. foreign and national security policy. By the end of the Obama administration, it was clear that having a strategy and a dedicated State Department office for cyber diplomacy did not guarantee success. Simply replicating the Office of the Coordinator for Cyber Issues and regurgitating the International

Strategy for Cyberspace will not answer the metastasizing cyber dilemmas confounding U.S. foreign and national security policy.

Warrant: The Trump administration passed an important cyber diplomacy bill.

> "Year in Review: The Trump Administration Disrupts U.S. Cyber Diplomacy." Council on Foreign Relations, 2017, www.cfr.org/blog/year-review-trump-administration-disrupts-us-cyber-diplomacy.

One of the most high-profile efforts to emerge from the deliberations stimulated by the Trump administration's disruption of U.S. cyber diplomacy was the bipartisan "Cyber Diplomacy Act of 2017" introduced in the House of Representatives in September and reported out of the House Committee on Foreign Affairs in November. **The bill catalogs why cyber diplomacy is important to the United States (Section 2), contains provisions to shape U.S. international cyberspace policy (Section 3), creates an Office of Cyber Diplomacy in the State Department to advance such U.S. policy (Section 4), and requires the Secretary of State produce an international strategy for cyberspace (Section 6). This proposed legislation has been largely received as a serious and welcome response to the strategic and institutional challenges of conducting effective cyber diplomacy.** As Cameron Kerry has argued, the bill recognizes that "protecting security in cyberspace and promoting digital communications . . . have become critical to the mission of the U.S. government," which will can better execute strategic initiatives "with a fully empowered Office of Cyber Issues able to represent the full range of issues involved."

Analysis: Coupled with the Trump administration's decision to use offensive operations, they've also taken steps to improve channels of communication that prevent miscalculation. Pro teams can frame the miscalculation argument as not looking at the whole story.

CON: Offensive operations erode international cyber norms

Argument: By using offensive operations, the U.S. changes the rules of cyber warfare and sets a precedent that other countries can act in the same manner.

Warrant: U.S. offensive operations allow other countries to claim their offensive hacking is acceptable.

> Marks, Joseph. "Analysis | The Cybersecurity 202: Trump Gave the Military Freer Rein for Offensive Hacking. Security Experts Say That's a Good Idea." The Washington Post, 11 Feb. 2019, www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/11/the-cybersecurity-202-trump-gave-the-military-freer-rein-for-offensive-hacking-security-experts-say-that-s-a-good-idea/5c607a571b326b66eb098678/.

> More broadly, former White House cybersecurity coordinator Michael Daniel worried that **U.S. cyber strikes would allow adversary nations to claim their offensive hacking is acceptable behavior. "We don't have a monopoly on these capabilities and any offensive action we take legitimizes such actions -- meaning another nation could take the same action against us. We are especially vulnerable to disruption through cyberspace,**" said Daniel who is now president of the Cyber Threat Alliance, a cybersecurity information sharing group. "Therefore, we need to use this tool carefully and judiciously[.]"

Warrant: It's questionable as to whether or not the U.S. can justify offensive operations under international law.

> Djabatey, Edwin. "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis - Part I." Just Security, 16 July 2019,

www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/.

If the targets of economic cyber intrusions, like the United States, were to adopt the U.K. view to the contrary, it would be impossible for them to claim that such cyber activity violates their sovereignty. This view may give a State like the U.S. the freedom to conduct 'below the threshold' cyber operations without fear of violating international law, but it would also remove all international legal constraints on the economic cyber intrusions conducted by an adversary State like China. **The likely inability of the United States to demonstrate that economic cyber intrusions violate international law calls into question the legality of the offensive cyber operations the U.S. seeks to deploy in response, to the extent those operations would themselves violate international legal obligations owed by the United States to the target State.** Accordingly, Part II will examine the legality of these responses.

Warrant: U.S. hypocrisy makes norms unenforceable.

Farrell, Henry. "Why It's so Hard to Create Norms in Cyberspace." The Washington Post, 6 Apr. 2015, www.washingtonpost.com/news/monkey-cage/wp/2015/04/06/why-its-so-hard-to-create-norms-in-cyberspace/.

Second – the U.S.'s own commitment to many of its values has been called into question. The Snowden revelations appear to show, for example, that the NSA has tried to compromise basic cryptographic standards that are required for an open and robust Internet to work. **This makes it hard for the U.S. to be an effective advocate for its norms. Some degree of hypocrisy is tolerable in international politics when others can turn a blind eye to it. However, when one's secrets have been leaked, other states may neither want to, nor be able to, ignore the difference between the U.S.'s lofty normative aspirations, and its self-interested behavior. The result, all too often, is**

battles over norms where neither side is likely to persuade the other. For example, the U.S. and China are facing off over commercial cyber-espionage aimed to grab the trade secrets of firms located in other countries, and pass them on to one's own businesses.

Warrant: Irresponsible use of force is destabilizing.

Wolff, Josephine. "Opinion | Trump's Reckless Cybersecurity Strategy." The New York Times, 2 Oct. 2018, www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html.

A smart national cyber strategy would focus on securing our computer systems, data and networks by allocating more money for their protection and by allocating more time and energy to regularly update, measure and test their security. It would charge the government with attacking its own servers and systems domestically to identify potential vulnerabilities before foreign adversaries have a chance to exploit them, rather than encouraging officials to strike out at overseas targets. And it would reserve the use of offensive cyber capabilities for situations that allow for careful consideration of the possible unintended consequences, narrow tailoring to a specific mission and contained, targeted damage. **Ironically, the new national cyber strategy also charges the United States government with enhancing cyber stability "through norms of responsible state behavior." As the rest of its policies make all too clear, this administration has already committed itself to irresponsible uses of cyber force that may serve to destabilize everyone's online infrastructure, including our own.**

Impact: Norms prevent conflicts from escalating by delegitimizing certain kinds of attacks.

Farrell, Henry. "Why It's so Hard to Create Norms in Cyberspace." The Washington Post, 6 Apr. 2015, www.washingtonpost.com/news/monkey-cage/wp/2015/04/06/why-its-so-hard-to-create-norms-in-cyberspace/.

Second, **sufficiently strong norms can delegitimize certain kinds of attacks. It would be unthinkable today for the U.S. to use nuclear weapons except in a truly dire situation where national survival was threatened.** This wasn't always the case, as Nina Tannenwald has argued. Nuclear weapons initially seemed like a more powerful version of traditional weapons, until a normative "taboo" began to spring up around them. **The reason why the U.S. would like to promote norms is that norms can determine both the acceptable limits of conflict, and the specific ways in which conflicts are conducted. Hence, norms can be incredibly powerful.**

Impact: Changes in cyber norms risk escalation between great powers.

Valeriano, Brandon. "The Myth of the Cyber Offense: The Case for Restraint." Cato Institute, 8 Jan. 2019, www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.

Cyber operations to date have not been escalatory or particularly effective in decisively achieving desired outcomes. Recent policy changes and strategy pronouncements by the Trump administration, however, could make escalation more likely while doing nothing to improve effectiveness. These changes are driven by a dangerous myth that offense is an effective and easy way to stop rival states from hacking America. **New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game.** Cyberspace, to date, has been a domain of political warfare and coercive diplomacy, a world of spies developing long-term access and infrastructure for covert action, not soldiers planning limited-objective raids. **Recent policy shifts appear to favor the soldier over the spy, thus creating a new risk of offensive cyber events triggering inadvertent escalation between great powers. Senior leaders throughout the federal government should consider a more prudent and restrained approach to cyber operations.** Building on Sir Julian Corbett's Principles of

> Maritime Strategy, one of the preeminent works in 20th century military theory, **we argue for a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation**.5 This approach counsels stepping back from preemption and focusing on sharing intelligence and hardening targets (that is, updating systems to repair existing vulnerabilities). The United States should exercise restraint and avoid preemptive strikes against great powers in cyberspace.

Analysis: This argument can be weighed on scope; the erosion of cyber norms will not only impact a potential cyber attack on the U.S. but also the scale of global cyber warfare. It can also be weighed on magnitude because cyber warfare will be significantly worse in a world without clear norms.

A/2: Offensive operations erode international cyber norms

Answer: Cyber norms are not followed in the status quo.

Warrant: Cyber norms aren't well established.

Barrinha, André, and Thomas Renard. "Cyber-Diplomacy: The Making of an International Society in the Digital Age." Global Affairs, vol. 3, no. 4–5, 20 Oct. 2017, pp. 353–364, 10.1080/23340460.2017.1414924.

Whereas cases such as the July 2016 Democratic National Committee hacking evidence that state activity in cyberspace is still very much determined by strategic (rather than normative) considerations (the realm of the international system), it is the aim of cyber-diplomacy to progressively shift those behaviours and attitudes towards a space of peaceful co-existence, defined by clear rules and principles: from a system of interactive units to a society of states. In that regard, cyber-diplomacy is to cyberspace what diplomacy is to IR: a fundamental pillar of international society. **Unlike other areas of international life, cyberspace is constituted by a rather incipient set of binding normative arrangements and there is an overall consensus from the diplomats interviewed for this article that much needs to be done in this realm. In the words of one of the interviewees, "in practical terms, at the moment the cyber-world still needs work to ensure adherence to international law and norms of responsible behaviour – otherwise it's pure anarchy"** For instance, whereas armed forces around the world are developing their own cyber-capabilities, there are no "parallel diplomatic processes to develop the agreed parameters for such operations"

Warrant: China and Russia are pushing back against cyber norms.

Zegart, Amy. "Trump's National Cyber Strategy Is Overly Optimistic." The Atlantic, The Atlantic, 2 Feb. 2019, www.theatlantic.com/ideas/archive/2019/02/trumps-national-cyber-strategy-overly-optimistic/581839/.

The National Cyber Strategy also declared that **the U.S. would "preserve peace through strength" in cyberspace by, among other things, encouraging adherence to global cyber norms. Here, too, this week's DNI testimony put the kibosh on all that hopey-changey talk, making clear that cyber norms have been very much contested by China, Russia, and their autocratic buddies who believe that every country should repress free expression within their own borders and free enterprise from outside them. Not only that, but Team Autocrat seems to be winning through a devious strategy of populating international organizations like the UN with their own countrymen to push their own views of "global norms."** In case you missed it, China is now the second-largest contributor to the United Nations budget. "[China] is successfully lobbying for its nationals to obtain senior posts in the UN Secretariat and associated organizations," notes the intelligence threat assessment, "and it is using its influence to press the UN and member states to acquiesce in China's preferences on issues such as human rights and Taiwan."

Analysis: This response makes the argument effectively nonunique. It doesn't matter that cyber operations would erode norms in cyberspace if those norms never existed in the first place.

Answer: Non-state actors can't be controlled regardless of the strength of cyber norms.

Warrant: Malicious cyber conduct by non-state actors exceeds that committed by states.

Buchan, Russell. "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm." Journal of Conflict and Security Law, vol. 21, no. 3, 19 Oct. 2016, pp. 429–453,

eprints.whiterose.ac.uk/103386/11/Buchan%20FINAL%20Cyberspace.pdf, 10.1093/jcsl/krw011.

The presence of non-state actors on the international stage has grown steadily in recent years. The unique features of cyberspace, including its borderless character, its inherent interconnectedness, the anonymity it affords and its accessibility, has provided a thriving environment for non-state actors and cyberspace has thus further empowered non-state actors to act independently from states in the international arena. Indeed, it is likely that malicious transboundary cyber conduct committed by non-state actors now exceeds that committed by states. In an international community based upon the sovereignty equality of its member states, international law demands the existence of effective international legal rules that provide states with protection from non-state actors that commit malicious cyber conduct from the territory of other states.

Warrant: Non-state actors burden existing norms.

Bussolati, Nicolò. "'The Rise of Non-State Actors in Cyberwarfare.'" Ssrn.Com, 2015, papers.ssrn.com/sol3/papers.cfm?abstract_id=2764185.

This chapter pointed out how **the digitalization of warfare has augmented the importance of non-state actors in the twenty-first century digital conflict, both as autonomous actors and instruments in the hands of the state. Furthermore, it evidenced how such a process challenged international law, burdening the existing norms regulating armed conflicts and generating several regulatory issues. The rise of non-state actors in cyberwarfare perpetuated the process of erosion of the role of the state as primary actor in the international scenario, following the path set in motion by international terrorism.** However, as pointed out in the preceding sections, the digitalization of war offers completely new boundaries to the phenomenon: it strongly enhances the role and the capacity of non-state actors involved, and offers them

structural and operative characteristics which deeply challenge the traditional corpus of norms regulating conflicts.

Analysis: Pro teams can frame con teams as ignoring the nuance of the means in which cyber attacks are carried out. Because of the rise of non-state actors conducting cyber attacks, these perpetrators are increasingly difficult to control.