NATIONAL SPEECH & DEBATE ASSOCIATION
NATIONAL FORENSIC LEAGUE

PUBLIC FORUM DEBATE

NOVEMBER-DECEMBER 2019 ADVANCED PUBLIC FORUM BRIEF

National Speech & Debate Association © 2018-2019 • updated 11/18/2019

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

This topic brief was written by Jesse Meyer. Jesse is a diamond coach, recipient of the Donald Crabtree Service Award, the state of Iowa's 2015 Coach of the Year, and board member of the Iowa Forensics League. He is currently an assistant coach at Iowa City West High School. He can be reached at jessemeyer@gmail.com.

November-December 2019 Advanced Public Forum Brief

Table of Contents

Introduction

The November/December public forum debate topic is US Cyber Operations.

The internet, or at least the concept of the internet, is almost as old as modern computers. Going back as far as the 1960's, computer programmers were looking for ways to link their computers with computers at research institutions in distant labs to share data and information. At the same time, the military realized that in the event of a nuclear war, it would be strategic for an enemy nation to target and destroy one central location and wipe out the entire records databases for both civilian and government operations. Furthermore, in the event of a war, losing one central military command and control location could cripple the response to an attack. The concept was then born to create a central system of computers that could link together and share critical data and create backups of information to hedge against the pitfalls of war and to allow academic institution to share research. In the late 1960's the first coded internet transmission was from computer to computer. Despite a network failure that caused the full message to fail and only two letters (which were "LO" for those planning for a final Jeopardy question) the test was deemed a success.

By the time we get into the 1970's, computer networks are more stable and better designed. Computers are more powerful and their size has brought their overall size down to what we could call manageable. Instead of being the size of whole rooms with the processing power of several bits per second, computers and their microprocessors could fit into desk sized boxes (not desktops, but actual boxes the size of desks) and the processors could operate in the range of several kilobytes per second. This is not impressive by modern standards as most remotes for electronic devices have about the same processing power, at the time, it was legendary. Due to the nature of computers being limited to data processing, a lack of commercial software, and the sheer cost, computers were limited those in government, business, and the ultra-wealthy. The internet was also nonexistent for commercial use as most commercial telephone companies didn't yet have the capacity to deal with data transmission over their phonelines. So, network communication was limited to government and business entities to share data. The first true cyber operations were born from this. The concept wasn't to break into an enemy system to get sensitive information but rather to intercept data as it was in the process of transmission so that surveillance could take place.

In the 1980's we see the birth of the home computer market. Instead of being in the range of $10000, home computers and the mass production of their internal parts brought the cost of computers down to sub $3000. Apple and Microsoft began their wars with the Mac OS and the DOS OS. The Commodore 64 was the first computer that also doubled as a video game machine with graphics that were not in black and white or green and black. The first laptop computers hit the market, and despite their weight of 20 pounds or more, they gave business users on the go a way to take the office with them. The internet also became faster and commercial. The first 14.4 KBPS modem was released, and people began sharing their ideas on text based message boards.

The internet in the 1980’s was simpler. There was no YouTube, there was no google, you didn’t have ad’s every 30 seconds asking you to donate to the DNC or poll on Trump’s Wall. Everything was text based and since most internet providers at the time charged by the minute for access and since posting things was slow, most conversations were serious discussions rather than people looking to troll and start flam wars on the internet comment sections of news articles.

Hacking in the 1980’s began to develop more. As more computers were added to the network, more and more people gained the ability to access sensitive data of the government if you knew where to look and how to use computer code. Although better defended that the computers in the movie “War Games” the concept remains true that government computers became vulnerable to outside attacks from enemy operatives seeking information. And it was an information seeking operation. Since little could be done to critical infrastructure via computers, at this time the main goal of hacking was still focused on intelligence gathering and reconnaissance. It was also in the late 1980’s that we see the first malicious software start to pop up and infect computers. These early viruses were designed to slow down computers rather than steal critical financial information like the software of today. This is primarily due to the fact that commerce and finances were still done in person or by phone and not online.

In the 1990’s we see the internet revolution. Personal computers become cheap, small, and user friendly. Graphic user interfaces made operating systems like Mac OS and Windows into click based shells rather than the text and command based operating systems of the past, so anyone could figure out how to get online. The internet kept getting faster. Speeds doubled from 14.4 to 28.8 and finally to 56.6. Then companies figured out how to use the cable tv systems in most urban homes to send internet signals and speeds jumped into the hundreds of kpbs. Websites became flashier and better designed. E-commerce became a big deal as modern encryption and faster internet speeds increased safety and reliability. Amazon launched as a bookstore. If you wanted to research, you could AskJeeves or go to DogPile, or even use a crude version of Google.

The website for Space Jam, copyright 1996. Yes, it is still live. https://www.spacejam.com/archive/spacejam/movie/jam.htm

Sadly, it was at this time that malicious software really began to take hold. Government computers fully utilized the internet to transmit data and store files. Enemy nations realized that a skilled hacker could find ways of getting past security measures and gain access to these files. It was at this time that the government also realized that our military command was connected to the same internet that was allowing teens to share illegally downloaded music and families to share vacation pictures. As one security expert put it, "It's like having a nuclear missile silo in the middle of a downtown shopping center." The concept became a "what if" of nightmare scenarios. What if someone gained access to the launch system, what if someone hacked our power grid, what if someone shut down our treasury department for a day? Several experts on the matter voiced concerns but their pleas fell on deaf ears.

In the 2000's, we reach modern times. Nearly everyone in the United States has access to an internet capable device and just over half of people living outside of the United States have access as well. Computer are fast and cheap. You can buy a computer on Black Friday that is several thousands of times more powerful than the first computers in the 1970's, weights only a few pounds, and will cost you less than your coach is likely paying for your team's entry fees at the next few tournaments. (assuming your team is small).

We also see a proliferation of cyber-attacks on government resources. In 2006, the Stuxnet virus first appeared as a basic and undeveloped version of the virus that would ravage the Iranian nuclear program seven years later. Each day, our government fight out attempts by random attackers, foreign governments, and automated systems that are attempting to gain access to our critical systems. Under increasing pressure from the military and with the threat level rising, the president and congress knew they had to act.

In 2015, the US Department of Defense was tasked with creating a stargegy to defend the United States from malicious cyber-attacks. The strategy that came from this included five pillars.

1. Build and maintain ready forces and capabilities to conduct cyberspace operations

2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions

3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence

4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages

5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

In short, you can summarize these with the "3 D's of Cyber Operations." Disinformation, Defend, Destroy. First, you try to mislead those that would seek to do harm to you or your nation or those that would try to gain entry to your systems. Second, defend your nation by building relationships and creating safeguards, and finally you destroy your enemy either in a counterattack after you have defended your network or as a a preemptive strike.

After the election of Donald Trump, the mission was granted new powers. In the congressional budget of 2016 and 2017, congress granted new powers to the military to use covert cyber operations at their discretion. This strayed from previous doctrine as in the past, cyber operations were considered the same as a military operation and thus, members of the house leadership were to be notified when an operation was to take place. Now, under presidential authorization, the Department of Defense could carry out covert offensive attacks without congressional oversite. At the same time, the president granted the Department of Defense broad latitude in what constituted an "offensive cyber operation." The policy that came from this was "defense forward." Although few people have concretely defined this, the general philosophy is understood to be one of preemption. If the US sees a threat online, they may respond with a first strike online to eliminate the target.

As of today, due to the covert nature of our offensive cyber operations, little is known. US Cyber Command, the department of the military tasked with coordinating our cyber operations and defense, has told the public little about their mission. Speculation abounds that the US was at least partially responsible for attacking the Russian power grid last summer and aiding the Israeli military in creating Stuxnet, the virus that would cripple Iran in 2013. Sporting one of the largest budgets at the Pentagon, the US government is trying to make up ground as our cyber operations have been seen by almost every member of the intelligence community as being lagging behind almost every other developed nation.

Framework and Definitions

When I think framework on this topic, the first thing my mind jumps to is a cost benefit analysis. I mean, the topic almost points you there with giant flashing neon signs because of the wording and the use of the phrase "benefits" and "outweigh." And I can tell you that you wouldn't be wrong in this assumption. In fact, you wouldn't be wrong to run a cost benefit analysis as your framework and you will win many rounds if you do so. However, let's look beyond the obvious and look at other options.

The way that I have always viewed frameworks is that they are a lens that tell the judge how to prioritize impacts. If you are running a human rights impact with lives saved your opponent is running an economic impact with billions earned, a good framework will tell the judge why I should evaluate lives before profits. In this way, a cost benefit doesn't really meet this criterion of prioritization. I would still be stuck with the same lives vs money debate and in the end, I'd have to default to making up my own mind, and as we discussed in the September/October brief, you never want the judge making up their own mind. So in this debate, I view the cost benefit that the resolution hits us in the head with as a secondary framework. What I mean by this is that in the end, the judge will weight impacts for costs and benefits, but the primary framework that you and your opponent should be advocating for will tell the judge how to prioritize the impacts.

To this end, I think the pro team would be smart to advocate a world of realism. Realism is the concept that we don't live in a perfect world. We have friends, but our friends can be our enemies. We also have to live with the concept that each nation is looking for self-preservation and survival as a primary motive for action. No nation wants to "go quietly into the night" nor will any nation just sit back while others take advantage for them and their ignorance of the situation. In this case, it is in the best interests of nations to "prepare for the worst and hope for the best." It's the same reason that some people keep an extra winter coat in the car or why people fishing in Alaska carry a handgun; you hope you never break down in a winter storm and you hope that you don't run into a hungry brown bear, but you know that the world is a scary place with real dangers.

Rohrlich, Justin. "The Pentagon thinks cyber ops could be the next WMDs," Quartz, https://qz.com/1500647/the-pentagon-asks-researchers-for-help-planning-for-cyberattacks/https://qz.com/1500647/the-pentagon-asks-researchers-for-help-planning-for-cyberattacks/,

The Pentagon thinks cyber ops could be the next WMDs
In recent years, Russia, China, North Korea, and a number of violent extremist organizations have launched offensive cyberspace operations against the US. PASCC says the cyber-attacks are becoming more sophisticated—and a more integral part of US adversaries' military strategy. PASCC points out that a powerful enough cyberstrike could destroy critical infrastructure, take the financial system offline, or compromise the accuracy of essential military systems. **It also noted the potential threat of social media, which it says could be used to spread "false rumors and innuendo designed to strain alliances, divide polities, and undercut public confidence in institutional integrity and social cohesion."**

Another pro option is to weight lives saved. This debate will come down to hypotheticals on the impact level debate as there is little good evidence about how much damage would be caused not having offensive cyber operations. Likewise, the hypothetical wars that the con team will likely argue might result from our cyber operations are also hypothetical. But judges would be far more likely to vote off of damages and lives that have the potential to be harmed from a nuclear reactor being shutdown or the financial sector being messed up when compared to the hypothetical link chain that gets us from hacking North Korea to them nuking Chicago.

Economics is another strong pro framework. Some real-world data that is available si the financial impact that offensive cyber operations done to the United States. In this case, the argument revolves around deterrence and preemption. One would argue that we vulnerable to attacks now and that our offensive capabilities allows us to head off a financial attack or at least we can deter others from launching an attack on us. Then you would just need to show how past attacks have crippled banks or cost the consumer X millions of dollars.

On the con, I could see teams going for a securitization bad argument. This argument is a kritik from policy debate, but it can function in PF. The argument is that we create threat so that we have something to solve. Whether we do this because as humans, we enjoy conflict, because of the industrial military complex, or because we are paranoid, we like to create threats. This means that we have taken the concept of the "hacker," a faceless entity and made it into a ghost in the night. We fear what we can't see because we don't know what it is up to. This is only magnified if your opponents argue that the threat is foreign. At that time, it becomes a threat construction argument with the foreign invader as the opponent to fear. So, in a way, the framework becomes not only a prioritization mechanism but also a contention as well.

Gartzke, Erik. 2013 The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth International Security 38:2
https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136

Given the inherent difficulty of credibly threatening cyberattacks without also compromising operational effectiveness, it will be tempting for actors to practice cyberwar rather than engage in coercive threats. Here, too, however, key limitations exist regarding what can be achieved over the internet. It is one thing for an opponent to interrupt a country's infrastructure, communications, or military coordination and planning. It is another to ensure that the damage inflicted translates into a lasting shift in the balance of national power or resolve. Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary. In many, perhaps most, circumstances, this will occur only if cyberwar is accompanied by terrestrial military force or other actions designed to capitalize on any temporary incapacity achieved via the internet. Those initiating cyberattacks must therefore decide whether they are prepared to exploit the windows of opportunity generated by internet attacks through other modes of combat. If they are not willing and able to do so, then in grand strategic terms, there are few compelling reasons to initiate cyberwar. The need to back up cyber with other modes of conflict in turn suggests that the chief beneficiaries of cyberwar are less likely to be marginal groups or rising challengers looking to overturn the existing international order and more likely to be nation-states that already possess important terrestrial military advantages. Conceived of in this way, the internet poses no revolution in military affairs but instead promises simply to extend existing international disparities in power and influence.

Another more traditional framework is to vote for the side that best reduces miscalculations. In this debate, you would argue that the essence of the pro team causes people to become skeptical of US action. Understanding that the actions of the US based on the mandate from congress are covert, nations might misunderstand the intent of a US move or posture and out of fear of a pending cyber-attack, launch a first strike on our cyber systems or physical systems first. This would escalate into a full-blown war. Whether this war leads to a nuclear attack or not, you can gain huge impacts off of the concept of two armies engaged in a huge shooting conflict.

In a similar vein to miscalculation, you could run promotion of international relations. The link chain would be very similar up to the point of miscalculations leading to war. Instead of a war, you would argue that the resulting tension would leads to a reduced sense of unity and cooperation and this would lead to a world of isolationism. In advanced scenarios, you could argue that this creates a unipolar world where multiple countries are fighting for domination and influence and that brings us to the brink of war.

No matter what framework you use, it is important in the end to remember that you are choosing the prioritization mechanism for which all other impacts then be fed through the given lens of a cost benefit analysis. Against teams that argue that cost benefit is the framework, you will need to lay out for the judge the argument stated in the first paragraph of this section because judges, especially judges who are younger and who might have debated in the past, will be predisposed to assume that cost benefit is the superior framework. Their mentality can be changed but you have to do the work to get there.

When we look at the definition debate, we see some distinctions that have to be made rather than actual debate over the meaning of words. This comes from people making assumptions about the topic rather than actually reading what the topic says.

-United States federal government- The centralized government of the United States. Check your opponent's literature and check yours as well. Private companies have been doing lots of offensive cyber warfare in the past whether as private business defending their own interests or under independent contract by the government. This makes a huge difference in terms of international law and who is allowed to launch attacks against infrastructure A or B. As per the topic introduction, the most common United States federal government agency is the Department of Defense and the US Cyber Command.

- Offensive vs defensive- Offensive by most traditional definitions means that you are going on the attack rather than waiting to be attacked. Think troops marching out of the fort rather than the troops defending the walls of the fort. Does this make a difference? In most situations, if you are attacked first, you are rightfully justified in defending yourself. No court or tribunal would necessarily fault a person or nation from defending themselves within reason if they are attacked and on the defense. However, to go on offense and launch a first strike required premeditation. To use another criminal law example, if you are walking in the part and you are attacked and in the process of fighting that person off, you injure them, in most jurisdictions, your actions are ruled to be justifiable. That's defense. However, if you feel that a person might be plotting against you, so you ambush them first in the park attempting to injure them, you are in the wrong because you were the aggressor. There is also a debate over whether offensive and defense really are different and exist. Anti-virus or election tampering safeguards are likely defensive. Offensive use requires a dedicated motivation to action.

-Cyber operations- I can see this being a broad topic that defined by experts in the field debating what their specific field of research is and that is "cyber operations." In a hugely broad sense, the term means anything done on a computer towards other computers. It will become critical and strategic to find a definition of cyber operations that limits the case literature to what you want to debate.

Finally, I have some last topic thoughts that I wanted to list and that fit into no other good part of this brief.

- Outweighing harms- Don't get drawn into a debate where you try to defend zero harms. Rather, you concede minor things and go for the big outweighing mechanisms. Teams that try to win that their side has zero harms will have zero ballots at a tournament.

- Nothing in the topic says that offense has to be in response to a threat or that a threat has to exist. Threats are largely perceived. Especially in the world of cyber warfare, we know so little about the position and intent of our enemies. With traditional armies, we can see troop movements. Online we can't.

- In traditional warfare, we justify proportional warfare and response. This means we respond and attack in equal measures to what is done or what we expect to be done. We don't nuke a country because they shot down a drone. In cyberwar, especially in covert wars, would this mentality still exist, or should it exist?

- Nowhere in the resolution does it say that the offensive cyber operations have to carried out and directed at another nation or state. This means that we could target businesses, individuals, or groups with our offensive cyber operations. We could target ISIS, Chinese tech companies, or public figures with these operations. This poses a problem if we target individuals like leaders of foreign countries as in international law, it is illegal to target foreign officials for assassination. It is true that this would not be a traditional attack leading to death, but it could still be classified as a hit. It might also violate due process of the individual or group as the covert nature of the attacks would deny them a chance to defend themselves in the public sphere.

- Likewise, nothing says the targets have to be international. We could target domestic figures or groups. This poses a huge issue as it is illegal to use the military as a domestic police force. This would also definitely violate the due process clause as it denies the person a chance to defend themselves in a courtroom. It would also deny the trial by a jury, a chance to confront an accuser, and cruel and unusual punishment.

This topic has board implications for both international and domestic politics as long as you are willing to do the work to find the links. What I encourage each team to do is find a framework that complements the narrative you and your partner are creating with your cases and think creatively. Not every judge wants to hear a China debate every round. Creative teams with well thought out cases win rounds on sheer entertainment value in some cases. And above all, remember that this topic is open to a vast world of interpretations as long as you are willing to keep an open mind.

Other Countries

This core of the topic is the most straight forward argument contentions that can be run. The purpose of an offensive cyber operations system is to counter the threat posed by other countries. The hard part about this is finding and isolating the threats to the United States. As I was reading over the research online and looking for countries that could fit the criteria, the four that kept coming up were Russia, China, North Korea, and Iran. These will be the big four that you will likely hear in debate rounds.

Other countries that might come up are likely to have a smaller literature base and in reality, likely pose little threat in terms of both an offensive cyber security risk or a physical military risk mindset. This is why the literature is thin and why our operations are not focused on them. Nations in this list might include India (a rapidly developing nation that has expanded their tech sector), Germany, Great Brittan, Canada, France, Italy, Spain (all nations that are allies but also are competing for the same slice of the geopolitical power pie), Japan and South Korea (major power players in East Asia), Israel Egypt, and Saudi Arabia (Middle East movers and shakers), Brazil (biggest threat to our farming industry), Venezuela (noted rival and socialist dictatorship in South America), and Australia (the largest power player in the South Pacific).

What is important to note is that in almost every nation listed above, the threat they pose online is slim if nonexistent. For the most part, those nations pose more of a regional stability threat or an economic threat. However, the topic does not require that the offensive cyber operations the US is using be directed at other cyber operations. The operations can be used and directed at nations to slow their growth and clear a path for US dominance in any given field.

If you were to argue one of the nations that are not one of the big 4, you are going to need to clearly establish the fact that they still pose a threat to the US and that our offensive cyber operations are the only counterbalance. You will need to work hard to establish the link for the judge because most judges will want to apply the “equal and opposite force” doctrine and without a credible cyber threat, they will be hard pressed to agree that one type of force demands a response with a completely different force type.

China

In the world of cyber operations, there is no nation that the US fears more than China. China is the largest nation on Earth with the one of the largest economies and the fastest growing economy on Earth. Their desire to expand their sphere of influence is well known. Through their artificial island building in the South China Sea to the Belt and Road Initiative, the Chinese hope to become a dominant force in international relations. The barrier to their rise to power is the US. Past American presidents have always been wary of the Chinese and their ulterior motives; however, the situation was kept at a stable sense of peace due to the need for international cooperation. With the election of President Donald Trump, however, the status quo has changed.

In 2015 under the new Cyber Operations Guidelines, the US government proposed a series of offensive measures designed to preempt intervention of foreign agents into our country via our networks and the internet. This posture was further powered by the idea of "defense forward" or a digital first strike when necessary. These strategies were aimed at countering our two biggest rivals in the world, Russia and China.

What has China done to draw the ire of the United States? Although the bulk of daily cyber-attacks on the US and our civilian and governmental resources are directed from the Eastern Europe region of the world, the second largest zone is from mainland China. Chinese hackers have been blamed for the data breach at the Office of Personal Management in 2015 that stole the personal and financial data on thousands of US federal government employees. Experts in the fields of security and computer crimes have stated that the biggest reason for this targeting was likely either for identity theft or for blackmail purposes. In 2019, cyber security experts found that ten of the largest telecom providers in the world, including several on US soil had their mainframes breached by Chinese hackers. On these systems, spying and surveillance software was implanted to monitor US communications.

Under the new doctrine of "defense forward" the US government would be allowed to first strike Chinese cyber operations command and control facilities and centers. They could shut down threats before they are used against the United States, and furthermore, they are a strong deterrent against further Chinese aggression. Although much of cyberwarfare is done under the cover of the internet, nations still know who carries the "big stick" and out of fear of retaliation or in this case, first strike prioritization, China might unilaterally back down.

On the flip side, a first strike might only provoke a war or lead to miscalculations; Experts in the field of warfighting argue that unless a strike cripples the Chinese military enough so that they themselves can't fight a retaliatory war (like disabling their communications or radar), then the results could be a devastating second strike with physical armies. In this scenario, it is important to remember that China is a nuclear power and has the world's largest navy. In the sphere of miscalculations, as China sees the United States building up their cyber operations, they might grow nervous as to the true intent of the networks. Fearing for a first strike that might cripple their nation, they might strike first leading to a conflict. Or actions or statements from our leaders might inflame the situation and cause there to be a conflict that rises out of a misunderstanding of the situation.

When debating this argument, remember that as judges, we have heard this for the last two months. We are both experts on China and kind of tired of the argument. This can cause us to become desensitized to what you are saying. You will might have to really articulate the link chain to keep us in the game and focused on the story you are telling. I am saying this not to sound mean but to be honest with everyone. Also, if you want to earn that extra speaker point, find a unique story for your cyberwar arguments. Find a cool impact and really hype up the story. On the con, you need to argue that the Chinese have no reason to be a threat to the United States. This could be due to trade instability, the amount of debt they own, or because they have other targets to focus on first.

Sample Evidence

Offensive Cyber Operations are needed to counter China

O'Donnell, Wes. 6-26-2019, "The US Enters a New Era of Offensive Cyber Operations," InCyberDefense, https://incyberdefense.com/editors-picks/the-us-enters-a-new-era-of-offensive-cyber-operations/

Offense, Not Defense, Is a Different US Tactic in Cyberspace Currently, in China, the U.S. is likely engaging in a similar campaign to our Russian attacks — planting the seeds for deep disruption in the event of a larger conflict. Like space, the digital realm is the newest front in the competition between nations. Operations in cyberspace have a role in the ongoing game of economic, military and diplomatic one-upmanship. One of the reasons that the previous administration hesitated to utilize our nation's full range of offensive cyber capabilities was a fear that these tools could be used against us in the future. Given our adversaries' devastating capabilities, it seems now that the United States is growing more risk-averse and fully prepared to bring to bear the full might of America's cyber arsenal.

Chinese attacks kills the US economy. We lose billions a year. Need offensive cyber operations to counter the threat

Strobel, Warren. 10-17-2019, "Bolton Says U.S. Is Expanding Offensive Cyber Operations," WSJ, https://www.wsj.com/articles/bolton-says-u-s-is-expanding-offensive-cyber-operations-11560266199

Addressing economically motivated hacking from foreign adversaries, particularly China, has been a top cybersecurity priority of the Trump administration. The Justice Department late last year unsealed a flurry of indictments blaming Beijing for a host of cyberattacks targeting a range of different industries, including aviation and information technology. Some government estimates calculate that China's cybertheft costs the American economy hundreds of **billions of dollars** annually. The Obama administration sought to broker agreements with China to curtail its cybertheft, signing a 2015 bilateral accord that pledged not to engage in hacking for the purpose of economic espionage. China has been violating that agreement for at least the past 18 months, according to some private-sector cybersecurity analysts, and last November a senior National Security Agency official publicly accused the rival of violating that deal. In addition to Mr. Bolton, U.S. Cyber Command Commander and NSA Director Gen. Paul Nakasone has also articulated a more aggressive cybersecurity posture referred to as "persistent engagement." The goal is to be constantly watching adversaries in order to understand what they are doing and planning to do in cyberspace in order to be ready with appropriate responses, Mr. Nakasone has said.

Further Reading

Heginbotham, Eric. "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities from The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017 on JSTOR," https://www.jstor.org/stable/10.7249/j.ctt17rw5gb.19#metadata_info_tab_contents

Jinghua, Lyu, 4-1-2019, "What Are China's Cyber Capabilities and Intentions?," Carnegie Endowment for International Peace, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Lindsay, Jon R. "Exaggerating the Chinese Cyber Threat," Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/exaggerating-chinese-cyber-threat

Sellin, Lawrence. 9-6-2019, "The US is unprepared for space cyberwarfare," Military Times, https://www.militarytimes.com/opinion/commentary/2019/09/04/the-us-is-unprepared-for-space-cyberwarfare/

"The U.S. Unleashes Its Cyberweapons," Stratfor, https://worldview.stratfor.com/article/us-unleashes-its-cyberweapons-iran-russia-china-cyberwar

Wagner, Daniel. "Why China may reign supreme in cyberwarfare," South China Morning Post, https://www.scmp.com/comment/insight-opinion/united-states/article/2188873/chinas-head-start-cyberwarfare-leaves-us-and

Iran

In 1979 when the nation of Iran overthrew the US backed monarchy and installed Grand Ayatollah Ruhollah Khomeini and converted the nation from Iran to the Islamic Republic of Iran, the world changed. The US lost not only a critical member a Middle Eastern alliance, but also gained an enemy in the region. This new nation was formed under growing opposition to US presence in the Middle East, the US support for Israel, and the perceived Westernization of the Middle East by the United States at the expense of the religion of Islam. Tensions were further inflamed later that year by a failed rescue attempt by the US that resulted in the deaths of several American soldiers in a sandstorm, an oil embargo that would cripple the US economy in the 1980's, support for terrorist and radical extremist groups in the 1990 and through today, and the development of the Iranian nuclear program in the 2000's. Despite sanctions from the US, our allies, and the United Nations, Iran has maintained their track on the path towards nuclearization. It is this last point that has many people very worried about the status of Iran. A nuclear Iran would tip the balance of power in the Middle East.

As of now, there are no declared nuclear powers in the region. Israel likely has nuclear weapons, but they will not declare for fear of a massive invasion and attack from multiple nations. A fully nuclear Iran would worry Israel as the Iranians have threatened to "Drive the Israelis into the sea" in the very recent past and their sponsorship of terrorist groups in Israel has marked them as a target of the regime. The Iranians claim that their nuclear reactors are for research and civilian power only however after the collapse of the Iran Nuclear Deal early in the Trump Administration, it became obvious that the amount of uranium that was being enriched was for more than research purposes.

To counter this threat to the region, early in 2006, a virus popped up on the internet. It was called Stuxnet. The virus was simple and crude. It infiltrated machines that had security exploits in their operation systems and attempted to disable key operations in the computers, rendering their use mute. The virus was crude and, in most cases,, it failed. However, the virus was programmed to save data on successful infiltration and transmit it to a black ops site. In 2013, the Stuxnet virus reemerged with new code. It swept around the world shutting down personal computers and business servers alike. One target however seemed to be front and center, and that was the nation of Iran. Systems in Iran were hit especially hard. Their power grid would be crippled for months, and their nuclear reactor research sites would be shut down for months and in a few cases, up to a year for repairs. In 2015, it came out that this virus was likely made by hackers working for Israel with US assistance. Their goal was to slow the development of the Iranian nuclear program and force them to the table to negotiate a treaty. This strategy might have worked as later that year, the Iranians would open negotiations and shortly before he left office, Obama signed an executive order ratifying the Iranian Nuclear Deal.

Under the presidency of Donald Trump, the Iranian Nuclear Deal has been voided and we are back to pre-2015 relations. The Iranians have begun to enrich their uranium again. Under the cyber operations guidelines, experts see that another hacker attack on Iran is not just assured, but imminent. A cyber-attack would be preferable to a first strike in the eyes of the military command as it would mean fewer frontline deaths. In the eyes of the President, despite his dislike of cyberwar, he can shut down Iran without actually invading any country. With the cover of covert actions, the US can remain in a state of plausible denial to the source of the attack or attacks.

The big concern about this strategy is that, like a Chinese digital first strike, you would need to destroy the Iranian response and keep the identity of the attackers hidden. If Iran isn't destroyed, we risk a relation in the area to our allies in Saudi Arabia, our bases in Europe, Israel, and the Strait of Hormuz. These have implications for a snowball war in the case of an attack on Israel or Saudi Arabia, harmed relations and civilian deaths in the case of an European attack, and harm to the economy in the case of a Strait shutdown.

As debaters, this advantage has good ground on the pro as we have seen success in offensive cyber operations. The Stuxnet virus was deemed a success by almost every security expert in the world. The nature and identity of the attackers is speculated but isn't 100% known so there is still the mask of deniability. For a con team that has to debate this, your best bet is to have up to date defense on their impact scenarios. Also, there is a uniqueness argument to be had that Trump really dislikes cyber operations and he will never authorize one against Iran due to his dislike. In this case, you will be forced to go defensive.

Sample Evidence

Offensive cyber operations are necessary to counter Iran and their attacks on oil shipping

Barnes, Julian E. 2019, New York Times, U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

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. Iran is still trying to recover information destroyed in the June 20 attack and restart some of the computer systems — including military communications networks — taken offline, the officials said. Senior officials discussed the results of the strike in part to quell doubts within the Trump administration about whether the benefits of the operation outweighed the cost — lost intelligence and lost access to a critical network used by the Islamic Revolutionary Guards Corps, Iran's paramilitary forces. **The United States and Iran have long been involved in an undeclared cyberconflict, one carefully calibrated to remain in the gray zone between war and peace. The June 20 strike was a critical attack in that ongoing battle, officials said, and it went forward even after President Trump called off a retaliatory airstrike that day after Iran shot down an American drone. Iran has not escalated its attacks in response**, continuing its cyberoperations against the United States government and American corporations at a steady rate, according to American government officials. ***American cyberoperations are designed to change Iran's behavior without initiating a broader conflict or prompting retaliation***, said Norman Roule, a former senior intelligence official. Because they are rarely acknowledged publicly, cyberstrikes are much like covert operations, he said. "**You need to ensure your adversary understands one message: The United States has enormous capabilities which they can never hope to match, and it would be best for all concerned if they simply stopped their offending actions**," Mr. Roule said. Defying U.S. Sanctions, China and Others Take Oil From 12 Iranian Tankers **The U.S. has been unable to halt Iranian oil exports. Cyberoperations do not work exactly like other conventional warfare. A cyberattack does not necessarily deter future aggression in the same way a traditional military strike would, current and former officials say.** That is in part because cyberoperations are hard to attribute and not always publicly acknowledged by either side, the senior defense official said. Yet **cyberoperations can demonstrate strength and show that the United States will respond to attacks or other hostile acts and impose costs**, the official said. Cyber Command has taken a more aggressive stance toward potential operations under the Trump administration, thanks to new congressional authorities and an executive order giving the Defense Department more leeway to plan and execute strikes. **The head of United States Cyber Command, Army Gen. Paul M. Nakasone, describes his strategy as "persistent engagement" against adversaries. Operatives for the United States and for various adversaries are carrying out constant low-level digital attacks, said** the senior defense official. The American operations are calibrated to stay well below the threshold of war, the official added. **The strike on the Revolutionary Guards' intelligence group diminished Iran's ability to conduct covert attacks**, said a senior official. The United States government obtained intelligence that officials said showed that the Revolutionary Guards were behind the limpet mine attacks that disabled oil tankers in the Gulf in attacks in May and June, although other governments did not directly blame Iran. The military's Central Command showed some of its evidence against Iran one day before the cyberstrike. **The White House judged the strike as a proportional response to the downing of the drone — and a way to penalize Tehran for destroying crewless aircraft. D**espite the devastation cyberweapons have caused around the world over the last decade, they are still in their infancy. David E. Sanger, a New York Times national security correspondent, explains why the threat is growing. The database targeted in the cyberattacks, according to the senior official, helped Tehran choose which tankers to target and where. No tankers have been targeted in significant covert attacks since the June 20 cyberoperation, although Tehran did seize a British tanker in retaliation for the detention of one of its own vessels. Though the effects of the June 20 cyberoperation were always designed to be temporary, they have lasted longer than expected and Iran is still trying to repair critical communications systems and has not recovered the data lost in the attack, officials said. Officials have not publicly outlined details of the operation. Air defense and missile systems were not targeted, the senior defense official said, calling media reports citing those targets inaccurate.

Offensive cyber operations are the only way to stop Iran

Djabatey, Edwin. 10-17-2019, "Reassessing U.S. Cyber Operations against Iran and the Use of Force," Just Security, https://www.justsecurity.org/66628/reassessing-u-s-cyber-operations-against-iran-and-the-use-of-force/

On June 20, the ongoing confrontation between the United States and Iran almost escalated into a shooting war. Air and naval attacks on Iranian missile and radar installations, in response to the shooting down of a U.S. Navy surveillance drone and in the wake of the alleged mining of Norwegian and Japanese tankers by the Iranian Revolutionary Guard Corps (IRGC), were cancelled at the eleventh hour. Nevertheless, an offensive operation of a different kind still went ahead. **U.S. Cyber Command (CYBERCOM) carried out operations against Iranian targets,** presumably at the same time as the aborted conventional strikes were ordered. **The cyber operations were reportedly aimed at an IRGC-affiliated cyber group that supported the tanker mining incident and that has allegedly been interfering with civilian and military ships and personnel passing through the Strait of Hormuz**, for example, the British tanker "Stena Impero." From what is publicly known about the operation, **it was "intended to take down the computers and networks used by the . . . group, at least temporarily." It "wiped out a critical database" used by the IRGC to plan attacks against ships in the Gulf, leaving Iran attempting to restart the affected computer systems and recover the information lost. In this way it apparently "diminished Iran's ability to conduct covert attacks."**

Cyber-attacks cause miscalc with Iran. Leads to conflict

Sanger, David E. 9-23-2019, "The Urgent Search for a Cyber Silver Bullet Against Iran," No Publication, https://www.nytimes.com/2019/09/23/world/middleeast/iran-cyberattack-

After spending billions of dollars to assemble the world's most potent arsenal of cyberweapons and plant them in networks around the world, United States Cyber Command — and the new era of warfighting it has come to represent — may face a critical test in the coming weeks. President Trump is considering a range of options to punish Iran for this month's attack on Saudi oil facilities, and has toughened sanctions on Iran and ordered the deployment of additional troops to the region. But a second cyberstrike — after one launched against Iran just three months ago — has emerged as the most appealing course of action for Mr. Trump, who is reluctant to widen the conflict in a region he has said the United States should leave, according to senior American officials. But even as the Pentagon considers specific targets — an attempt to shut down Iran's oil fields and refineries has been one of the "proportionate responses" under review — a broader debate is taking place inside and outside the administration over whether a cyberattack alone will be enough to alter Iran's calculations, and what kind of retaliation a particularly damaging cyberstrike might provoke. "The president talked about our use of those previously, but I'm certainly not going to forecast what we'll do as we move forward," Secretary of State Mike Pompeo said Sunday on CBS's "Face the Nation" when asked whether a cyberattack might be an artful, non-escalatory response to this month's drone or missile strikes on two of Saudi Arabia's most important facilities. "This was Iran true and true, and the United States will respond in a way that reflects that act of war by this Iranian revolutionary regime." Mr. Pompeo noted that the American military was already sending additional troops to Saudi Arabia and the United Arab Emirates, largely to bolster air defenses. But those moves alone are viewed as unlikely to be enough to prevent further Iranian actions. **The question circulating now through the White House, the Pentagon and Cyber Command's operations room is whether it is possible to send a strong message of deterrence with a cyberattack without doing so much damage that it would prompt an even larger Iranian counterstrike. At least three times over the past decade, the United States has staged major cyberattacks against Iran**, intended to halt its nuclear or missile programs, punish the country or send a clear message to its leadership that it should end its support for proxy militant groups. **In each case, the damage to Iranian systems could be repaired over time. And in each case, the effort to deter Iran was at best only partly successful**. If the American charge that

Iran was behind the attack in Saudi Arabia proves accurate, it would constitute the latest example of Tehran shaking off a cyberattack and continuing to engage in the kind of behavior the United States had hoped to deter. The most famous and complex effort was a sophisticated sabotage campaign a decade ago to blow up Iran's nuclear enrichment center using code, not bombs. The Obama administration later began a program, accelerated by Mr. Trump, to try to use cyberattacks to slow Iran's missile development. And this past June, Mr. Trump approved a clandestine operation to destroy a key database used by the Iranian military to target oil-carrying ships — and canceled a traditional missile strike he had ordered to respond to the downing of an American surveillance drone. The June cyberattack, according to two American officials, also did damage that Iran has not yet detected. "Cyber can certainly be a deterrent, it can be a very powerful weapon," said Senator Angus King, the Maine independent who is a chairman of the Cyberspace Solarium Commission, created by Congress, that is examining American offensive cyberstrategy. "It is an option that can cause real damage." ImageA Saudi military spokesman during a recent news conference in Riyadh displaying what he said were pieces of Iranian cruise missiles that hit the kingdom&rsquo;s oil fields. A Saudi military spokesman during a recent news conference in Riyadh displaying what he said were pieces of Iranian cruise missiles that hit the kingdom's oil fields.Credit...Fayez Nureldine/Agence France-Presse — Getty Images **Mr. King and other experts said Iran would most likely respond to a cyberattack with one of its own, given the vulnerabilities that exist in the United States and the hyper-connected nature of American life. But current and former intelligence officials say a cycle of retaliation need not be confined to one military domain.** Just as the United States responded in June to the Iranian downing of a drone and sabotage of oil tankers with a cyberattack, **Iran could respond to an American cyberoperation with a terrorist attack by a proxy force or a missile strike.** The Pentagon has long held that a cyberattack could constitute an act of war that requires a physical response, and there is no reason to think that Iran would not pursue the same policy. One senior administration official recently acknowledged that even Gen. Paul M. Nakasone, the commander of Cyber Command and the director of the National Security Agency, has warned Mr. Trump and his aides that **the cyberarsenal is "no magic bullet" for deterring Iranian aggression in the Middle East.** In war games — essentially online simulations — held before the attack on the Saudi oil fields, officials have tried to figure out how Iran's increasingly skillful "cyber corps" would respond to an American cyberattack. These Iranian fighters have already racked up a significant record: wiping out 30,000 computers at Saudi Aramco, freezing operations at American banks with a "denial of service" attack, and crippling a Las Vegas casino. Last year, they began to study the ins and outs of election interference, according to private experts and government studies of the 2018 midterms. When General Nakasone was nominated for his job, he acknowledged that one of the biggest problems facing Cyber Command was that it had not cracked the deterrence problem. Nations that are attacking the United States via cyber "do not think much will happen to them," he told Senator Dan Sullivan, Republican of Alaska. "They don't fear us." In his first 18 months in office, General Nakasone has raced to bolster Cyber Command's authority to act preemptively — and its preparations to respond to attacks. New, classified directives given to him by Mr. Trump, and built upon by Congress, allow Cyber Command to place "implants" of malicious software inside foreign networks without lengthy approval processes that run up to the president. Congress has called such efforts part of "traditional military authority." Iran has reportedly been a major target — no surprise, since General Nakasone was a key player in designing a plan called "Nitro Zeus" to shut down Tehran and other Iranian cities in the event of a war. The idea was to put together an attack so devastating that Iran might surrender without a shot being fired. The 2015 nuclear agreement between the Iranian leadership and President Barack Obama eased the threat of war, and the American cyberoperations plan was put back on the shelf, at least until recently. **At the Pentagon, and even at Cyber Command, many senior officers are cautious about cyberwarfare, arguing that it is difficult for such weapons alone to deter an enemy.** ***The attack using the "Stuxnet" virus that crippled Iranian nuclear-enrichment centrifuges a decade ago was successful in a narrow sense: It blew up 1,000 of the 5,000 centrifuges up and running at the time. But when it recovered, Iran built upward of 14,000 more, and counterattacked by crippling Saudi Aramco's computer systems.*** Iran&rsquo;s Salman oil field. Shutting down Iran&rsquo;s oil fields and refineries would not be easy, and even if it worked, there is no assurance that conflict with Iran would not escalate. Iran's Salman oil field. Shutting down Iran's oil fields and refineries would not be easy, and even if it worked, there is no assurance that conflict with Iran would not escalate.Credit...Ali Mohammedi/Bloomberg **A long-running series of cyberattacks has slowed but not stopped Iran's missile program** — and Iran has continued to provide thousands of short-range rockets to Hamas and other terrorist groups. The Saudis are studying whether a new generation of Iranian-made missiles were central to this month's attack on its oil facilities. The Pentagon and other military officials have told the White House that neither another cyberattack nor the new deployment announced Friday will likely prove robust enough to re-establish deterrence and prevent another attack by Iran on United States allies. Part of the problem is that most cyberactivity is clandestine, so it is easy for a government to play down the consequences of an attack or deny it even took place. But some people who favor stepping up cyberoperations suggest that officials are simply thinking too small. If a cyberstrike is damaging enough — taking a refinery offline or shutting down an electric grid, for example — it would be hard to hide. That might have a much more deterrent effect than the smaller bore operations the United States has undertaken so far, they argue. But such **a devastating cyberoperation would also increase the risk of escalation** — just as a bombing run on the oil refineries would. Iran, or any other adversary, could claim that people were killed or injured, and that might be difficult to disprove. A key element of deterrence is ensuring that an adversary understands the other side's basic capabilities. Unlike nuclear weapons, though, which are widely understood, the American cyberarsenal is shrouded in secrecy, for fear adversaries will develop counter measures if even basic capabilities are known. General Nakasone has argued that his cyberwarriors must be roaming cyberspace "persistently engaging" enemies — a euphemism for skirmishing with adversaries inside their networks. "We must 'defend forward' in cyberspace, as we do in the physical domains," he wrote in a Defense Department publication in January. "Our naval forces do not defend by staying in port, and our air power does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace." But there is a growing consensus within Cyber Command that if cyberweapons are going to shape the actions of adversaries, they must be used in combination with other elements of power, including economic sanctions, diplomacy or traditional military strikes. Mr. King, the Maine senator, sees the decisions over the next few weeks on Iran as a test case. "The president's instinct is not to get in a shooting war, and I think he is right about that," he said. "So the question is how do we respond?" He argued that there was no urgency. "This was not a strike on New York City," Mr. King said. "This was not even a strike on Riyadh. There needs to be a response. But there is time to pause and take a deep breath and consider all of the options — one of which is cyber — but also to think about how we de-escalate the situation."

Further Reading

Abdollah, Tami. 6-24-2019, "Iran Increases Cyber Attacks on U.S. Gov't, Infrastructure: Cyber Security Firms," Insurance Journal, https://www.insurancejournal.com/news/national/2019/06/24/530257.htm

Anderson, Collin, 1-4-2018, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," Carnegie Endowment for International Peace, https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

Groll, Elias. 9-27-2019, "The U.S.-Iran Standoff Is Militarizing Cyberspace ," Foreign Policy, https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/

Volz. Dustin. 11-4-2019, "U.S. Launched Cyberattacks on Iran ," WSJ, https://www.wsj.com/articles/u-s-launched-cyberattacks-on-iran-11561263454

Zak Doffman, "Secret U.S. Cyber Mission Devastated Iran's Attack Capabilities, Officials Say," Forbes, https://www.forbes.com/sites/zakdoffman/2019/08/29/secret-cyber-mission-devastated-irans-attack-capabilities-us-officials-say/

Russia

For years, Russia was the largest counterbalance to US supremacy in the world. With the rise of China, that status is up for debate. However, no one can deny that Russia is still a threat to US global interests that must be addressed.

For as long as we have had computers, we have had data being intercepted and stolen. At first, the data thefts were done in hard copy with disks being taken or duplicated. As data moved to the electronic transmission system, nations began to intercept and decode our messages. And today, there is a whole world of hacking, data interception, and disinformation that nations can use against each other, and one nation that has specialized in all forms of this new warfare is Russia. Although their cyber operations task forces are kept as much of a secret as any other nations, it is assumed by security experts that Russia has second largest cyber operations division in the world; second only to China. Their operations can be seen if you take a look at any real time map of cyber-attacks. Maps on websites like the Real Time Attack Map show you the location and destination for known cyber-attacks. Now every attack is a government operation, but many are. Follow the track to sites in Eastern Europe and Russia and you see the issue. Whether they are done by the Russians or by Russian associates, attempted data breaches are growing in number.

Looks pretty until you realize you should be terrified. https://cybermap.kaspersky.com/

The Russian specialize in every form of hacking. In 2010, 2014 and 2017, the Department of Defense notes that Russians gained entry into databases of federal employees for much the same reasons that the Chinese also infiltrated US federal employee databases. However, there is one area that the Russians have found that they are especially good at, and that is election meddling. Political affiliations aside, very few people doubt that the Russians have played a hand at disinformation and hacking of political candidates in the past. In 2016, breaches of the DNC and the private email servers Hillary Clinton leaked thousands of emails that damaged her credibility as well as showed the strategies of the DNC in the upcoming election. Fake social media accounts on Facebook and Twitter recruited unsuspecting Americans into promoting false and misleading material on candidates. A greater worry is that as more and more election voting machines are linked to remote servers and networks, they will become open to hacking and vote total changes. Already, people have shown how it is easy to change vote totals with a small program you can find online and a flash drive. With access to the internet and the weight of a foreign government, there is no telling how much damage could be done.

Enter US offensive cyber operations. The US has hopped to use their newfound power as granted in 2015 and by congress in defense spending bills that followed to counterbalance Russia. The "defense forward" posture that we maintain could be used to shut down Russian disinformation campaigns or limit access to their agents. Their bots could be disabled before they have a chance to recruit real Americans, and if we can find and take out the centers where vote total hacking might occur from, we can stop any future election harm.

We already have shown success in cyber operations against Russia. In retaliation to 2016, the US launched an attack in 2018 to disable the Russian power grid as a warning shot that future intervention would not be tolerated. Although it didn't achieve all of it's objectives, it achieved enough of them to be labeled a success by the US military.

The big danger from this is much the same as from Iran and China; retaliation and miscalculation. However, the threat from Russia is much larger. Unlike China, they have a large and accurate nuclear missile arsenal and an up to date navy and an air force that has been training for years to fight an American strength adversary. The Russians also have a primed and large first strike cyber force of their own that they will not hesitate to use if they feel like the US has pushed the bounds ton far and is getting too close. This trigger on miscalculations means that both nations are at an elevated risk of an attack or a false attack and retaliation.

As a debater, this contention is pretty up in the air. There is good evidence on both sides to say that cyber operations are needed and that they are not needed. The uniqueness and solvency on the pro is pretty good about how Russia has posed a danger to us in the past and how we can get them now, but on the con, there is good evidence that says that any attack or threat of an attack would be met with a first strike or a crippling retaliation. In this case, newer is better. Also, weight the warrants of your evidence. Why does your card override your opponent's? The weighing mechanisms in this debate will be very critical as both sides are evenly balanced and it will come down to the explanations in the summary and final focus if you want to win.

Sample Evidence

Russia is running covert online opts. We need offensive cyber operations to find and take out the real attackers

O'Flaherty, Kate. "Russian Hackers Disguised As Iranian Spies Attacked 35 Countries," Forbes, https://www.forbes.com/sites/kateoflahertyuk/2019/10/21/nsa-and-ncsc-warning-russian-hackers-disguised-as-iranian-spies-hacked-35-countries/#3c5240126428

Russian cyber actors disguised themselves as Iranian spies so they could stealthily orchestrate attacks on countries across the world, the U.S. and U.K. said today (October 21) in a joint statement. **The so**-called **Turla group**, which is also known as Snake or Uroburos, **hid in plain sight by acquiring Iranian tools and infrastructure to perform their attacks,** the U.K.'s Cyber Security Centre (NCSC) and U.S. National Security Agency said. In total, **35 countries were attacked, including the U.K. and U.S.,** with a "large cluster" of victims based in the Middle East. Victims included military establishments, government departments, scientific organisations and universities. **Turla used implants derived from Iranian hackers' previous campaigns, "Neuron" and "Nautilus"–which they obtained through compromising the Iran based hackers themselves.** "Identifying those responsible for attacks can be very difficult, but the weight of evidence points towards the Turla group being behind this campaign," said Paul Chichester, the NCSC's director of operations. Today In: Innovation In a defiant statement, he sent a warning to attackers that "even when cyber actors seek to mask their identity," it's possible for intelligence agencies to identify them. The NCSC added that in some instances, it appeared that the implant had first been deployed by an IP address associated with an Iranian APT group, which was later accessed from infrastructure associated with the Russian group Turla. This suggests Turla effectively took control of victims previously compromised by a different actor, the NCSC said. Russian group Turla targets government, military, technology, energy and commercial organizations. The NCSC published two advisories on the use of Neuron and Nautilus tools by Turla in late 2017 and early 2018. NSA and NCSC warning and the Russia plausible deniability problem **Russia is one of the most sophisticated cyber actors in the world, so it's no surprise that the country's hackers are finding new ways to confuse and stay hidden.** Plausible deniability is an ongoing issue in the increasing complex cyber warfare environment. "Cyberspace is not regulated in the same way as land, maritime, air or space when it comes to international actions relating to war with an equivalent of the Geneva Conventions and Protocols or an Outer Space Treaty," says Philip Ingram, MBE, a former colonel in British military intelligence. "To avoid political embarrassment and the possibility of political repercussions, the use of a plausibly deniable outlet is key: Without substantive proof, there can never be substantive repercussions." Meanwhile, the Russians have a doctrine called маскировка (maskirovka) which encourages "masking" or deception. "This is central to all they do; it allows them to interfere overseas but be able to deny it. We saw this with the attack on

Sergei Skripal in Salisbury last year," Ingram says. Ingram also points out that Iran is "a closed country with little access to western academia and training" yet apparently it appears to be able to "mount some of the most sophisticated cyber incidents." "We hear the same of North Korea, who should have zero access to technology, academia, and extremely controlled access to the internet," Ingram adds. Could it be that Russia is behind more incidents than people think? "A smudge of what could be a Russian fingerprint sits over many incidents," says Ingram. "Not enough for real proof, but something that always seems to be there."

There is no way we can win a cyber war with Russia

Greenberg. Andy. 2019 "Iranian Hackers Launch a New US Campaign as Tensions Mount," Wired, https://www.wired.com/story/iran-hackers-us-phishing-tensions/?fbclid=IwAR2T_Yo47vnwWH0DmOuPWJgGh5TMy6Dhty4RzBAe8jmXMao6dRsNWjRACfk

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."

Further Reading

Ben. Buchanan/ "Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration," Carnegie Endowment for International Peace, https://carnegieendowment.org/2016/12/13/russia-and-cyber-operations-challenges-and-opportunities-for-next-u.s.-administration-pub-66433

Doffman, Zak. "Cyber Warfare: Army Deploys 'Social Media Warfare' Division To Fight Russia," Forbes, https://www.forbes.com/sites/zakdoffman/2019/08/01/social-media-warfare-new-military-cyber-unit-will-fight-russias-dark-arts/

Nast, Condé. "How Not To Prevent a Cyberwar With Russia," Wired, https://www.wired.com/story/russia-cyberwar-escalation-power-grid/

Thornton, Rod. (2019) Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom, Journal of Cyber Policy, 4:2, 257-274, DOI: 10.1080/23738871.2019.1640757

Washington Post, 2-27-2019, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," 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

North Korea

North Korea is a nation that embodies the idea that when you meet a superior opponent on the field of battle, you have to find a way to outflank their advantage or you will be crushed by superior brute force. In this situation, North Korea is a recluse nation of only 24 million people. Since the ceasefire brought an end to major hostilities in the Korean War in 1953, the small hermit nation has been looking for ways to gain the advantage against the nation that they felt unfairly divided the Korean peninsula. Under the leadership of the Kim family, for over 50 years, the nation has plunged their people into a state of poverty and fear while fueling a growing military regime. In recent years, this has expanded to include nuclear arms as well as one of the most elite cyber operations units in the world.

North Korea, for all of their saber rattling, knows that in a direct head on conflict with the United States, they would not last long. Their air force is outdated with many planes dating back to the Vietnam War era. Their navy is just as old and is only 1/10th the size of the American fleet. They possess no satellite guidance or communication systems, nor do they have any modern equipment. What they do have is an advanced cyber operations team that has worked for years to be the best in the world. Their primary goal when they were created was to steal small amounts of money from banks and individuals in other nations to fuel an economy that had stagnated due to UN and US sanctions. Now, their focus has shifted to that of an offensive capacity. Again, data is limited, but defectors have said that their forces are training for a day when they will be called upon to cripple the US civilian sectors to distract the government from the war in Korea. This will be done because the top military leadership in Korea knows that it civilian targets are easier to attack than military targets and the US might be forced by unpopular opinion to end hostilities to end the cyber-attacks.

In this regard, an offensive cyber operations base would function like it would against Iran. Targets of value would be chosen for a covert cyber first strike and neutralized when and if the military registered that these targets had grown to be a threat. The difference between this threat and the others listed earlier in this brief is that the leader of North Korea is paranoid about losing power. A preemptive attack might easily send him into a frantic series of miscalculations that leads him to use his limited atomic weapons against our allies in the region like Japan, the city of Soule which is only 40 miles from the DMZ, or against the 40,000 US troops stationed along the DMZ.

When debating this contention, the pro will need to work on winning that North Korea really has the technology and expertise to launch a cyber operation against the US. We have been conditioned by years of media satire and our own leaders that North Korea is a joke. This desensitization has put teams that run this at a disadvantage because few people will be willing to buy this without explanation of the evidence. You will need to devote time in the rebuttal to clearly explain that this isn't a joke, this is a serious threat. On the con, you can argue a realism standpoint here. The Kim family values power, and they would not use cyber operations against the US nor do they have the means to do such. This however is mostly speculative as the evidence on the pro side is stronger. Your best bet is that North Korean retaliation poses no threat. Use the desensitization that I mentioned that the pro would have to deal with to your advantage and cast doubt on the ability of the North Koreans to launch anything that might threaten the US.

Sample Evidence

North Korea is years ahead of the US in cyber operations. We need to catch up or we will lose the race

Tai, Crystal. "Is North Korean cyberwarfare as big a threat as its nukes?," South China Morning Post, https://www.scmp.com/week-asia/geopolitics/article/2187363/north-korean-cyberwarfare-big-threat-its-nuclear-weapons

North Korea's nuclear weapons programme has for several years posed a growing threat to international security – to its neighbours in the South and to the rest of the world. However, the hermit kingdom has also been fashioning another weapon with which to harass the global community: it has **carefully and quietly honed its cyberwarfare capabilities to the point that today**, according to cybersecurity experts, its **hackers are among the best in the world. In terms of speed – a crucial weapon in the arsenal of a cyber hacker – they are second only to Russian intrusion groups and ahead of the Chinese**, according to American cybersecurity technology company Crowdstrike. Watch out. North Korean hackers are coming for your bitcoin It's not just that banks, governments and institutions stand to lose millions if not billions of dollars; **personal identities and information can be stolen and ransomed, and entire economies could theoretically be dismantled. North Korean leader Kim Jong-un has been quoted as saying nuclear arms go hand in hand with cyber weapons.** "Cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly," he said, according to a report by Washington-based think tank the Centre for Strategic and International Studies. : "North Korea's offensive cyber capabilities could supplant its nuclear arsenal and ambitions for intercontinental ballistic missiles, if North Korea were to give up nuclear capabilities, as main pillar of deterrence," said Jakob Bund, a research associate at the University of Oxford's Global Cyber Security Capacity Centre. "From a deterrence perspective, both sets of capabilities cause similar concerns." To Geoffrey Cain, an American journalist and Korean peninsula specialist, North Korean hacking "doesn't kill populations, but I do think as a threat it's more up front than nuclear weapons". "North Korea will never launch the first nuclear strike because that will turn them into a crater," he said, adding that c**yberwarfare**, on the other hand, **was a real and immediate threat that could be used in guerilla fashion. "It can be used covertly and secretly to steal secrets, shut down an electrical grid. Hackers can mess with markets, mess with financial institutions, sell off assets."** Since the early 2010s, hacking attacks from the North have increased in frequency – from one attack in 2015 to four in 2017, and four last year as well. North Korean hackers blamed for wave of cyberattacks on banks Last October, North Korean hackers were suspected of breaking into 30 South Korean computers to steal confidential information about next-generation fighter aircraft and other weapons. Two months later, hackers from the North stole personal information such as the names, addresses and birth dates of almost 1,000 defectors living in South Korea from a refugee resettlement centre – potentially endangering their families and friends still living in the hermit kingdom. Other North Korean cyberattacks have ranged from being financially motivated to destructive and malicious, with the goal of breaking down institutions and wreaking havoc upon organisations and entire societies. Listen to the Asia Briefing podcast According to an October report from cybersecurity firm FireEye, an elite North Korean hacking group nicknamed Apt38 has attempted to steal US$1.1 billion in funds from various institutions around the world. The group's most lucrative hack yet was the theft of US$571 million in cryptocurrency from Japanese bitcoin exchange Coincheck in January 2018, while in 2016 it funnelled US$81 million from the central bank of Bangladesh. South Korea's bitcoin exchange lost more than 40 billion won (US$35.5 million) to hackers in June last year. In 2017, **Pyongyang was also allegedly responsible for the notorious WannaCry ransomware attack, an act of cyberterrorism that saw data stolen from 200,000 computers in 150 countries – causing billions of dollars in damage**. The hackers demanded payment in return for handing the data back, and received more than US$130,000. Despite the nation's widespread poverty and limited technology – only a small portion of the population has access to the nation's "Kwangmyong" intranet services – **experts say North Korea's cyber capabilities are sophisticated and well developed.** "During the Soviet era, North Korea was not even able to make colour televisions, but still they conducted nuclear weapons tests and even looked into developing a space programme," said Jang Ji-hyang, a senior fellow in political sciences at South Korea's Asan Institute for Policy Studies. North Korea's leader has charmed Trump, Xi and Moon. But are they all just keeping up with the Kims? "**When dictatorial regimes like North Korea decide to achieve something new, they exploit public human resources and force them to make that happen."** North Korea has been investing in its cyber capabilities since the early 1990s, according to Danielle Cave, deputy head of the Australian Strategic Policy Institute's International Cyber Policy Centre. "It's been reported the regime has long been sending its best students to study computer science and cybersecurity in China's top universities," she said. "Estimates put North Korea's cyber army at about 6,000 hackers, and their cyber capabilities are both a weapon and also a source of income for the country." North Korea's cyber capabilities are both a weapon and a source of income for the country, experts say. Photo: K.Y. Cheng North Korea's cyber capabilities are both a weapon and a source of income for the country, experts say. Photo: K.Y. Cheng Share: What sets North Korea apart is the single-mindedness with which promising talent is recruited, according to Bund from the University of Oxford. "Children with particular skills in maths or other scientific subjects are identified at an early age, with their education subsequently geared towards a career in the country's cyber forces." Bund said such recruitment was organised by Bureau 121, the nation's principal cyber operations unit. Best of the Best: South Korean school trains elite hackers to fight Pyongyang in cyberspace "The unit was likely created around 2013 and is embedded into the Reconnaissance General Bureau – North Korea's main foreign intelligence service, which reports to the Korean People's Army," he said. The unit's cyber operations largely take place in South and Southeast Asia, as well as a North Korean-owned hotel in Shenyang, China, that serves as an unofficial headquarters. **At the core of these activities is a hacking collective frequently referred to as the Lazarus Group,** which the United States Department of Homeland Security and the FBI believe to be controlled by the North Korean government. DEFENCELESS Unfortunately, there is little nations and institutions can do to protect themselves from North Korean hackers. Oxford researcher Bund said even banks, conglomerates and government institutions with high levels of cybersecurity had been unable to protect themselves. "In the case of the Sony Pictures Entertainment hack for instance, the FBI concluded that the hackers, once inside the networks, unleashed an offensive operation that would have brought down 90 per cent of companies targeted," he said. "Conflating an unsophisticated attack with an unsophisticated threat actor can prove a dangerous fallacy," Bund added, explaining that simple methods of hacking have often allowed the rogue state to break into a system. Experts say it is unsafe to negotiate cyber peace in conjunction with nuclear issues. Photo: EPA Experts say it is unsafe to negotiate cyber peace in conjunction with nuclear issues. Photo: EPA Share: Over recent years, North Korean hackers have become more sophisticated in their techniques, tools, and procedures, according to Jenny Jun, a former cybersecurity consultant who is currently an international relations PhD researcher at Columbia University. "They started out with rudimentary denial-of-service attacks on websites, a tactic more often associated with individual hacktivists with relatively low skills," she said. "But as the recent bank heists show, they have become much bolder and more systematic in the course of about five years. The scarier thing is that much like the nuclear issue, there is not too much the victims can do to credibly deter North Korea from engaging in these activities." Given the very real and constant threat of North Korean cyberwarfare, and the danger it poses, it's difficult to understand why such attacks are not being addressed at any of the high-level talks with the hermit kingdom. Can North Korea copy Vietnam's economic miracle? The short answer is that while cyber issues are important, it's unsafe to negotiate cyber peace in conjunction with nuclear issues, experts say. **Another part of the problem is a lack of understanding surrounding the capabilities of – and damage caused by – such attacks, according to Jang,** from the Asan Institute for Policy Studies. "There are no global rules for cyber warfare yet. **And it's difficult for even the US and other [followers of the] liberal order and international norms to initiate making boundaries in the uncertain environment of cyberspace," she said. "All actors can do is check each other's moves." Ultimately, experts warn that even nuclear disarmament by North Korea doesn't mean it will give up its highly lucrative and disruptive cyberattacks. From Singapore to Canada, fans of North Korea praise its 'juche' ideology and supreme leader "Under one man's dictatorship, full disarmament does not mean fully integrating into the international community,"** Jang said. "**Kim Jong-un will keep his hacking units to ensure his regime's survival."** Others, like Cave from the Australian Strategic Policy Institute, agree that North Korea will never fully disarm itself. "There is a clear disconnect between what the regime claims publicly and does privately," she said. "Unfortunately, because they earn income and steal secrets that they believe are valuable, the world is stuck with North Korean hackers for many years to come."

Cyber warfare will lead to a North Korean war

Capaccio, Tony. 11-3-2019, "North Korea's cyber warfare capability grows, U.S. general says," Honolulu Star-Advertiser, https://www.staradvertiser.com/2012/03/28/breaking-news/north-koreas-cyber-warfare-capability-grows-u-s-general-says/

North Korea's military has been increasing its ability to launch cyber-attacks against American and South Korean forces, the top U.S. commander in the region said. "**North Korea employs sophisticated computer hackers trained to launch cyber infiltration and cyber attacks**," Army General James Thurman, the commander of U.S. Forces Korea, said in testimony prepared for a congressional hearing today in Washington. **"Such attacks are ideal for North Korea" because they can be done anonymously, and they "have been increasingly employed against a variety of targets including military, governmental, educational and commercial institutions."** Thurman's presentation for the House Armed Services Committee's annual regional overview presented a starker appraisal of North Korea's threat to South Korea and to U.S. forces than did his predecessor, U.S. Army General Walter Sharp, in testimony last year. Sharp didn't cite cyber attacks as part of the North Korean arsenal, and Thurman spoke of continued improvements in conventional weaponry. North Korea can attack Seoul "and can deliver both high explosive and chemical munitions with little or no warning," Thurman said. **The regime** in Pyongyang also continues to improve "the capabilities of the world's largest special operations force, which **includes 60,000 soldiers trained in** a variety of **infiltration methods,"** he said.

Further Reading

Korean Economic Institute "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance," http://keia.org/publication/north-koreas-cyber-warfare-and-challenges-us-rok-alliance

Kowalewski, Annie. 4-22-2018, "DPRK Cyber Capabilities," Georgetown Security Studies Review, https://georgetownsecuritystudiesreview.org/2018/04/22/dprk-cyber-capabilities/

Stent, Dylan. 9-23-2018, "Can the Cyber Terrorism Tactics of North Korea Be Deterred?," National Interest, https://nationalinterest.org/blog/skeptics/can-cyber-terrorism-tactics-north-korea-be-deterred-31662

"North Korea’s Cyber Operations," No Publication, https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations

Wright, Morgan. 6-5-2018, "North Korea's nuclear threat is nothing compared to its cyber warfare capabilities," TheHill, https://thehill.com/opinion/cybersecurity/390601-north-koreas-nuclear-threat-is-nothing-compared-to-its-cyber-warfare

Humanitarian/Social

"War is hell." The authors of this quotation didn't just mean for this to be aimed at the soldiers but for all of those affected by war. Because cyber war is done online with no fancy explosions, no invasions, no shooting, people think that the action is "out of sight and out of mind." However, as with most things in life, the correct motto should be "Every action and an equal and opposite reaction." Action rarely takes place in a bubble and rarely does it not have unintended consequences.

When researching for this section, there were a few surprises that came up. The development of artificial intelligence was an argument that I had not thought to look into at first, but after reading why a cyber operations system would need it, it makes complete sense to me. This will likely be one of the harder arguments to get judges to buy just because of the lack of a solid impact. In this debate, the team that wins will be the team that finds that impact and takes full use of it.

One argument that I did not explore was the impact to democracy. To me, this argument seems like it should be an impact to the legality contention, but I have seen that some teams are running this as an independent main point. The argument is that offensive cyber operations run counter to the ideas that establishes a democracy like law and order. The harm then would be the erosion of democracy and modeling by other nations that would then erode their democracy. Again, I feel that this is better left as an impact to the legality contention as the link work is too similar to the internal link work for the legality point.

These points are going to be refreshing to judges as most of the debates are going to come down to the big 4 countries and the threats that they pose. By the time we hit December and tournaments like George Mason and Dowling, judges will be longing for anything that doesn't talk about election meddling or a rouge nuclear bomb in the Middle East or East Asia. I think that because of this, these points will get better as the topic ages.

Civilians

It has been said that in war, there are no such things as unintended targets. Everything has a purpose and serves a greater end. But there is also a rule of war that demands that those wishing to remain outside the conflict are allowed to seek refuge and safety from the conflict. To this end, in traditional war, the targeting of civilians has been forbidden for years by international treaties like the Geneva Convention as well as both national military law and international law. Attacks are planned to minimize civilian deaths and structural harm and it is seen as uncivilized for an enemy army to intentionally target the infrastructure of the populace unless the centers are used for military purposes. So great is the desire to reduce civilian deaths that some military forces have built their bases and have stationed troops in civilian areas knowing that should air strikes be called in, the enemy would be hard pressed to fire into a civilian neighborhood.

However, these rules of war were designed for a simpler time when the enemy met on the field of battle and declared their open intentions to destroy the military fighting power of another. The reason that these laws were instituted was that in the past, civilians in the past have proven themselves to be a soft target that one army could use as leverage during an attack. During his march to the sea, the Northern general Sherman specifically targeted civilians and their property hoping that their demoralization would drive the South to surrender. In Vietnam, under the stress from repeated ambushes, American soldiers were known to target civilian villages hoping to send a message to their attackers that they were going to take much more.

Under the concept of an offensive cyber offensive or war, what standards of war exist? Will armies and militaries hold true to the rules of war and leave civilian system alone or will they be the first to be destroyed? After all, their systems are much easier to hack and disable than military targets, and crippling a power grid would double the burden that the government would have to face as they confronted both a civilian relief effort as well as cyber war. What of the civilians that would be harmed by these attacks? How long and to what degree would shutting down a power grid or crippling a hospital system have on a desperate populace? If we were attacking an enemy whose soul goal was to harm Americans, would this in fact make civilians a priority target?

On the flip side, could our war planning for an offensive cyber operation solve the potential for disaster? Against an enemy state who is already looking to attack our civilian power grid, both the concept of a first strike as well as a strategic defense and deterrence are strong obstacles for an attacker to overcome. When evaluating the harm from a cyber attack from an enemy state or group, the deaths and disaster caused might be far larger than the harm caused by any retaliation caused as a result of US offensive cyber operations as we would have time to put into effect our response plan.

When debating this contention, you will be debating a very emotional and ethos driven argument. The impact cards on this debate, at least form the US perspective aren't really all that strong in terms of a numbers debate, so you will need to win the hypothetical of "what if" this event happened. It might not hurt to ask the judge to imagine their lives without electricity for a few days and how they would react. If however you need numbers, if you could tie the loss of power back to loss productivity or work or a shutdown in the financial sector, you can get a quantifiable economic impact. For other things like health care systems or transportation, talk about how that means people are denied critical access to lifesaving services and this causes deaths. Again, numbers won't be solid, but they will be there. On the con, you need to out weight the fact that a retaliation to an offensive cyber-attack would be as bad if not worse than being attacked first by an enemy. You might be able to find defense that says our civilian systems are safe, but that evidence will be sketchy at best as almost no expert can say that with a straight face.

Sample Evidence

Cyber operations cripple healthcare systems

Humanitarian Law & Policy Blog, 11-14-2018, "The potential human cost of cyber operations: Starting the conversation," https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/

The healthcare sector Of special importance is cybersecurity and risk in the healthcare sector, as is the ability of hospitals and other services to continue providing healthcare to civilian populations when affected by cyber attacks. Cyber attacks on—and infections in—the healthcare sector are **on the rise.** Ransomware infections that impact the availability of medical data or systems, and that affect the provision of health services are a growing challenge. WannaCry underlined the complex question of the security posture of the health sector. While the consequences of a coordinated attack that would affect all health care providers in one area and thus prevent referral to a fully functioning facility remain unclear, they are concerning. In parallel, a dangerous trend is emerging where actors seem to be targeting healthcare sector suppliers. Attacks tampering with medical devices could potentially lead to the administration of wrong doses, impact the technical processes of diagnosis or affect the proper functioning of life-supporting instruments such as pacemakers. In extreme cases, this could potentially result in life-threatening risks.

Cyber operations target the power grid, hurting civilians who need electricity and heating

Humanitarian Law & Policy Blog, 11-14-2018, "The potential human cost of cyber operations: Starting the conversation," https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/

Cyber-attacks against industrial systems Cyber-attacks targeting industrial systems are developing rapidly, both in terms of technical capabilities and an increase in the number of threat actors involved. They may affect other sectors providing essential services for the population—such as, for example, electricity and water—and in specific cases potentially result in physical damage. The energy sector was estimated this year to be the one most commonly attacked (38.7%) among industries affected by cyber-attacks on facilities with industrial control systems (ICS). While not many detailed examples are available to the public, the threat landscape is evolving and attacks are becoming more sophisticated. For example, the 2016 cyber attacks that affected the Ukrainian electricity grid demonstrated an increase in automation compared to those of 2015. There are also several cases of cyber attacks affecting power plants, including nuclear power plants. Persistent cyber operations' campaigns show how attackers try to gain access to operational systems, which potentially could be used later for more disruptive purposes. Water treatment facilities are also increasingly dependent on ICS, which potentially renders them vulnerable to cyber-attacks. For example, in 2015 attackers were able to manipulate valves to cause a change of the chemical mix at a water treatment facility. Fortunately, in this case the change was detected, and the negative effects minimized. Recently, ransomware infections occurred at the outset of a natural disaster (a hurricane). This highlights how cyber attacks that take place in difficult situations can complicate recovery. Past track record of publicly known cyberattacks against industrial facilities demonstrates their feasibility and ability to cause physical damage, as evidenced by cases such as Stuxnet, the 'inability of a proper shut down of a furnace [at a German steel mill] resulting in unexpected conditions and physical damage to the system', and the disruption caused by the Triton malware already mentioned. Attacks on critical networks and the ability to interfere with industrial equipment may require specialised resources, like the access to expertise and equipment. Cyber operations targeting industrial sites could potentially be very dangerous and carry with them real risk of humanitarian consequences.

US PowerGrid is vulnerable to a cyber-attack. Need a clear defense now

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."

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-itskind-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.**

Further Reading

Anthony J., 10-28-2019, "Playing with fire: Global offensive cyber operations," TheHill, https://thehill.com/opinion/cybersecurity/467701-playing-with-fire-global-offensive-cyber-operations

Gronberg, Katherine. "The U.S. Military Must Defend Its Power Grid," SIGNAL Magazine, https://www.afcea.org/content/us-military-must-defend-its-power-grid

Halpern, Sue. 7-18-2019, "How Cyber Weapons Are Changing the Landscape of Modern Warfare," New Yorker, https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

Schmitt, Michael N. 5-27-2019, "Wired warfare 3.0: Protecting the civilian population during cyber operations," Cambridge Core, https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/wired-warfare-30-protecting-the-civilian-population-during-cyber-operations/7C8F20A9B9F4ED0A49A3C8B07C0BC80D

This, Entering. 5-29-2019, "The potential human cost of cyber operations," International Committee of the Red Cross, https://www.icrc.org/en/document/potential-human-cost-cyber-operations

Artificial Intelligence

The biggest scare that I had this year was at the Valley Mid-American Cup when I was tabbing PF debate. I had just finished round 2 and all ballots had been entered via the online system. I went to pair round 3 only to find that it was already paired with rooms and judges assigned. I was perplexed as to why this was. I checked the time stamp at the bottom of the page and saw that the round had been paired recently. I knew that the tournament director and the LD tab staff were at another building, so I figured they saw that the round was done and paired the round to help out. I called over and asked if this was the case and to my horror, I discovered that not only had they not done this, but they were about to call me to ask if I had paired policy for them. It was only a few days later after talking to a few other coaches that we discovered that a new feature added to Tabroom this year was the ability for the tournament to auto pair all arounds after the presets. The goal of the development staff is that someday, debate tournaments might be able to run like a plane in auto pilot mode. Ladies and Gentlemen, Skynet is real and it wants our ballots.

What this illustrates is that the concept of automation is infiltrating every aspect of our lives. Ever since the first computers replaced switchboard operators, people have dreamed of a world where our lives could be put in the hands of automation. After all, a computer can do things hundreds of times faster with no complaints about working hours, they don't need pay, and they rarely make mistakes. In this regard, the concept of artificial intelligence or smart programs that can sort data for military applications was not only a dream but an inevitability. When we look at the map of all cyber-attacks occurring in real time, one can see the daunting prospect of the humans that would have to sort through all of that data to find out which ones were malicious, which ones were targeted at the government, and which ones were the work of foreign agents and which agents they were. This all would have be done as the attackers were allowed to escape into the void of the internet, and it would have to be done 24/7/365. To solve the demands of sheer people power that would be required for this operation, the government has decided to develop a system of smart algorithms that can sort the data at the blink of an eye. This new form of artificial intelligence can detect a hack, track it, and determine an appropriate response and then implement a response with little to no input from a human user. This saves on both the human time needed for a response as well as minimizing errors in data sorting.

With any new technology, there are benefits to the civilian markets. Many military devices and creations have worked their way down to the civilian market. One day, the technology that allows us to sort data from cyber-attacks might be used to help the postal service sort mail, help us sort our email, help schools coordinate admissions, or help hospitals file medical records or scan test results for illness. The applications could be limitless and life changing.

On the other hand, one must ask ourselves if we really want our response to a potential international event to be left in the hands of a computer program. In the Tabroom example above, the system was able to place judges, and it was able to place judges according to the preference system that was established before the tournament started. But a computer can't fine tune the judging pool to account for the best judges to be placed in bubble rounds or handle student issues at the tournament. For things like that, you still need a human to listen and look at the raw data and make a determination.

Finally, you have the doomsday "Terminator" scenarios where the artificial intelligence runs amok and turns against humans. This isn't as farfetched as it might sound. Programming is only as good as the person doing the programming and since we're only humans with our flaws and errors, and since the intelligence would still be a program, it is reasonable to think that it would be vulnerable to any errors that modern software faces. Questions remain such as "How will it determine a foreign vs domestic attack, and will the response be the same?" or "What if it is a false alarm?" Might there be a miscalculation in response due to computer error?

This contention is one of the more "out there" arguments on this topic. It however isn't unwinnable. It just required the preround work to make it happen. On the pro, you will need to argue that artificial intelligence is the next wave of responses that will need to be developed. You will also need a solid impact. Make your link chain as believable with solid research grounded in scientific and qualified writings and make sure the link chain is as short as possible. This will give your opponents as few opportunities for an attack as well as keeping the judge from being able to say they just can't buy it. On the con, you need to argue that the concept of artificial intelligence won't be used for a response or to the extent of the pro team's case. It will be used to identify attacks and a human will still be doing the work. This takes out all future impacts they might run. You can also go full on Terminator and run machines will rise up but I'll leave you to find that research.

Sample Research

Cyber operations necessitate the development of AI to integrate physical command and control to digital assets

Lawlor, Maryann. 5-31-2109, "AI May Pose More Questions Than Answers," SIGNAL Magazine, https://www.afcea.org/content/ai-may-pose-more-questions-answers

Artificial intelligence and machine learning techniques could help information and network defenders recognize patterns of potential attackers so their next moves can be proactively blocked. In addition, cyber tools enhanced with these capabilities could provide a much more detailed picture of the cyber battlefield and increase the potential of success in a cyber campaign. This knowledge would complement the kinetic battlefield and could permit war planners to choose the appropriate mix of cyber and kinetic operations.

The invisible nature of cyber operations makes it a powerful weapon. Unlike its kinetic counterpart, victims usually aren't aware of an attack until they experience the effects. As a result, much of the most important discussions about U.S. cyber activities must take place behind closed doors in a classified environment. This is one of the reasons AFCEA International is hosting the association's fourth Classified Cyber Forum.

Jim Richberg, one of the forum's organizers, says the event aims to address several emerging implications of artificial intelligence and machine learning (AI/ML). Among the topics, event presenters will discuss the prognosis for near-, mid- and long-term development and adoption of AI/ML; adversarial machine learning; and the interaction between defensive and offensive cyber use of AI/ML.

Richberg, who has more than 30 years of experience in the U.S. government leading and driving innovation in cyber intelligence, policy and strategy, says, "The long term development of AI/ML and its impact on cybersecurity are worth examining since it's unlikely to play out in a simple or predicable manner."

John Gilligan, CEO, Center for Internet Security, agrees that AI/ML in adversaries' hands will pose challenges unlike those seen today. "Using AI/ML, attackers can refine their methods of attack more rapidly by 'learning' about the defenses of a target and quickly turning to other methods of attack that might be more successful," he says.

AI/ML also may affect kinetic warfare strategic planning, Gilligan adds. "There is the potential that AI/ML cyber tools could provide a much more detailed picture of the cyber 'battlefield' and increase the potential of success in a cyber campaign. This knowledge would complement that knowledge of the kinetic battlefield to permit war planners to choose the appropriate mix of cyber and kinetic operations,” he explains.

While cyber and kinetic capabilities may complement each other in the battlespace, Richberg points out several other issues still must be addressed regarding how artificial intelligence and machine learning fit into industry planning when it comes to the government and military environment. For example, he points out developers must still determine where cybersecurity ranks when compared to more readily monetized areas for AI/ML investment.

Richberg also asks, “Are we doing things in AI/ML that may make sense in the near term or from a narrow organizational perspective, but that are suboptimal from strategic/whole-of-nation perspective activities? Are we 'eating our seed corn' as a nation and picking 'winners' prematurely instead of hedging our bets? For instance, many early adapters are making their efforts proprietary and academic research is becoming commercialized. [Do] we lack an adequate academic or commercial training pipeline, etc.?”

AI will be integrated into a new age cyber operations strategy. AI can detect and destroy threats faster than their human counterparts

VanVuren, Kane S. 2018"Cyber Offensive Operations: Is There a Digital Delta Force?," Small Wars Journal, https://smallwarsjournal.com/jrnl/art/cyber-offensive-operations-there-digital-delta-force

The Department of Defense has the legal authority of the President to launch both cyber and kinetic attacks against an aggressor if it is deemed the best course of action (McLaughlin 2011, 61). Also, each US military service has cyber response teams capable of launching cyber counterattacks supported by ground, sea, or air attack if needed (McLaughlin 2011, 61). One of the most powerful entities that the United States has in cyber warfare is the National Security Agency (NSA), but sometimes it forgets it is a DoD support agency and it does not like to collaborate and share with others (McGhee 2016, 59).

McGhee reports that the NSA has spent years penetrating and implanting cyber code in foreign networks, but once deployed those implants can no longer be used again and the host will build protections against further similar attacks (2016, 60). Taking into account the DNC hack, Huskaj and Moradian (2018, 304) introduce the strategy of cyber deterrence and that existing research does not consider the connection between the "human and technological dimensions" highlighting that the relationship between an adversary and a deterrent (i.e., legal or physical/military strength projection) has not been fully developed.

Artificial Intelligence (AI) is another consideration that should be further developed in both cyber and military domains. Machine Learning (ML) applications are already employed through civil and military technologies like speech/image/face recognition, and battlefield solutions to aid Commanders to make real-time decisions are being developed (Hallaq et al. 2017, 153). ML operates by applying algorithms to data sets to discover patterns of interest, and in the case of cyber warfare, Hallaq et al. (2017, 155) cite that cyber relevant strategies "are likely to become increasingly reliant on artificial intelligence" in areas of computational speed and situational awareness as an equal but opposite strategy against automated cyber-attacks from adversaries.

Further Research

Ahmad, Nabeel. 8-1-2019, "Artificial Intelligence: A Tool or a Threat to Cybersecurity?," ReadWrite, https://readwrite.com/2019/08/21/artificial-intelligence-a-tool-or-a-threat-to-cybersecurity/

Lawlor, Maryann. 5-31-2109, "AI May Pose More Questions Than Answers," SIGNAL Magazine, https://www.afcea.org/content/ai-may-pose-more-questions-answers

Hoover Institution, 8-26-2019, "Cyber And Artificial Intelligence Boot Camp," https://www.hoover.org/events/cyber-and-artificial-intelligence-boot-camp-2019

ResearchGate, "AI and Machine Learning for Offensive Cyber Operations," https://www.researchgate.net/publication/334160690_AI_and_Machine_Learning_for_Offensive_Cyber_Operations

Vergun, David. 9-5-2019, "Cyber Ops to Gain Speed, Accuracy From AI," U.S. DEPARTMENT OF DEFENSE, https://www.defense.gov/explore/story/Article/1953183/cyber-ops-to-gain-speed-accuracy-from-ai/

ISIS/Cyber Terrorism

I have chosen to combine these two points as they share multiple arguments in common and in fact cross over 90% of the time.

In an age of modernity, even our enemies are evolving to fit the new technology centered lifestyles that has taken over the world. This includes both the nation state actor as well as the stateless terrorist. After the invasion of Afghanistan, Iraq, and the US offensive in the Middle East to combat the rise of ISIS, radical anti-American terrorist groups realized that fighting the United States in a head to dead matchup was a no-win game. Unlike the war in Vietnam and the pervious Soviet wars in Afghanistan, the United States had a massive setup of superior vehicles and a 10:1 military plan that would overwhelm any attacking force. Fueled by a modern air force and space based surveillance, the terrorist networks began to look for more modern ways of both attacking the United States as well as a means to recover some of the financial revenue that they needed to overpower the United States. Their search was short lived as they quickly turned to the internet for both.

With assistance from state run anti-American governments like Iran, splinter groups in Turkey, North Korea, and Syria, the Islamic State in Syria and its splinter cells located around the world began to use computers to infiltrate the United States. In many war-torn areas, it was not hard to recruit computer trained students who would be willing to put their skills to use for the networks operating against the United States. So far, these terrorist groups have launched attacks against Department of Defense contractors hoping to gain access to critical data and employee information. They also have waged war against the allies of the United States. Programmers for ISIS have used their skills honed in the cyberwars against American allies to build better bomb timers and program attack drones. Furthermore, the terrorist networks have used their hacking skills to steal millions of dollars from unsuspecting groups and websites to fund their terrorist networks and operations.

The argument here is that unlike war against a state actor, the concept of a first strike is perfectly legitimate and accepted, thus an offensive cyber operation is at it's most legitimate. If the United States can find out where a command and control center is, our cyber operations can knock it out before it can attack first. This argument poses few risks for the pro team as most terrorist networks don't possess the same military capacity that nations like Russia or China does so the risk of a physical strike in return is low.

When debating this argument, the pro team will need to win two arguments. The first is the inherency that the terrorist networks have the capacity to actually carry out an attack. This is much like the North Korea threat argument insofar that the media has convinced us that we are far safer than we really are. You will need good evidence that says that the next wave of terrorism will be digital, and it is coming now. The second argument you will need to win is that there is an impact. This against comes from the media's portrayal that we are safe. The argument that will win you the round here is that terrorist will go after soft targets like civilians and that is where the harms come in. It's just far fetched to assume or argue that a terrorist network will gain access to our nuclear weapons, but shutting down a nuclear power plant could happen. On the con, you will need to win that the threat is over blown and that our physical military can destroy any cell before they get their cyber operations up and running first. The other argument is that most terrorist cells operate in foreign nations and that if we launch a strike against a sponsored terrorist cell, we might prompt a response from the sponsor like Iran or North Korea. In the end, the debate will come down to who can tell the most realistic story.

Sample Evidence

Offensive cyber operations necessary to stop ISIS from command and control of their worldwide terrorist network

Lin and Zegart, 2016, Bytes, Bombs, and Spies Brookings Institution Press. Preview can be found here https://www.google.com/books/edition/Bytes_Bombs_and_Spies/eMhyDwAAQBAJ?hl=en&gbpv=1&printsec=frontcover

The DoD has publicly acknowledged using cyber weapons in its fight against the Islamic State of Iraq and Syria (ISIS). For example, in February 2016 Secretary of Defense Carter said that U.S. Cyber Command is conducting offensive cyber operations to cause ISIS to “lose confidence in their networks, to overload their networks so that they can’t function, and do all of these things that will interrupt their ability to command and control forces.” Bytes, Bombs, and Spies (p. 2). Brookings Institution Press.

No proof of cyber terrorism exists

Morozov, 2009 “Cyber-Scare: The exaggerated fears over digital warfare”, July/August, http://bostonreview.net/BR34.4/morozov.php

The age of cyber-warfare has arrived. That, at any rate, is the message we are now hearing from a broad range of journalists, policy analysts, and government officials. Introducing a comprehensive White House report on cyber-security released at the end of May, President Obama called cyber-security “one of the most serious economic and national security challenges we face as a nation.” His words echo a flurry of gloomy think-tank reports. **The Defense Science Board, a federal advisory group, recently warned that “cyber-warfare is here to stay,” and that it will “encompass not only military attacks but also civilian commercial systems**.” And “Securing Cyberspace for the 44th President,” prepared by **the Center for Strategic and International Studies, suggests that cyber-security is as great a concern as “weapons of mass destruction** or global jihad.” Unfortunately, **these reports are**usually **richer in vivid metaphor**—with fears of “digital Pearl Harbors” and “cyber-Katrinas”—**than in factual foundation**. Consider a frequently quoted CIA claim about using the Internet to cause widespread power outages. It derives from a public presentation by a senior CIA cyber-security analyst in early 2008. Here is what he said: We have information, from multiple regions outside the United States, of cyber-intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber-attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet. **So "there is info**rmation" **that cyber-attacks " have been used." When? Why? By whom?** And have the attacks caused any power outages? **The CIA may have some classified information, but very little that is unclassified suggests that such cyber-intrusions have occurred**.Or consider an April 2009 Wall Street Journal article entitled "Electricity Grid in U.S. Penetrated By Spies." **The article quotes no attributable sources for its starkest claims about cyber-spying**, **names no utility companies as victims of intrusions, and mentions just one real cyber-attack**, which occurred in Australia in 2000 and was conducted by a disgruntled employee rather than an external hacker. **It is alarming that so many** people **have accepted** the White House's **assertions** about cyber-security as a key national security problem **without** demanding **further evidence**. Have we learned nothing from the WMD debacle? The administration's claims could lead to policies with serious, long-term, troubling consequences for network openness and personal privacy.

Further Reading

Doffman, Zak."New Cyber Warning: ISIS Or Al-Qaeda Could Attack Using ‘Dirty Bomb’," Forbes, https://www.forbes.com/sites/zakdoffman/2019/09/13/cyber-dirty-bomb-terrorist-threat-is-real-warns-us-cyber-general/

Temple-Raston, Dina. 9-26-2019, "How The U.S. Hacked ISIS," NPR.org, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

Tesauro, Lyda. "The Role Al Qaeda Plays in Cyberterrorism," No Publication, https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism

Wyman, Oliver. "Global Cyber Terrorism Incidents on the Rise," No Publication, https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html

Yunos, Z, and S Sulaman. “Understanding Cyber Terrorism from Motivational Perspectives.” Journal of Information Warfare, vol. 16, no. 4, 2017, pp. 1–13. JSTOR, www.jstor.org/stable/26504114.

Legality

--- Disclaimer---The thoughts and comments expressed below are those of the author and not that of the NSDA. Any questions can and should be directed to the author of this brief.

Poets and scholars alike have said for generations that technology increases the distance from the humanity of real-world problems and those on distant shores. It is my belief that for many people under the age of 40 (and this does include me), our ability to have a connection with the concept of what is "war" differs from that of our parents. My parents grew up not only watching the news nightly for stories about Vietnam, but they saw their friends leave their small hometown in Iowa to fight in the tropical forests thousands of miles away. To them, war was a real experience that has real world implications.

Things have changed. The advent of modern video games and the lack of an inclusive draft (don't get me wrong, I am not advocating for a draft, I'm merely stating that a volunteer army has a different impact on the populace when compared to a forced draft army.) has turned war into a video game. Kids can turn on their consoles and play the latest Battlefield or Call of Duty game and if they are killed, they can respawn. If they fail an objective, they can reset the map. In some levels, you are rewarded for collateral damage. Then these kids turn on the tv and they see images of drones flying in for a kill and ads for the army that show technicians sitting in an air-conditioned command center flyi8ng a drone with a headset and a joystick just like the game they turned off. To many, this "war as a game" mentality has divorced people from the reality of pulling the trigger. The little dots on the screen right before the hellfire missile hits the target are (or were) real living people.

What does this amount to besides a rant from a debate coach in Iowa? In our games, war has no rules. When there are rules, failure to follow those rules results in a game reset. The deaths and harm that were caused are wiped away for try number two. In real life, war has rules. You follow orders, and those orders are given by commanders who are schooled in the rules of engagement and war. Even at training, life isn't all physical training and drill. Lots of time is spent learning what the rules are and how to follow the rules as established by the pentagon, the US congress, and international law.

This changes online. When every action that is taken is covert, when every movement is in theory, untraceable, and when you can strike without warning and with no regard for borders, and where the enemy is faceless and the innocent people are not seen, it is easy to take actions like it is a video game. In fact, it doesn't hurt that cyber warfare takes place in front of a computer just like the video games that we play so frequently.

So, on one hand, you have the ease of use, the stealth aspect, and the ability to covertly defend your nation from enemies, both foreign and domestic. But on the other hand, you have to weigh the legality. Just because borders don't exist, does that mean we can act with impunity? Just because we can't be seen, does that mean we get to deny due process?

First, in a real war, if we find that there is a threat building in an enemy nation, we have two choices. Either we violate that nations sovereignty and launch an attack into their airspace using our air force, or we present a notification to the leaders of that nation that we are preparing to take military action and we hope they sign off. However, let's say that the enemy is the state we would have to clear action with. Asking permission would be foolish. In this case, we could strike, but we are mandated to minimize civilian harms. This respects the border and established airspace of nations. This is even true of times when we would use a missile strike. We wouldn't need to inform our target of the attack but it is customary to inform our allies in the region that there is about to be action so they don't panic when they see the US launching tomahawk missiles from a destroyer in the Gulf of Oman. In a situation an offensive cyber operation, the covert nature and hidden aspects of the internet means that no permission has to be followed and borders don't exist.

Due process is another issue that comes up. In the United States or internationally, if we accuse a person of a crime, they are allowed a chance to present evidence to defend themselves against the accusations. They are allotted a trial. Gone are the days where we declare someone a fugitive and shoot to kill. Even for wanted terrorist, modern legal scholars state that the news media has changed how we view due process. The simple act of discussion a person on tv and their ability to respond from anywhere can act as a pseudo form of due process. But with cyber operations, once we mark a target, that target is oblivious to the attack until it has happened. It is similar to a person being marked by a physical hitman. They don't know they are a target until they have been eliminated.

Proportional response is another issue. In the traditional concept of defense to action, we obey the laws of Newton. By that I mean that any actions solidities an equal and opposite reaction. In this regard, we wouldn't launch a nuke to respond to a car bomb blowing up a guard post at a military base. However, in cyber operations, the concept of "proportional" doesn't really mean much as it is hard to gauge the actions that are taken and how much damage might occur. A hack might shut down one computer or it might disable the entire country's power grid. Results generally can't be known until action is taken.

Finally, if the target is a US citizen or if they are in the US, we face a few issues. First is that accused citizens are allotted the same legal protections of the US constitution which includes due process, a trial by a jury of their peers, the ability to present evidence on their behalf, the right to contact an attorney, and the ability to confront their accuser among others. These simple procedures are laid out in our bill of rights and constitution. The courts have ruled that just because action is taken online using digital means does not nullify those documents, and just because the covert nature of cyber operations exists, that shouldn't nullify those rights either. If the subjects is on US soil, we face the Posse Comitatus Act of 1878. What this law says (and it is still law despite being over 100 years old) is that the military can't be used as a domestic law enforcement agency to enforce domestic laws. What this means is that if the military is targeting an individual in the US because they have been accused of drug smuggling (a violation of a domestic law) civilian law enforcement like local police or the FBI would have to use their cyber operations capabilities and not the military. Just as with real physical force, just because someone is robbing a bank does not give the government the right to bring in a full M1 tank or call in an air strike.

When debating this topic, the pro will need to argue that the internet has changed the frontier of what it means to have a national border. Explain to the judge that when they place an order with Amazon, their order travels through four or five different countries before being filled at an Amazon warehouse. In fact, find a good website that everyone used and find out where their central shipping HQ is located or where their tech servers are located. I bet that most are located overseas. The internet has globalized and united the world in a borderless society where we cross servers like debaters go from round to round. This point should show the judge the futility of trying to enforce borders online. The other way is to argue that threats are real and are growing and that if we saw a division of tanks massing at the Canadian border, we would strike regardless of Canada's feelings. On the con, you will want to go for law and order. The first part of this essay explains the concept of civility in war and conflict and how that is lost when we ignore things and make them into games. The analogy that this has become one big game is a good one. We have turned people into non playable characters and rules are ignored in leu of achieving an objective. Especially in a day and age where the United States is trying to stand for values and democracy, this is the moral equivalent of shaking hands while crossing fingers.

Sample Evidence

Offensive cyber operations would violate multiple legal norms

Djabatey, Edwin. 7-11-2019, "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis," Just Security, https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/

Offensive cyber operations in response to economic cyber intrusions may violate international legal obligations owed by the United States to the State at which the operations are targeted – including potential violations of their sovereignty, the principle of non-intervention, or even the prohibition on the threat or use of force (as I will examine in Part II of this series). This would have to be evaluated on a case-by-case basis, depending on the particular facts of the operation at issue. But to the extent an offensive cyber operation does violate international law, the wrongfulness of that operation would be precluded if it were undertaken as a valid countermeasure. **A State is entitled to take countermeasures – which are otherwise unlawful actions or omissions – in response to an internationally wrongful act by another State only if certain conditions are met.** As Prof. Mike Schmitt recently explained:

The requirements for countermeasures have been set forth by the International Law Commission in its Articles on State Responsibility, which are generally considered to reflect, in great part, customary international law. **The key requirement is that the "injured" State's countermeasure be intended to convince the "responsible" State to desist in its unlawful activities, in this case the emplacement and continued presence of the malware**. Countermeasures are also permissible to secure assurances, guarantees or reparations. The option of taking countermeasures to secure guarantees is particularly important, for a guarantee may take the form of neutralization or removal of the malware in question by the responsible State. **Additionally, countermeasures may not be anticipatory in character** (unlike self-defense), **must be proportionate to the unlawful act to which they respond, and must not constitute a use of force.**

Thus, **the United States is only entitled to respond to economic cyber intrusions with countermeasures if it can establish that the intrusions undertaken against it breach international law. In the context of China's alleged economic cyber intrusions against the United States, the United States would need to establish that those intrusions breach a particular rule of international law, and the breach is attributable to China.** (I will assume for these purposes that attribution for the relevant cyber activity can be made to China, the main adversary State at issue.)

International law doesn't govern cyber warfare

Lindsey, Nicole. 10-14-2019, "Cyber War Between Iran and United States Could Have Far-Reaching Implications," CPO Magazine, https://www.cpomagazine.com/cyber-security/cyber-war-between-iran-and-united-states-could-have-far-reaching-implications/

The U.S. has thus far been careful to avoid a full-out "shooting war" with Iran, but it's clear that it won't sit around and wait for Iran to destroy more oil targets in U.S. ally states, or to disrupt shipping lanes in the Strait of Hormuz. Oil from the Middle East is the lifeblood of the world's economy, and the U.S. has been careful to avoid chaos in the region. Which brings us to where we are today: on the threshold of a major new cyber war between two heavily armed powers with plenty of offensive cyber strike capabilities on both sides. The only question, really, is which targets the U.S. plans to hit next. The Iranian oil ministry, for example, has said that cyber retaliation would likely come against Iranian oil targets, and warned that the nation's oil industry should be on "high alert" for U.S. cyber attacks.

Where things head next is anyone's guess, and that's why the current situation is so alarming to military and political analysts. Simply stated, **there are no international rules or norms for digital warfare, and no cyber version of the Geneva Convention to protect innocent civilians from a potentially destructive cyber attack on critical infrastructure.** Adding to the complexity of the current situation is that it is close to impossible to identify who is behind a cyber attack, or to figure out where a cyber attack originated.

Traditional rules of war as stated by the UN don't apply to cyber conflicts

Goldsmith, Jack. 4-1-2013, "How Cyber Changes the Laws of War," OUP Academic, https://academic.oup.com/ejil/article/24/1/129/438526#6543860

One challenge is to figure out when a cyber-attack implicates jus ad bellum. The hard question is how to translate the UN Charter concepts of 'use of force' and 'armed attack' into the cyber realm. The main answer that has emerged, drawing on Michael Schmitt's work, has been to **focus on the scale of the kinetic effects of the cyber operation.5 When the effects of a cyber operation are akin to the effects that would implicate the UN Charter terms, then cyber**

operations implicate the UN Charter. So, for example, a cyber attack that renders the electricity grid or air-traffic control system inoperable, and that as a result causes many deaths, would count as a use of force. But a cyber operation that merely involves espionage or that disrupts DOD

computers conducting military research, likely would not be considered a use of force. These cases are easy enough. But cyber operations introduce more challenging questions.6 The challenges arise mainly because **the Charter focuses its prohibitions on military means of inflicting damage on another state, but does not prohibit economic or political means of inflicting damage on another state.** As a general matter, **military means by one state that leads to deaths or physical destruction in another implicate the Charter**, but **political or economic sanctions that lead to deaths or physical destruction in another state do not. Cyber operations can cause havoc in a nation, including death and destruction, which might appear more like economic sanctions than a military use of force.** Consider, for example, a cyber attack that corrupts data on a stock exchange and which in turn causes widespread economic harm but no direct physical damage. Is this more like a physical use of force or like economic sanctions? What about widespread economic harm caused by massive theft of digitalized intellectual property? Theft and espionage are not generally viewed as implicating the Charter, but the cyber context changes the scale and consequences of theft and espionage to a degree that can result in harm to the country at least as severe as a physical attack. **Another difficulty with cyber operations is that, unlike many kinetic attacks, they can take place slowly and can be reversible.** There is no settled answer to the question whether or when a slow disruptive cyber attack on critical infrastructure or an analogous system that gradually renders it sub-optimally operable becomes a use of force. **Similarly, there is no settled answer to the question whether a temporary but reversible shut down of a computer system, lasting perhaps two days or two weeks, associated with a fighter-jet squadron or a reconnaissance-satellite system is a use of force. Nor is it clear whether 'mere' destruction of critical economic or military data, without any physical consequences, is a use of force.**

Future Reading

Djabatey, Edwin. 7-16-2019, "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part II," Just Security, https://www.justsecurity.org/64935/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-ii/

Ellers, MaríA. 10-23-2019, "How America's Cyber Strategy Could Create an International Crisis," National Interest, https://nationalinterest.org/blog/skeptics/how-americas-cyber-strategy-could-create-international-crisis-90526

Lotrionte, Catherine. “Cyber Operations: Conflict Under International Law.” Georgetown Journal of International Affairs, 2012, pp. 15–24. JSTOR, www.jstor.org/stable/43134334.

"Weighing the Case For a Convention to Limit Cyberwarfare," No Publication, https://www.armscontrol.org/act/2009-11/weighing-case-convention-limit-cyberwarfare

Wheeler, Tarah. 9-12-2018, "In Cyberwar, There are No Rules," Foreign Policy, https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/

Alliances

The final major set of arguments that I chose to look at involve alliances. Alliances are important in our globalized world. People want to feel like you have friends when you stand against the threats and darkness that fills the world. In the same way, when we are fighting a war on a new battlefield, we need allies to help navigate the many complications and aspects of this new frontier.

Alliances are broken down into two very general but large areas. The first is NATO as that has the largest literature base to focus on. The link chain on this contention gets a bit longer than on others, but the arguments are more solid than most others. To judges, you will need to keep the arguments short and to the point as we spent a lot of time on the last topic listening to arguments about NATO and the EU and we are suffering from a bit of a burnout when it comes to Europe. Also, just because we spent the last two months becoming experts in Europe, don't assume that your contention makes sense and thus you can gloss over large holes. You still have to do the world to get us to vote on this.

Alliances in general is the second large body of literature. I could have gone by a country specific list but the NSDA frowns on posting files larger than several hundred pages and I'm commissioned to write a brief not an almanac. But trust me when I say that there is a lot of research on multiple countries that says our allies (insert your favorite nation because guaranteed you can and will find the research on them) will be put off by our development and deployment of offensive cyber operations and that will strain and break our alliances. The hard part is going to be finding an impact to those specific nations. The historical examples I listed in the brief are good for background but you will need to find the country specific arguments and impacts that create the viable link chain and contentions. This set of arguments is more like a Mr. Potatohead style argument where the base is certainly there, but it is up to you to make it look like a thing.

NATO

The North Atlantic Treaty Organization, or NATO, is a holdover from an era of eye to eye tensions with our global rivals, the USSR and the Soviet Blok nations. Today, more than 70 years since the formation of this coalition of nations, there are skeptics both in the United States as well as internationally that wonder if this body is worth keeping around. After all, the West won. The Soviet Union collapsed, right?

Having stood strong for over 70 years, the NATO alliance has united the countries of Western Europe and the United States against threats to democracy and our national soverngity. One of the key phrases from the NATO Charter proclaims that “an attack on one-member ought to be treated as an attack on all.” It is in this sentence that we see the purpose of the alliance; We are stronger as a group fighting an enemy than we are individually. We win by showing strength and with overwhelming force so that no one nation carries the burden, cost, or casualties alone. After the attack of September 11th, 2001, the NATO alliance dispatched rescue crews to New York and Washington. Military leaders coordinated an international effort to track down the identity of the attackers, and when the time came for a retaliation, the alliance helped the United States in the invasion of Afghanistan.

Today, we face a new threat. Although the Soviet Union fell in 1991 and we no longer face the threat of the expansion of communism into Western Europe, we still face the treat of a new Russian sphere of influence that has filled the vacuum of the USSR. This influence has spread into Eastern Ukraine during the Ukraine/Russian invasion and occupation. This is felt by Russian election meddling in Germany, France, and the United States, and it has been felt by the renewed push for naval superiority in the North and Baltic Seas. The Russians want influence and power and they are not afraid of showing their desires. As stated in the “Russia” section of this brief, the Russians have employed a huge army of cyber operatives that are tasked with disrupting life in the West. NATO is aware of this. Their response has been to pool resources into a collective of offensive cyber operations designed to both neutralize and deter the Russian aggressors before the threat grows into a real-world conflict. Thus far, almost every developed NATO nation has put resources into this collective except the United States. This is due to a lack of willingness on the part of our president to commit money and resources to the alliance as well as the lack of resources we can actually commit. Since 2015 and the development of the US Cyber Command, NATO has been pushing for the United States to dedicate more resources to the effort. Their argument is that this is necessary to counterbalance Russia in Europe and to stop their slow takeover of the internet via subversive and covert cyber operations.

Based on the wording of this resolution, the pro team could argue that the counterbalance and alliance building caused as a result of our offensive cyber operations will outweigh almost any other impact. As was argued on the previous topic, the alliance can solve a laundry list of impacts through influence and sheer force. In round, this would amount to arguing that the US is a key partner in the alliance and that we are necessary to build on the current framework of cyber operations. The key to this debate will be the internal link debate. You will have to find good research that argues that we can do enough to stop Russia. This is made harder to do since most cyber operations are covert and thus we don't know the true extend that any nation really has. You will also need to win a clear impact to a Russian spread. I want to remind debates that in public forum, judges like realistic impacts. Nuke war leads to world ending extinction is more of a policy thing. Keep things on the level and keep it realistic to the expectations of things that could really happen without a huge link chain. On the con, you need to argue that the alliance isn't key to stopping Russia or that the US isn't key, and the alliance is working now. Russia has been involved in the cyber operations game for years and the US hasn't gotten involved yet. The fact that we know they are up to infiltration means that their true intentions aren't hidden and that it just comes down to actually getting governments to act rather than a united front. You could also try to argue a uniqueness takeout that our president will never commit to anything like this so the impacts are inevitable. Whatever the route, also keep things reasonable and realistic.

Sample Evidence

NATO is serious about offensive cyber operations now but they need the US. The US is key

Tucker, Patrick. 5-24-2019, "NATO Getting More Aggressive on Offensive Cyber," Defense One, 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 missions,” 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.**

That’s the strength of the article, according to NATO Deputy General Secretary Rose Gottemoeller. However, while an Article 5 response can be unpredictable, it must be coordinated, which can be tricky with many different partners in possession of many different capabilities.

At an event in May, Gottemoeller said NATO was in the processes of establishing a new innovation board to “bring together all of the parts of and pieces of NATO that have to wrestle with these new technologies to really try to get a flow of information. Many of you having served in any international institution or government, you know how things can get stove-piped. So we are resolved to break down those stove-pipes, particularly where innovation is concerned,” she said.

NATO is building a cyber command that is scheduled to be fully operational in 2023 and will coordinate and conduct all offensive cyber operations. Until then, whatever NATO does offensively, it will rely heavily on the United States and the discretion of U.S. commanders, according to Sophie Arts, program coordinator for security and defense at the German Marshall Fund, who explains in this December report.

"Yesterday's remarks indicate that NATO's leadership is thinking more seriously about buttressing the alliance's deterrence posture in cyberspace and address threats that fall under the threshold of an Article 5 violation," she told Defense One.

NATO's offensive cyber operations are necessary to check against Russia in Eastern Europe

Lewis, James A. "THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE", Tallinn Paper No. 8, https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf

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.** These topics are essential for planning purposes, but leave NATO in a reactive mode when it comes to cyber warfare.4 The **central question for NATO's cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend. Put another way, can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal? Offensive capabilities,** unlike NATO's current defensive posture, **involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction**. The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term. **The US has always been overly secretive about its offensive cyber capabilities**, even after a flood of media leaks have made the most sensitive doctrine publicly available. **This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or**

coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations. Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that **cyber attack is a “weapon” with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO’s defensive actions are not at all obvious, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO’s defensive activities**, and NATO’s credibility in defence requires some public discussion on the use of offensive cyber operations. There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the **ability to deter cyber attack work best when embedded in a larger military force structure**. Adding offensive cyber capabilities to NATO’s **force structure and response doctrine will increase its deterrent capabilities** – by how much is unclear, but what is clear is that a failure to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.5

Further Reading

Emmott, Robin. 10-16-2018, "NATO cyber command to be fully operational in 2023," U.S., https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9

"NATO's Cyber Operations Center – Will Russia Feel Threatened?," CyberDB, https://www.cyberdb.co/natos-cyber-operations-center-will-russia-feel-threatened/

"Offense as the New Defense: New Life for NATO's Cyber Policy," German Marshall Fund of the United States, http://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy

Smeets, Max. 11-3-2019, "NATO Allies Need to Come to Terms With Offensive Cyber Operations," Lawfare, https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations

Vavra, Shannon. 8-30-2019, "NATO cyber-operations center will be leaning on its members for offensive hacks," CyberScoop, https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/

Allies

The basis for any good relationship is built on trust and honesty. In the arena of international relations, this is especially true. If we go back to the start of this brief when I talked about how nations function under a veil of realism, or the idea that each nation will try to better the standing of their own people and actions that are taken are done with self-promotion in mind, then one can assume that what is the purpose of allies? After all, the saying is “to the victor goes the spoils,” not “to the victor we share what we plundered.” To answer this, we need to look to the concept that there are tasks in this world that are larger than any one nation. Fighting disease, famine, natural disasters, and fighting massive wars all become draining on nations, no matter how large. In this regard, nations find it better to create unions of like-minded nations that can assist each other with tasks when the time calls for it. This has been the dominant principal for international relations for centuries. When fighting the ancient Romans, the Gauls founds allies to stand with (and die with as the Roman Empire was just that much better prepared), the US found allies in France during the American Revolution, the French would find an ally in the US during World War I, and as a world, we united to fight terrorism after September 11th

The concept of alliances has weathered the tests of time, however it has all been done under the old rules of warfare when nations marched large armies out into the open to fight and everyone was essentially playing “with all cards on the table.” What happens when there are covert actions that nations can’t see and the warfighting moves to the shadows? In World War I, the system of secret alliances between pretty much every nation in Europe causes a convoluted domino chain to form. When the Archduke was assassinated and retribution was demanded, alliances kicked in, some of which were in direct contradiction with other alliances. This pulled nations into the conflict whether they were ready for war or not, and whether the side they ended up fighting for was the side they truly supported or not. After the signing of the Paris Peace Treaty, the nations of Europe proposed the League of nations to keep alliances open and to solve disputes before it came to war. This was promptly shot down and nations went back to holding back room secret meetings and signing secret alliances. Germany signed a treaty with Russia for non-aggression, France with Great Brittan, Japan with Germany. This would play out in much the same way in 1939 when Germany declared war against the nations Europe. Following World War II, the United Nations was formed to keep alliances open and to prevent another great power war. This union has survived for decades.

The concept of offensive cyber operations could change this. With nations rushing to develop internet task forces with the goal of protecting the digital borders, and with actions that nations can take online being shrouded in secrecy, nations are naturally wary of each other. International Relations scholars fear we are devolving back to the world pre-World War I. Alliances are made behind back doors to share secret cyber operations data while at the same time you work to undermine your allies to keep yourself and your nation in a position of power. This state of paranoia and self-promotion puts all nations on edge. At the same time, we face global threats like the world has never seen. Climate change, international terrorism, economic collapse all threatens our nations. If we are skeptical of each other and we do not trust each other to act in the best interests of the world, how can we unite to face these threats?

When debating this topic, the pro needs to clearly explain the historical significance of secrecy and how it damaged alliances in the past. This is a concrete example of secrecy killing the alliance system and leading to death. Judges will understand historical examples. Judges love historical examples. Then the pro team will need to draw the parallel to modern times and how this is the new prelude to World War I. This is the summer of 1914 again. The con team will need to argue the uniqueness of this. The presidency of Donald Trump has changed how alliances work. We have been shedding alliances not only since 2016 but longer under a growing cloud of isolationism that has been growing since the Clinton administration. As long as we can unite when the time calls for it, we don’t need long standing alliances.

Sample Evidence

Offensive operations kills trust between our allies and makes everyone wary of everyone else

Slayton, Rebecca, 4-22-2015, "Why Cyber Operations Do Not Always Favor the Offense," Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense

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. The skills and organizational capabilities for offense and defense are very similar. Defense requires understanding how to compromise computer systems; one of the best ways to protect computer systems is to engage in penetration testing (i.e., controlled offensive operations on one’s own systems). The similarity between offensive and defensive skills makes it unnecessary to conduct offensive operations against adversaries to maintain offensive capability. Thus, rather than stockpiling technologies in the hope of gaining offensive advantage, states should develop the skills and organizational capabilities required to innovate and maintain information and communications technologies.

Cyber offense undermines US relationships with its allies

Smeets, Max. 11-4-2019, "Cyber Command’s Strategy Risks Friction With Allies," Lawfare, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies

Much has been written about the fundamental changes in U.S. cyber strategy. **U.S. Cyber Command’s vision of “persistent engagement” and the Department of Defense’s new strategy of “defend forward” have, in particular, led to numerous critical remarks about the**

risks of escalation between the U.S. and its main adversaries in cyberspace. These debates are worth continuing, including about what the change in strategy means for establishing norms in cyberspace. But commentators have so far ignored a key dimension: The strategy's main implications may not reside in how it changes the dynamics between the U.S. and its adversaries but, instead, in how it affects broader alliance relationships, especially beyond the Five Eyes (Australia, Canada, the U.K., the U.S. and New Zealand). U.S. Cyber Command's mission to cause friction in adversaries' freedom of maneuver in cyberspace may end up causing significant friction in allies' trust and confidence—and adversaries may be able to exploit that.

Further Reading

Brewster Murray. · Cbc News · Posted, 2-6-2019, "Cyber-warfare could be entering a new and alarming phase, ex-CIA analyst tells MPs," CBC, https://www.cbc.ca/news/politics/cyber-warfare-sanctions-denial-service-cia-1.5008956

Ikeda, Scott. 5-6-2019, "Aggressive Changes to Deterrence, International Response and the Use of Offensive Cyber Capabilities on the Horizon," CPO Magazine, https://www.cpomagazine.com/cyber-security/aggressive-changes-to-deterrence-international-response-and-the-use-of-offensive-cyber-capabilities-on-the-horizon/

"Persistent Cyber Training Environment," No Publication, https://www.raytheon.com/capabilities/products/persistent-cyber-training-environment?gclid=Cj0KCQjw9fntBRCGARIsAGjFq5Fm6RHELMbVZhThsMHpyegeFrVNujal1Lgxnhlyf_jLCQt0POvqEvoaArrpEALw_wcB

Seco, Francisco. 10-10-2018, "Sharing is Caring: The United States' New Cyber Commitment for NATO," Council on Foreign Relations, https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato

Vergun, David. 9-6-2019, "Cyber Strategy Embodies Lethality, Reform, Partnerships," U.S. DEPARTMENT OF DEFENSE, https://www.defense.gov/explore/story/Article/1954302/cyber-strategy-embodies-lethality-reform-partnerships/

Conclusion

As we approach the January of 2020 and the first set of primaries that will determine the candidates that will represent the major political parties in the general election of 2020, the concept of electronic sabotage and espionage are still fresh in our minds. The Muller Report was clear that Russia used subversive means to influence the populace in the last election and reports from top security experts say that they are gearing up to do it again. At the same time, our nation faces great threats from our enemies online who seek to gain even a small advantage over in areas like diplomacy, economics, and even conflict management. To this end, the United States has been ramping up our offensive cyber operations to meet these new threats. This topic asks us not “if” we are, but “should we” and to what extent the benefit run.

When debating this topic, remember that last part. Don’t get drawn into a debate over whether it will happen or if it won’t. It is happening. We are increasing our cyber operations now. There is no doubt to that fact. The true debate is whether there are benefits and whether we should base it on the costs. You are weighing impacts in this debate.

As a judge, I ask you to remember to go back to the basics. Weight your impacts with probability, timeframe, and magnitude. Use the new summary time limits to do the work for the judge by contextualizing the nature of the impacts and stating why a five-year timeframe with smaller overall impacts is greater than a world ending impact with a 0.0001% chance of happening. Also, do the evidence comparison. This is a debate topic where you will have arguments on both sides about the same contentions. It is possible that both teams will run China or Russia. In that case, it is necessary to compare evidence to determine whose link is better. When debating the link turn arguments that will likely happen in other debates, evaluate the warrants of the evidence and explain why yours solves or preempts their evidence. Simple things like evidence comparison can save you the round. To this end, if you can point out specific lines from your evidence and your opponents’ evidence, you make your argument all that more powerful.

Above all, you are dealing with a resolution that takes place in the shadows. Cyberwar and operations are covert. There is little we know outside of experts testifying to what they can, hypothetical assumptions about how the world works, what is publicly known from government press releases, and our own common sense. Double check to make sure that you have logic and as much truth on your side as you can and stand your ground. Believe in the points you and your partner are running, research them well, known them in and out, and above all, have fun.

Pro Arguments At-A-Glance

ARGUMENT	TALKING POINTS	CON RESPONCES
CHINA	China is working to subvert interests US interests in East Asia. China has the largest cyber army in the world, and they are targeting the US now.	China doesn't have the ability to harm the US now. We are deterring china now with economic policies. Cyber operations lead to a physical conflict due to miscalc.
RUSSIA	Russia is subverting our elections now. Russia is working against the US now. Russia expanding into Eastern Europe. Need to counterbalance.	No threat from Russia. We know their tricks. We have safeguards in place no. No need for offense. Confrontation leads to war. Need to use diplomacy.
IRAN	Iran is a threat to oil shipping via cyber operations. Iran is funding cyber terrorism.	Other countries like Israel are solving Iran now. Risk of miscalc is high. Iran will strike back at regional allies and at shipping lanes.
NORTH KOREA	North Korea is launching daily attacks on the US via cyber weapons now. Biggest threat to the US in Asia.	No threat. North Korea can barely feed their people, they can't fund an army of hackers. We can detect their attacks. No risk of offense. Pressure works better than a cyber-attack.
CIVILIANS	Real war kills more than cyber war. Better for civilians.	Military won't restrict attacks to just military targets. Will attack civilian centers and will cause deaths.
ARTIFICIAL INTELLEGENCE	Development of Artificial Intelligence for cyber war spills over to civilian sector. Improves quality of life. Helps develop new tech for the world.	Military won't share their tech. Won't spill over. AI leads to harmful impacts. Invasion of privacy and miscalc leads to accidental deaths and loss of freedom.
TERRORISM/ISIS	Terrorism is moving to the internet. Need offensive cyber operations to counter. Terrorist focusing on cyber-attacks to cripple the West.	We can strike physical locations to shut down before cyber war becomes an issue. They don't have the tech to launch a coordinated cyber-attack.
LEGALITY	Violates international law. Violates tenants of the US constitution. Violates the basic ideals of international treaties.	Rules of war are still followed. If there is an issue, it's with the rules not cyberwar. The rules of cyber war are not set. It's a grey area.
NATO	NATO developing union of cyber war fighting now. Needed to counter Russia in Europe. Needs the US to assist.	Russia not a threat in East Europe. NATO working well without the US. NATO can't counter even with the US. US assisting now. Diplomacy works better.
ALLIES	Alliances are strengthened by US offensive cyber operations. Allies want the tech sharing that will come from our offensive cyber operations.	Offensive cyber operations cause fractures in the alliances. They have the link going the wrong direction. We won't share tech. We don't like to share our government secrets.

Con Arguments At-A-Glance

ARGUMENT	TALKING POINTS	CON RESPONCES
CHINA	No threat from China. All constructed around a false narrative. China is an ally.	Threats are real. They have stated their intentions clearly. They have the largest cyber army in the world. Allies can still work against you for personal gain.
RUSSIA	Russia will miscalc offensive cyber operations and start a conflict. Russia is not a threat. Treats are overblown	Impact should have happened after our very real attack on their power grid last year. They interfered in our elections; they are launching attacks now. Threats are rea.
IRAN	Iran won't risk an attack. They want a treaty. Iran is being counterbalanced by others in the region.	Iran is using cyberwar as leverage and intimidation of others. We need to show them we are willing to play ball. The counterbalance is the reason they will use cyber weapons. Their only good offense.
NORTH KOREA	North Korea is too broke to launch an attack. They have nukes to threaten the world.	Don't believe the media. North Korea is a threat. They aren't as helpless as we think. Cyberwar and nuclear war go hand in hand. Will need cyber war before nuke war to soften the target.
CIVILIANS	Civilians will be targeted and killed in a cyber-attack. Causes a humanitarian disaster.	Military can target the military only. No civilians will be targeted. The nations we are targeting are likely being liberated from disasters caused by the government. Safer than real war. Kills less.
ARTIFICIAL INTELLEGENCE	Will be used against the American people to spy on us and invade our privacy. Risks miscalc and could cause accidents.	Non unique. We are being watched by computers now. Fail safes prevent accidents. AI not linked to major weapons systems so no risk of world war. The Terminator isn't real.
TERRORISM/ISIS	Terrorism can eb taken care of with physical force. Don't need the cyberwar systems. ISIS is not advanced enough for this. They are on the run.	Cyberwar is safer than real conflict. Doesn't risk troops or equipment. ISIS is the most coordinated terrorist group in the world. They have websites that well merchandize. They love the internet. Need to get one step ahead.
LEGALITY	Rules of war prevent misuse. Only the guilty will be targeted.	Violates international law. Violates tenants of the US constitution. Guilt is only based on our assumptions not a trial.
NATO	NATO isn't necessary to counterbalance. They fuel Russian aggression. US involvement causes the major conflict.	NATO is the only thing keeping Russia in check. They are aggressive because they aren't getting their way. US keeping Russia in check. Our relations are keeping them calm. US involvement in cyber operations might calm the situation.
ALLIES	Covert offensive cyber operations cause paranoia. Leads to fractured alliances. History proves secrets are bad.	We have been doing this for years in other areas, no impact. Will work together for the greater good when we need to. History also shows times where we united under "The enemy of my enemy is my friend" mentality. Like in Vietnam and in natural disasters.