New Case

We negate.

Our Sole Contention is Cyber Instability.

In 2010, the United States launched the world's most dangerous cyberweapon called Stuxnet against Iran's nuclear program. This attack opened up Pandora's box, creating a world filled with cyber warfare.

America's use of offensive cyber operations increased cyber warfare in two ways.

First, Sparking an Arms Race.

Stuxnet was the starting gun in a cyber arms race.

Alex Middleton of the Journal of International Affairs explains that, even though cyber-attacks were used before Stuxnet, Stuxnet was a "game changer" because it was highly targeted, caused physical destruction, and showed other countries that military networks could be taken offline by their enemies.

In fact, Jason Healey of Columbia University explains that Iran generally ignored its cyber capabilities until the Stuxnet attack. After the attack, Iran increased cyber spending by 1,200 percent.

The second reason is Teaching our Enemies.

According to Ronald Lendvay of the University of Northern Florida, since Stuxnet was the first cyber-weapon to destroy another country's infrastructure, it gave terrorists and countries a blueprint to conduct cyberattacks. Jordan Brunner of Arizona State University explains that Iran's rapid development of its cyber-capabilities only happened because it had an excellent teacher named Stuxnet.

There are two impacts.

The first impact is cyber-terror.

Terrorism existed before 9/11, but the US didn't make it a priority. We cannot make the same mistake for cyber-terrorism.

Brunner explains that Iran has given its cyber capabilities to terrorist groups looking to commit large-scale attacks on the US in Lebanon, Yemen, and Syria.

Unfortunately, Jeremy Straub of PRI finds that a major cyberattack could cause irreparable economic damage and kill more people over time than a nuclear weapon. For context, the ISS quantifies that this would kill tens of thousands of people.

Jeremy Platt of the Marsh Institute explains that even though a major attack hasn't happened yet, it is more likely in the future for three reasons: first, the landscape for attacks is increasing because more devices are connected, second, terrorists are gaining access to more advanced capabilities, third, terrorists are facing defeat on the battlefield so they are shifting to cyberweapons to achieve their goals.

The second impact is deadly resource dependency.

Iranian cyber attacks are locking the Middle East into resource dependence. Right now, the Middle East is set on a dangerous path of oil dependency. Newsweek explains that due to fast population growth, Middle Eastern countries have high domestic oil consumption, leaving less oil available to sell on the global market.

Paul Stevens of Chatham House furthers that if the Middle East continues on its path of oil dependency, we can expect widespread conflicts over oil resources. Countries will be forced to start regional wars to gain access to new oil resources and to distract from their economic failure. For example, Newsweek predicts that Saudi Arabia will invade Iraq, Qatar, and Yemen to save their economy and control new oil. *In other words, thousands of lives are at risk.*

The only hope is for the Middle East is to diversify away from oil. Joyce Hakmeh of Chatham House explains that Middle Eastern countries are making massive investments into digital industries and smart cities to diversify their economies.

Unfortunately, current efforts are failing due to Iranian cyber-attacks.

Nicole Perlroth of the New York Times explains that Iran's recent cyberattacks on Saudi Arabia complicated Saudi efforts to increase private investment and diversify the economy. More broadly, Alkesh Sharma of the National furthers that state-backed cyber attacks have disrupted thousands of companies in regional economies. Thus, Hakmeh summarizes that cyberattacks have destroyed consumer confidence and investment in digital based industries and are thus the main barrier for Middle Eastern nations to transition away from oil dependency. *Without Iranian cyber-attacks, Middle Eastern states would be more able to diversify, reducing the chance of conflict.*

Thus, we negate.

US Fault Evidence

General

China

Rovner ‘17 of Oxford: China hadn’t updated its cyber program in 10 years until the Stuxnet attacks happened. Since Stuxnet attacked an air-gapped network, it showed China how vulnerable it was, causing them to invest massively into OCOs.[1]
Jiang ‘19: As there are also many foreign industrial control systems used in China, it faces the high risk of a Stuxnet-like cyberattack. A deteriorating cybersecurity situation provides good reasons for those who call for developing China’s own cyber deterrence.[2]
Washington Times: China increased cyber spending by 30 percent to compete with the US.[3]

Iran

North Korea

Sanger ‘17: In 2009, North Korean hacking abilities were a joke. They would occasionally take down US government websites, but that was about it. After the Stuxnet attack, they began collaborating with Iran for cyber-attacks and used a virus very similar to Stuxnet against South Korea.[4]

Russia

[1] Rovner (Oxford) china lagging before Stuxnet
[2] Jiang (School of International Relations and Public Affairs) china decided to pursue oco in 2015 bc of US
[3] Gertz (Washinton Times) to keep up with US spending increased by 30%
[4] Cut card; Evidence-9

Frontlines

Sub-point A

F2 Countries were doing cyber-attacks before

Middleton: Stuxnet was unique because it showed that cyber could destroy physical infrastructure specifically[5]
Healey: Iran ignored its cyber program before Stuxnet attack

F2 Cyber attacks are cheap

Stimpson: EFFECTIVE cyberweapons are too expensive for terrorists and lower-income countries to afford[6] CFR: Using the techniques from other countries and building off of their malware makes it more affordable[7]
Guardian: Nobody had the money to invest in cyberattacks like Stuxnet. Ivezic explains that Stuxnet gave them access to the millions of dollars of American investment.[8]

F2 Iran got cyber capabilities to do domestic surveillance

Our argument is about destructive attacks.

F2 Iran wanted cyber capabilities before Stuxnet

Columbia University: Iran ignored its cyber capabilities until it was attacked by the US.

F2 Military superiority prevents arms race

Clearly this isn't true. UCLA: After Stuxnet, attacks on critical infrastructure systems increased by 636%. Superiority doesn't solve as the NI explains that cyber superiority isn't a thing. Cyber can be regenerated easily so countries will always want to catch up.

F2 Allies would militarize

Middleton from case finds that nobody did cyber operations before Stuxnet because they didn't see cyber as viable for achieving their goals, including our allies.

F2 Rovner

- Card says the following: "Because the data we use to assess the response to Stuxnet and Snowden is immature and incomplete. We will surely learn more, and it is possible that additional information will lead to a different assessment."

---

[5] Middleton (Journal of International Affairs) holy SHIT THIS IS SO GOOD ansofsdhofi
[6] Stimpson (NDU) cyber and a2 conventional
[7]
[8] Hopkins (Guardian) America changed the paradigm & Ivezic (CSO) Stuxnet is satan (westlake)

F2 Iran and China attacks before 2010
These were just DDOS attacks where we temporarily took down a website.

Sub-point B

F2 Stuxnet virus existed before
Macquarie University: the PIECES of the Stuxnet virus existed before, but the US was the only one with the funding and expertise to put it all together[9]

F2 Patch vulnerabilities
Georgetown: Companies are always behind on security patches; even governmental networks are still vulnerable to Stuxnet[10]

F2 Don't have infrastructure to launch
Not true. UCLA: After Stuxnet, attacks on critical infrastructure systems increased by 636%

F2 Can use simple methods
These don't damage critical infrastructure. Stuxnet and its corresponding cyber weapons do.

First Impact

F2 Cyber is not in terrorist's strategic interest
USIP: Due to the war on terror, terrorists are less capable of physical attacks so cyber is their only chance of success[11]

F2 Why hasn't cyber-terror happened yet
Four reasons in case

F2 OCOs solve
RAND: Can't be tracked

F2 Can get other ways
EIR: Countries like China and Russia aren't willing to give terrorists support because they have greater diplomatic and economic ties with America.

---

[9] Collins (Macquarie U) Stuxnet is unique
[10] Lachow (Georgetown) more stuxnet frontline
[11] Weimann (US Inst of Peace 04) cyberterror bad

F2 Don’t have infrastructure

Even if the terrorists can’t come up with the infrastructure, ASU finds that Iran is adept at building these terrorists’ capabilities.

F2 Would rather do conventional attacks

Marsh Institute: Terrorists are losing on the ground so conventional attacks aren’t effective. This is why terrorists are more likely to launch large cyber attacks in the future.

Second Impact

F2 Diversification efforts fail for alt causes

They'll be like "education sucks, etc,'' just be like "most countries' education systems pre-industrialization sucked. It generates more diverse employment opportunities, more people get incomes, able to attend school or self-educate, etc"

F2 Hacked by other countries

Computer Weekly: Large scale attacks are the ones that really undermine investor confidence. Those are attributed to Iran.

F2 Hacking would have happened

Computer Weekly: Large scale attacks are the ones that really undermine investor confidence. Those are attributed to Iran.

The second impact is a Middle East catastrophe.

The Deverell Institute explains that America's offensive operations have created a cyber battleground in the Middle East, causing countries such as Iran, Qatar, and Saudi Arabia to hack each other aggressively.

Joyce Hakmeh of the International Security Institute explains that cyber attacks have ravaged the economies of Middle Eastern countries. Specifically, cyber attacks have destroyed consumer confidence in digital industries.

This is harmful, as Hakmeh explains that Middle Eastern economies can only transition away from their reliance on oil if they can protect their digital industries from cyber attacks.

Crucially, the Organization of Islamic Cooperation explains that increased digital growth in the Middle East can create 4 million jobs in just two years. *Not only will economic diversification away from oil make the Middle East prosperous, it will also prevent disastrous wars and conflicts.*

Robert Mabro of Oxford explains that oil dependence is the root cause of all of the Middle East's woes: it causes their economies to be volatile, encourages governments to become corrupt, and forces countries to fight over resources.

For example, Newsweek explains that if Saudi Arabia fails to diversify its economy, it will be forced to invade Iraq, Qatar, and Yemen to save their economy by controlling new oil. *In short, America's cyber attacks have caused a disastrous arms race in the Middle East, creating lower economic growth and increased conflict.*

Because America's actions have consequences, we negate.

Impact of major cyber attack

David Kennedy of the National Interest explains that Iran is less aware of red lines and boundaries than other US adversaries.

Kate O'Flaherty of Forbes explains as of two weeks ago that Iran's attacks have become more targeted against American critical infrastructure systems, targeting ten times more accounts, half of which are critical infrastructure.

This leaves room for collateral damage. Kennedy concludes that Iran's aggressive attacks against critical infrastructure can unexpectedly spread to other systems, triggering a dire event with major consequences.

Worse still, Sam Powers of Australia National University finds that Iran has given terrorist groups the information and technology to carry out attacks on American infrastructure.

Thus, the Pew Research Center finds that most cyber experts expect a major cyber terrorist attack by 2025.

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

In 2010, America launched Stuxnet, the most dangerous cyber attack of all time, changing the cyber world forever.

Subpoint A:

In our world, before America's Stuxnet attack, the Guardian finds that countries were neither willing nor able to use offensive cyber operations.

However, the pro world of Stuxnet showed other countries that they could use cyber attacks to achieve their goals, thus causing dozens of countries to increase their cyber weapons.

That's why UCLA finds that cyber attacks against critical infrastructure have increased by 636 percent.

Frontlines

Weighing

Case

We negate.

Our Sole Contention is Escalation.

In 2010, the United States launched the world's most dangerous cyberweapon called Stuxnet. The weapon's original purpose was to cripple Iran's nuclear program.

Marin Ivezic of CSO Online explains that Stuxnet continues to affect us today. By attacking Iran, we opened up Pandora's box, creating a world filled with cyber warfare.

America's use of offensive cyber operations created cyber warfare in two ways.

Subpoint A is Sparking an Arms Race.

The Stuxnet virus was the starting gun for a cyber arms race.

Stuxnet was definitive proof that cyber attacks could be used to degrade other countries' infrastructure. Alex Middleton of the Journal of International Affairs explains that Stuxnet showed other countries that cyber weapons are an effective way to achieve their goals, causing other countries to seek their own cyber capabilities.

As a result, Damian Paletta of the Wall Street Journal explains that dozens of countries have amassed their own stockpiles of cyberweapons, causing the militarization of the internet.

Subpoint B is Teaching our Enemies.

According to Ronald Lendvay of the University of Northern Florida, since Stuxnet was the first cyber-weapon to destroy another country's critical infrastructure, it gave criminals, terrorists, and other countries a blueprint to conduct dangerous cyberattacks.

Today, the InfoSecurity Group quantifies that over **22 MILLION** viruses use that blueprint to attack organizations and countries alike across the world.

For example, Jordan Brunner of Arizona State University explains that Iran's rapid development of its cyber-capabilities only happened because it had an excellent teacher named Stuxnet.

For these two reasons, James Davis of UCLA explains that cyberattacks based on the Stuxnet virus have increased by 636 percent, putting the entire world in danger.

Lendvay finds that Stuxnet has created a new generation of cyberattacks that are even more dangerous and difficult to address.

There are three impacts.

The first impact is saving the American economy.

Davis explains that, with small modifications, the Stuxnet virus can be used against American companies. A 2013 House Report explains that foreign nations infiltrate our networks and take our technology to benefit their own companies. This costs the U.S. over 2 million jobs every year.

In other words, America's offensive operations have deprived millions of their livelihoods.

The second impact is a developing economy disaster.

Emilio Iasiello of the Cyber Institute explains that developing countries can't handle the increasing use of cyber attacks against them.

As developing countries look up to developed countries, they see that other nations are ramping up their offensive cyber capabilities. Unfortunately, Iasiello finds that developing countries are following in America's footsteps and making their own dangerous cyberweapons.

Arun Vishwanath of the Washington Post explains that countries are pouring billions of dollars into offensive cyber capabilities at the expense of strong defensive systems for their civilians and businesses. This leaves millions vulnerable. The Global Security Review quantifies that in the Asia-Pacific region ALONE, cyber attacks cost developing countries 1.7 trillion dollars, or 7 percent of their economy.

The third impact is arming terrorists.

American cyber weapons fall into the hands of terrorist groups.

Brenner of Arizona State University explains that once Iran developed cyberweapons in response to America, it gave these weapons to terrorist groups in Lebanon, Syria, and Yemen. These terrorists are more dangerous than any of America's enemies. They are spread out across many countries, making them impossible to track down.

Gabriel Weimann of the Institute for Peace explains that as the world becomes more reliant on the internet and automation, the chance of a massive terrorist cyberattack increases. He quantifies that such an attack would cause millions of people to lose their lives.

Thus, we negate.