# 1AC Preset (Soft Left Framing)

## Framework

**The framework is structural violence**

#### Cognitive processes lead us to neglect the suffering of people we deem irrelevant which results in real and direct violence. It is key we target marginalization in discourse to fight its desensitizing effects.

**Winter and Leighton 01**

Christie, D. J., Wagner, R. V., & Winter, D. A. (Eds.). (2001). Peace, Conflict, and Violence: Peace Psychology for the 21st Century. Englewood Cliffs, New Jersey: Prentice-Hall.

While **structural violence** often **leads to direct violence**, the reverse is also true, **as brutality terrorizes bystanders, who** then **become** unwilling or **unable to confront social** **injustice**. Increasingly, **civilians pay enormous costs** of war, not only through death, but **through devastation of neighborhoods and ecosystems.** Ruling elites rarely suffer from armed conflict as much as civilian populations do, who endure decades of poverty and disease in war-tom societies. Recognizing the operation of structural violence forces us to ask questions about how and why we tolerate it, questions that often have painful answers. The first chapter in this section, "Social Injustice," by Susan Opotow, argues that our normal perceptual/**cognitive processes lead us to care about people inside our scope of justice, but rarely** care about those **people outside. Injustice that would be [instantly]** instantaneously **confronted if it occurred to someone we love or know is barely noticed if it occurs to** strangers or **those who are** invisible or **irrelevant to us.** We do not seem to be able to open our minds and our hearts to everyone; **[thus,] moral exclusion is a product of our** normal **cognitive processes**. But Opotow argues convincingly that **we can reduce its nefarious effects by becoming aware of our distorted perceptions.** Inclusionary thinking can be fostered by relationships, communication, and appreciation of diversity. One outcome of exclusionary thinking is the belief that victims of violence must in some way deserve their plight. But certainly it is easy to see that young children do not deserve to be victims. The next two chapters in this section address the violence experienced by children. In the first, "The War Close to Home: Children and Violence in the United States," Kathleen Kostelny and James Garbarino describe the direct and structural violence which children in Chicago and other urban areas of the United States endure, paralleling that experienced by children who live in countries at war. Children who endure these environments often become battle weary, numb, hopeless, and/or morally impaired. But children not only suffer directly from violence, they also suffer from the impaired parenting and communities which poverty inflicts. The authors describe how community and family support mechanisms can mitigate these effects. For example, home visitation and early childhood education programs provide crucial family and community support. While Kostelny and Garbarino focus on community intervention techniques, Milton Schwebel and Daniel Christie, in their article "Children and Structural Violence," extend the analysis of structural violence by examining how economic and psychological deprivation impairs at-risk children. Children living in poverty experience diminished intellectual development because parents are too overwhelmed to be able to provide crucial linguistic experiences. Schwebel and Christie's discussion concludes that economic structures must provide parents with living-wage employment, good prenatal medical care, and high-quality child-care ifwe are to see the next generation develop into the intelligent and caring citizens needed to create a peaceful world.

#### The role of the ballot is to construct value in those marginalized. Classroom style pedagogy forms our realities and allows us to acknowledge oppression.

**Espinoza 02**

Carlos Tejada & Manuel Espinoza, “Toward a Decolonializing Pedagogy: Social Justice Reconsidered” (PDF in Off-case folder)

Critical **pedagogy has put forth the notion that classroom practice integrates** particular curriculum content and design, instructional strategies and techniques, and **forms of evaluation. [and]** It **argues that these specify a particular version about what knowledge is of most worth**, what it means to know something, **and how we might construct a representation of our world and our place within it** (McLaren 1998). **From this perspective, the pedagogical is inherently political.** For us a decolonizing pedagogy encompasses both an anticolonial and decolonizing notion of pedagogy and an anticolonial and decolonizing pedagogical praxis. It is an anticolonial and decolonizing theory and praxis that insists that colonial domination and its ideological frameworks operate and are reproduced in and through the curricular content and design, the instructional practices, the social organization of learning, and the forms of evaluation that inexorably sort and label students into enduring categories of success and failure of schooling. Thus, an anticolonial and decolonizing pedagogical praxis explicitly works to transform these dimensions of schooling so that schools become sites for the development of a critical decolonizing consciousness and activity that work to ameliorate and ultimately end the mutually constitutive forms of violence that characterize our internal neocolonial condition. For us, a decolonizing pedagogy addresses both the means and the ends of schooling.

## C1: ISIS

**With that in mind, Our Sole contention is Ending ISIS Occupation**

### Inherency

### Link – Internet Access

**First is that OCO’s undermine ISIS internet access**

#### Cyber operations have been able to target specific domains and financial sectors of ISIS

**Raston 19**

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

Neil is a Marine reservist in his 30s, and it wouldn't be an exaggeration to say that **Operation Glowing Symphony** was his idea. "We were down in the basement at the NSA, and we had an epiphany," he said. He **had been tracking ISIS**'s **propaganda** arm for months — painstakingly tracing uploaded videos and magazines back to their source, looking for patterns **to reveal how** they were distributed or who was uploading them. Then he noticed something that he hadn't seen before: **ISIS was using** just **10 core accounts and servers to manage the distribution of its content across the world**. The mission — led by a special unit working with U.S. Cyber Command and the NSA — was to get inside the ISIS network and disrupt the terrorist organization's media operation. Josh Kramer for NPR "**Every account, every IP, every domain, every financial account, every email account** ... everything," Neil said. The group's network administrators weren't as careful as they should have been. They took a shortcut and kept going back to the same accounts to manage the whole ISIS media network. They bought things online through those nodes; they uploaded ISIS media; they made financial transactions. They even had file sharing through them. "If we could take those over," Neil said, grinning, "we were going to win everything." The young Marine ran into his leadership's office at the NSA, grabbed a marker and started drawing crazy circles and lines on a whiteboard. "I was pointing everywhere and saying, 'It's all connected; these are the key points. Let's go," he recalled. "I felt like I was in It's Always Sunny in Philadelphia, when he's doing the mystery investigation for Pepe Silvia. Pictures on the wall and red yarn everywhere and nobody was understanding me." But as Neil kept explaining and drawing he could see the leaders begin to nod. "I drew this bicycle tire with spokes and all the things that were tied to this one node and then there was another one," he said. "It was a house of cards." We confirmed this account with three people who were there at the time. And from those scrawls, the mission known as Operation Glowing Symphony began to take shape. The goal was to build a team and an operation that would deny, degrade and disrupt ISIS's media operation.

#### U.S cyber operations have been effective in undermining online finances and recruitment

**Vavra 19**

Shannon Vavra, 8-3-2019, "U.S. cyber-offensive against ISIS continues, and eyes are now on Afghanistan, general says," CyberScoop, <https://www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/>

As loyalties among Afghanistan’s Islamic extremists continue to shift, the U.S. military may be poised to rely more heavily on **offensive cyber capabilities** to **target** one group in particular — **the dispersed but still active membership of ISIS**, according to one military cyber commander. Joint Task Force ARES, the outfit charged with running joint and coalition cyber-operations against ISIS, is working to uncover information about how the terrorist group continues to operate in Afghanistan, the deputy commander said Monday. “JTF-ARES is in or around where ISIS is operating,” Brig. Gen. Len Anderson said during a question and answer at an Atlantic Council event Monday. “We are trying to illuminate the network, trying **to figure out how they’re communicating, what they’re using, [and] where the money might be flowing,** is there money.” Although the Islamic State’s physical caliphate has been crushed in Iraq and Syria, reporting from the Defense Intelligence Agency this year says the group still has a network of thousands of insurgents in Iraq and Syria, as well as militia in Iraq, Pakistan and Afghanistan. Security experts are concerned that ISIS is gaining momentum in Afghanistan in part because of the Trump administration’s efforts to establish a peace deal with the Taliban, according to the Financial Times. Taliban hardliners reportedly have been defecting to ISIS in Afghanistan, also known as ISIS-Khorasan or ISIS-K, over concerns the Taliban will establish a deal with the U.S. in exchange for counterterrorism help. Anderson would not discuss specific cyber-operations JTF-ARES **[Joint Task Force Ares]** is using against ISIS now. The task force **was established in 2016** **to cripple ISIS digitally** by developing malware **and** other tools **to knock out computer and communications equipment**. Known operations have included an operation in 2017 in which U.S. and coalition forces used digital means to shut down ISIS command posts one by one, forcing ISIS to reveal alternate command posts in Iraq and Syria. This allowed the Department of Defense to launch traditional military attacks against the outposts. Other **capabilities include obtaining terrorists’ credentials, deleting their files, or disrupting their online campaigns**, according to The Washington Post. While prospects for peace in Afghanistan appear to have stalled — President Donald Trump announced earlier this month that he canceled secret talks with the Taliban — Anderson said **cyber-operations** from the Department of Defense **could play a larger role** moving forward **if** the **Trump** administration **follows through on a promise to withdraw troops from the region**. “**When we don’t have drones** or … we don’t have **an actual task force** or any other kinetic option, **our only option to go in and get after these terrorists is going to be through non-kinetic means** or through JTF-ARES,” Anderson told CyberScoop after his remarks. “With ISIS or really ISIS in any region, as we look at the possibility of U.S. forces even leaving, there’s opportunities for us at JTF-ARES.” It is unclear if the proposal to drawdown troops in Afghanistan will come to fruition without a peace deal. After 18 years of war, the U.S. has approximately 14,000 troops in Afghanistan. Global cyber-offensive Anderson said JTF-ARES is tracking down terrorists globally from Africa to Southeast Asia. “We’re in their network. We want to know [how] they’re moving money — and sometimes we let them know we’re there,” Anderson said during his remarks, referring to how the task force may intentionally leave traces as a warning shot to terrorists that American cyber operators have been in their networks. “Now as that physical caliphate has gone away we’re focused on the digital caliphate which is worldwide, it’s global, and that’s where JTF-ARES is going to be,” he said, noting ISIS-K terrorists in Afghanistan “are one of the higher threats as far as the organizations across ISIS.” ISIS-K terrorists, whose first activity was recorded in 2015, have developed a pattern of attacking vulnerable targets. Just last month the group claimed responsibility for the bombing at a wedding in Afghanistan. In 2017 it was a mosque in Afghanistan; in 2016, a civil hospital in Pakistan; in 2015, a bus.

#### As a result of cyber, ISIS recruitment has collapsed

**ASP 17**

No Author, 6-16-2017, "Fighting ISIS in Cyberspace," American Security Project, https://www.americansecurityproject.org/fighting-isis-in-cyberspace/

To better understand the array of cyber options available against ISIS, observers can turn to a small handful of somewhat more informative comments from government officials. As early as last year, then-Secretary of Defense Ash Carter mentioned tools to “to cause them to lose confidence in their networks, to overload their network so that they can’t function.” This sounds like what is typically known as a denial of service (DoS) attack, which may appear to be a bit of an anemic strike; typically, this just brings down a website or server temporarily. However, on the ground, the consequences of website outages can be very real. In addition to inhibiting communication between members of the organization, this could also bring down media platforms critical to recruiting. Recent disclosures suggest that the NSA may have more precise mechanisms for taking down websites. According to recent reports, Operation Global Symphony [a cyber operation] **[OCO’s] allowed the Pentagon to deny ISIS** access to its own **propaganda outlets and delete content that could be used for recruiting.** Researchers indicate that “**the ISIS brand is contracting**,” **and** with it, “ISIS’ **[the]** international **recruitment rate has collapsed.”** Branding matters, and it is not difficult to imagine how U.S. offensive cyber tools may have helped break down ISIS’s capacity for propaganda.

#### The cyber coalition, Joint-Task-Force Ares, cuts off ISIS as they attempt to gather finances

**Temple 19**

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

"Within the first 60 minutes of go, I knew we were having success," Gen. Paul Nakasone, director of the NSA, told NPR in an interview. "We would see the targets start to come down. It's hard to describe but you can just sense it from being in the atmosphere, that the operators, they know they're doing really well. They're not saying that, but you're there and you know it." Nakasone was there because he was the head of Joint Task Force ARES when Operation Glowing Symphony actually launched. Nakasone said that before ARES the fight against ISIS in cyberspace was episodic. JTF **[Joint Task Force] ARES ensures** it is continuous. "We were going to make sure **that anytime ISIS was going to raise money or communicate with their followers, we were going to be there**." Some critics have said that the mere fact that ISIS is still on the Web means Operation Glowing Symphony didn't work. Nakasone, naturally, sees it differently. He says ISIS has had to change the way it operates. It isn't as strong in cyberspace as it was. It is still there, yes, but not in the same way. "We were seeing an adversary that was able to leverage cyber to raise a tremendous amount of money to proselytize," he said. "We were seeing a series of videos and posts and media products that were high-end. We haven't seen that recently. ... As ISIS shows their head or shows that ability to act, we're going to be right there."

### Link – Kinetic Strikes

**The second method of which OCO’s undermine ISIS is through cyber assistance in physical attacks that decimates ISIS militarily**

#### Cyber operations further increased the capabilities of current physical strikes

**Duffey 17**

Ryan Duffy, 6-3-2017, "The U.S. military combined cyber and kinetic operations to hunt down ISIS last year, general says," CyberScoop, <https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/>

The military used **cyber-operations alongside more conventional weaponry** in an important battle **against ISIS** last year, a senior U.S. official revealed recently. U.S. Cyber Command, the country’s leading cyberwarfare force, was involved in secretly launching a series of cyberattacks against the terrorist group in 2017 that **knocked out** its **computer systems** in Iraq, said Gen. Stephen Townsend, the former commander of the Army’s anti-ISIS coalition. The tactic **[which]** **caused ISIS personnel to leave their** heavy **command posts, exposing them to attack with kinetic weapons such as missile strikes**, Townsend said. The general discussed the covert operation in detail for the first time last week. His comments were first reported by Military.com. It’s unclear how often the U.S. military or its allies use such a combination of tactics against enemy forces, and it’s rare for top officials to even discuss such operations.

#### The intel from offensive cyber operations is key to military strikes

**Pomerleau 19**

Mark Pomerleau, 9-17-2019, "How Cyber Command can limit the reach of ISIS," C4ISRNET, <https://www.c4isrnet.com/dod/cybercom/2019/09/17/how-cyber-command-can-limit-the-reach-of-isis/>

**Joint Task Force-Ares is the** U.S. Cyber Command **digital offensive against ISIS that worked hand-in-hand with the [physical strikes]** kinetic operations as part of Operation Inherent Resolve, **the global coalition tasked with ridding the group from Iraq and Syria**. Originally run by Army Cyber Command, Marine Corps Forces Cyberspace Command was tasked with the mission in the fall of 2018. Anderson explained that the task force **has to be everywhere ISIS is** and it needs **to provide intelligence and battlefield options to military commanders** as well as senior leaders **who are interested in thwarting the group’s global presence**.“Now, as that physical caliphate has gone away, we’re focused on the digital caliphate, which is worldwide … that’s where JTF-Ares is going to be," Anderson said. Anderson said Ares can provide unique intelligence. First, the team can feed information to national agencies. Equating his cyber operators to pilots, he said on the way to a mission, the cyber operators are observing what ISIS is doing online. This could include suspicious terrorist financing that needs to be examined further. “We push all this intelligence right back into the overall national intelligence data. That could be used by Department of State, Department of Treasury, anybody else to get a Treasury designation – that’s a win for JTF-Ares,” Anderson said. “I might not have had to hit an enter key and destroy anybody’s server … but if I can get a terrorist designation on somebody and make it harder for them to move their money across the internet, I won in that particular realm. We’re not letting them operate unfettered out there.” Second, Ares can potentially provide the necessarily intelligence to forces around the world where troops are not on the ground. For example, in Afghanistan, Ares could help make up for a lack of intelligence, surveillance and reconnaissance forces or a lack of kinetic forces. “Our only option to go in and get after these terrorists is going to be through non-kinetic means or through Joint Task Force-Ares,” he said.

### Impact – Stabilization

#### ISIS occupation keeps them in slavery

**Jamieson 16**

Alastair Jamieson, 1-19-2016, "ISIS Death Toll: 18,800 Civilians Killed in Iraq in 2 Years: U.N.," NBC News, <https://www.nbcnews.com/storyline/isis-terror/isis-death-toll-18-800-killed-iraq-2-years-u-n499426>

LONDON — At least 18,802 civilians have been killed in Iraq in **ISIS**-linked violence in under two years, a United Nations report said Tuesday — with millions of others **forced [millions] from their homes and thousands more held as slaves**. “**The violence suffered by civilians in Iraq remains staggering,**” said the report by the Office of the United Nations High Comissioner for Human Rights [PDF link here]. **ISIS continues to commit “systematic and widespread violence and abuses of international human rights law and humanitarian law**,” it said, adding that some of those act amount “**crimes against humanity, and** possibly **genocide.”** FROM OCT. 27: Pentagon Chief Outlines 'Three R's' to Defeating ISIS OCT. 27, 201501:07 U.N. monitors recorded at least 55,047 civilian casualties as a result of the conflict between Jan. 1, 2014 and Oct. 31, 2015, with 18,802 people killed and 36,245 wounded, it said. Over the same period, 3.2 million people became “internally displaced” including over one million school-age girls and boys. “The persistent violence and scale of the displacement” limit their access to housing, clean water and education, the report said. It also documented human rights abuses, saying some 3,500 people are believed to be held as captives, mostly women and children from the Yazidi religious minority who have been forced into sexual slavery.

#### ISIS is being defeated and its freed millions from oppressive rule.

**Rogers 18**

Michael S Rogers, HOUSE COMMITTEE ON ARMED SERVICES, "EMERGING THREATS AND CAPABILITIES SUBCOMMITTEE", April 11 2018, <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf>

A significant story in cyberspace over the past year relates to the progress made against the Islamic State in Iraq and Syria (ISIS), and USCYBERCOM contributions to the eviction of ISIS fighters from their geographic strongholds. Today, **ISIS**’s so-called “Caliphate” is crumbling. It **has lost 98 percent of** the **territory** it once controlled **in Iraq and Syria,** **and** approximately **3.2 million Syrians and 4.5 million Iraqis now** have a pathway to **begin to rebuild their cities and their lives**. Denying sanctuary to ISIS in Iraq and Syria is a victory for civilization, **and an important step in stabilizing the nations of that region and building peace in the Middle East. Cyberspace operations played an important role in this campaign**, with 3 USCYBERCOM **supporting the successful offensive by U.S. Central Command** (USCENTCOM), **U.S. Special Operations Command** (USSOCOM), **and our coalition partners**.We learned a great deal performing those missions, and continue to execute some today. Mounting cyber operations against ISIS helped us re-learn and reinforce important lessons learned over the last decade of cyber operations against violent extremists.

#### The international community has taken up the mantel for assisting those freed.

**IMF 17**

Phil de Imus, 12-xx-2017, "The Cost of Conflict - Finance & Development, December 2017", IMF, <https://www.imf.org/external/pubs/ft/fandd/2017/12/imus.htm>

rioritizing public spending to protect human life, limiting the rise in fiscal deficits, and, to the extent possible, helping to preserve economic growth potential: These policies try to tackle directly the challenges of damage to human and physical capital. Maintaining some fiscal discipline can reduce the government’s burden when the violence recedes. In Iraq, for example, the **authorities** are making plans with the World Bank and others to **target public investment to** geographical **areas that have been retaken from ISIS following intense violence, with a view to** achieving quick wins to **improve public services, restore social cohesion, and lay the foundation for growth.** In Afghanistan, the new government in 2002 and 2003 tried to maintain fiscal discipline and provide basic services to the population with the help of external assistance. It focused spending on security, education, health, and humanitarian assistance. The circumstances were extremely challenging given the loss of qualified staff at the Ministry of Finance following emigration during the years of war, the partial destruction of the ministry’s regional offices, and the damage to telecommunications and transportation infrastructure. Stabilizing macroeconomic and financial developments through effective monetary and exchange rate policies: Appropriate policies can help contain inflation and exchange rate volatility, which exacerbate the hit to living standards. Lebanon offers a good example. Following the formation of a national unity government in 1989, the country’s economy remained fragile for some years. In 1992, authorities adopted an exchange-rate-based nominal anchor policy that targeted a slight nominal appreciation of the Lebanese pound against the US dollar. This policy successfully stabilized expectations, and inflation fell to single digits.

**Since cyber is key to defeating an oppressive regime**

**I urge a Pro Ballot**

# 1AC Preset (Lay Speed)

## C1: ISIS

**We affirm that offensive cyber operations are on net beneficial**

**Our Sole contention is Ending ISIS Occupation**

**ISIS has been massively undermined by U.S cyber operations in two ways**

### Link – Internet Access

**First is that OCO’s digitally undermine the financial transaction, internet recruitment, and communication methods that ISIS uses.**

#### ISIS is and was heavily reliant on the internet

**Carter 16**

Ash Carter, 12-11-2016, "A Lasting Defeat: The Campaign to Destroy ISIS," Belfer Center for Science and International Affairs, <https://www.belfercenter.org/LastingDefeat>

The Islamic State, or **ISIS, is the first terrorist group to hold** both physical and **digital territory**: in addition to the swaths of land it controls in Iraq and Syria, it dominates pockets of the Internet with relative impunity. But it will hardly be the last. Although there are still some fringe terrorist groups in the western Sahel or other rural areas that do not supplement their violence digitally, it is only a matter of time before they also go online. In fact, the next prominent terrorist organization will be more likely to have extensive digital operations than control physical ground. Although the military battle against ISIS is undeniably a top priority, the importance of the digital front should not be underestimated. **The group has relied extensively on the Internet to market its poisonous ideology and recruit** **would-be** **terrorists**. According to the International Centre for the Study of Radicalisation and Political Violence, **the territory controlled by ISIS now ranks as the place with the highest number of foreign fighters since Afghanistan** in the 1980s, **with recent estimates putting the total number of foreign recruits at around 20,000**, nearly 4,000 of whom hail from Western countries. Many of these recruits made initial contact with ISIS and its ideology via the Internet. Other followers, meanwhile, are inspired by the group’s online propaganda to carry out terrorist attacks without traveling to the Middle East. ISIS also relies on the digital sphere to wage psychological warfare, which directly contributes to its physical success. For example, before the group captured the Iraqi city of Mosul in June 2014, it rolled out an extensive online campaign with text, images, and videos that threatened the city’s residents with unparalleled death and destruction. Such intimidation makes it easier to bring populations under ISIS' control and reduces the likelihood of a local revolt. Foiling ISIS' efforts on the Internet will thus make the group less successful on the battlefield. To date, however, most digital efforts against ISIS have been too limited, TO READ THE FULL ARTICLE

#### U.S cyber operations have undermined ISIS and may be the only available tool in the future

**Vavra 19**

Shannon Vavra, 8-3-2019, "U.S. cyber-offensive against ISIS continues, and eyes are now on Afghanistan, general says," CyberScoop, <https://www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/>

As loyalties among Afghanistan’s Islamic extremists continue to shift, the U.S. military may be poised to rely more heavily on **offensive cyber capabilities** to **target** one group in particular — **the** dispersed but still active **membership of ISIS**, according to one military cyber commander. Joint Task Force ARES, the outfit charged with running joint and coalition cyber-operations against ISIS, is working to uncover information about how the terrorist group continues to operate in Afghanistan, the deputy commander said Monday. “JTF-ARES is in or around where ISIS is operating,” Brig. Gen. Len Anderson said during a question and answer at an Atlantic Council event Monday. “We are trying to illuminate the network, trying **to figure out how they’re communicating, what they’re using, [and] where the money might be flowing,** is there money.” Although the Islamic State’s physical caliphate has been crushed in Iraq and Syria, reporting from the Defense Intelligence Agency this year says **the group still has a network of thousands of insurgents in Iraq and Syria, as well as militia in Iraq, Pakistan and Afghanistan**. Security experts are concerned that ISIS is gaining momentum in Afghanistan in part because of the Trump administration’s efforts to establish a peace deal with the Taliban, according to the Financial Times. Taliban hardliners reportedly have been defecting to ISIS in Afghanistan, also known as ISIS-Khorasan or ISIS-K, over concerns the Taliban will establish a deal with the U.S. in exchange for counterterrorism help. Anderson would not discuss specific cyber-operations JTF-ARES is using against ISIS now. **The task force was established** in 2016 **to cripple ISIS digitally** by developing malware **and** other tools **to knock out computer and communications equipment**. Known operations have included an operation in 2017 in which **U.S**. and coalition **forces used** **digital means to shut down ISIS command posts one by one, forcing ISIS to reveal alternate command posts in Iraq and Syria**. **This allowed the Department of Defense to launch** traditional **military attacks against the outposts.** **Other capabilities include obtaining terrorists’ credentials, deleting their files, or disrupting their online campaigns**, according to The Washington Post. While prospects for peace in Afghanistan appear to have stalled — President Donald Trump announced earlier this month that he canceled secret talks with the Taliban — Anderson said **cyber-operations** from the Department of Defense **could play a larger role** moving forward **if** the **Trump** administration **follows through on a promise to withdraw troops from the region**. “**When we don’t have drones** or … we don’t have **an actual task force** or any other kinetic option, **our only option to go in and get after these terrorists is going to be through non-kinetic means** or through JTF-ARES,” Anderson told CyberScoop after his remarks. “With ISIS or really ISIS in any region, as we look at the possibility of U.S. forces even leaving, there’s opportunities for us at JTF-ARES.” It is unclear if the proposal to drawdown troops in Afghanistan will come to fruition without a peace deal. After 18 years of war, the U.S. has approximately 14,000 troops in Afghanistan. Global cyber-offensive Anderson said JTF-ARES is tracking down terrorists globally from Africa to Southeast Asia. “We’re in their network. We want to know [how] they’re moving money — and sometimes we let them know we’re there,” Anderson said during his remarks, referring to how the task force may intentionally leave traces as a warning shot to terrorists that American cyber operators have been in their networks. “Now as that physical caliphate has gone away we’re focused on the digital caliphate which is worldwide, it’s global, and that’s where JTF-ARES is going to be,” he said, noting ISIS-K terrorists in Afghanistan “are one of the higher threats as far as the organizations across ISIS.” ISIS-K terrorists, whose first activity was recorded in 2015, have developed a pattern of attacking vulnerable targets. Just last month the group claimed responsibility for the bombing at a wedding in Afghanistan. In 2017 it was a mosque in Afghanistan; in 2016, a civil hospital in Pakistan; in 2015, a bus.

### Link – Kinetic Strikes

**Second is cyber assistance for military strikes**

#### Cyber operations further increased the capabilities of current physical strikes

**Duffey 17**

Ryan Duffy, 6-3-2017, "The U.S. military combined cyber and kinetic operations to hunt down ISIS last year, general says," CyberScoop, <https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/>

The military used **cyber-operations alongside more conventional weaponry** in an important battle **against ISIS** last year, a senior U.S. official revealed recently. U.S. Cyber Command, the country’s leading cyberwarfare force, was involved in secretly launching a series of cyberattacks against the terrorist group in 2017 that **knocked out** its **computer systems** in Iraq, said Gen. Stephen Townsend, the former commander of the Army’s anti-ISIS coalition. The tactic **[which]** **caused ISIS personnel to leave their** heavy **command posts, exposing them to attack with kinetic weapons such as missile strikes**, Townsend said. The general discussed the covert operation in detail for the first time last week. His comments were first reported by Military.com. It’s unclear how often the U.S. military or its allies use such a combination of tactics against enemy forces, and it’s rare for top officials to even discuss such operations.

#### Offensive cyber operations with cooperative physical strikes are key in the fight to defeat ISIS

**Pomerleau 19**

Mark Pomerleau, 9-17-2019, "How Cyber Command can limit the reach of ISIS," C4ISRNET, <https://www.c4isrnet.com/dod/cybercom/2019/09/17/how-cyber-command-can-limit-the-reach-of-isis/>

**Joint Task Force-Ares is the U.S. Cyber Command digital offensive against ISIS that worked hand-in-hand with the kinetic operations** as part of Operation Inherent Resolve, **the global coalition tasked with ridding the group from Iraq and Syria**. Originally run by Army Cyber Command, Marine Corps Forces Cyberspace Command was tasked with the mission in the fall of 2018. Anderson explained that **the task force has to be everywhere ISIS is and it needs to provide intelligence and battlefield options to military commanders as well as senior leaders who are interested in thwarting the group’s global presence**.“Now, as that physical caliphate has gone away, we’re focused on the digital caliphate, which is worldwide … that’s where JTF-Ares is going to be," Anderson said. Anderson said Ares can provide unique intelligence. First, the team can feed information to national agencies. Equating his cyber operators to pilots, he said on the way to a mission, the cyber operators are observing what ISIS is doing online. This could include suspicious terrorist financing that needs to be examined further. “We push all this intelligence right back into the overall national intelligence data. That could be used by Department of State, Department of Treasury, anybody else to get a Treasury designation – that’s a win for JTF-Ares,” Anderson said. “I might not have had to hit an enter key and destroy anybody’s server … but if I can get a terrorist designation on somebody and make it harder for them to move their money across the internet, I won in that particular realm. We’re not letting them operate unfettered out there.” Second, Ares can potentially provide the necessarily intelligence to forces around the world where troops are not on the ground. For example, in Afghanistan, Ares could help make up for a lack of intelligence, surveillance and reconnaissance forces or a lack of kinetic forces. “Our only option to go in and get after these terrorists is going to be through non-kinetic means or through Joint Task Force-Ares,” he said.

### Impact – Occupation

#### ISIS occupation keeps them in slavery

**Jamieson 16**

Alastair Jamieson, 1-19-2016, "ISIS Death Toll: 18,800 Civilians Killed in Iraq in 2 Years: U.N.," NBC News, <https://www.nbcnews.com/storyline/isis-terror/isis-death-toll-18-800-killed-iraq-2-years-u-n499426>

LONDON — At least 18,802 civilians have been killed in Iraq in **ISIS**-linked violence in under two years, a United Nations report said Tuesday — with millions of others **forced [millions] from their homes and thousands more held as slaves**. “**The violence suffered by civilians in Iraq remains staggering,**” said the report by the Office of the United Nations High Comissioner for Human Rights [PDF link here]. **ISIS continues to commit “systematic and widespread violence and abuses of international human rights law and humanitarian law**,” it said, adding that some of those act amount “**crimes against humanity, and possibly genocide.”** FROM OCT. 27: Pentagon Chief Outlines 'Three R's' to Defeating ISIS OCT. 27, 201501:07 U.N. monitors recorded at least 55,047 civilian casualties as a result of the conflict between Jan. 1, 2014 and Oct. 31, 2015, with 18,802 people killed and 36,245 wounded, it said. Over the same period, 3.2 million people became “internally displaced” including over one million school-age girls and boys. “The persistent violence and scale of the displacement” limit their access to housing, clean water and education, the report said. It also documented human rights abuses, saying some 3,500 people are believed to be held as captives, mostly women and children from the Yazidi religious minority who have been forced into sexual slavery.

#### ISIS is being defeated and its freed millions from oppressive rule.

**Rogers 18**

Michael S Rogers, HOUSE COMMITTEE ON ARMED SERVICES, "EMERGING THREATS AND CAPABILITIES SUBCOMMITTEE", April 11 2018, <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf>

A significant story in cyberspace over the past year relates to the progress made against the Islamic State in Iraq and Syria (ISIS), and USCYBERCOM contributions to the eviction of ISIS fighters from their geographic strongholds. Today, **ISIS**’s so-called “Caliphate” is crumbling. It **has lost 98 percent of the territory it once controlled** in Iraq and Syria, **and** approximately **3.2 million Syrians and 4.5 million Iraqis now** have a pathway to **begin to rebuild their cities and their lives**. Denying sanctuary to ISIS in Iraq and Syria is a victory for civilization, **and an important step in stabilizing the nations of that region and building peace in the Middle East. Cyberspace operations played an important role in this campaign**, with 3 USCYBERCOM **supporting the successful offensive by U.S. Central Command** (USCENTCOM), **U.S. Special Operations Command** (USSOCOM), **and our coalition partners**.We learned a great deal performing those missions, and continue to execute some today. Mounting cyber operations against ISIS helped us re-learn and reinforce important lessons learned over the last decade of cyber operations against violent extremists.

**Since cyber is key to defeating an oppressive regime**

**I urge a Pro Ballot**

# **Overviews**

## OV: Skepticism

**General probability analysis. Deploy careful skepticism when encountering negative impact**

#### Cyber-attack effects have been overblown for media attention and commercial interest of military contractors.

**Tucker 14**

Patrick Tucker, 10-29-2014, "Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict," Defense One, <https://www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts-predict/97688/>

It’s worth noting that the Pew survey was made public one day after the group FireEye released a major report stating that a Russian-government affiliated group was responsible for hacking into the servers of a firm keeping classified U.S. military data. In his remarks at the summit, Rogers singled out Russia as a prime target for future, U.S.-lead cyber operations. But SCADA vulnerabilities look quaint compared to the exploitable security gaps that will persist across the Internet of Things as more infrastructure components are linked together. “Current threats include economic transactions, power grid, and air traffic control. This will expand to include others such as self-driving cars, unmanned aerial vehicles, and building infrastructure,” said Mark Nall, a program manager for NASA [emphasis added]. Other experts told Pew that **military contractors**, **facing declining business** for missiles and tanks, **have purposefully overblown** the **threats posed by cyber-attacks to scare** up an enemy for **the nation to arm** against. “…This concern seems exaggerated by the **political and commercial interests** that **benefit** **from** us **directing massive resources** **to** those who **offer themselves as our protectors**. **It is also exaggerated by the media because it is a dramatic story**,” said Joseph Guardin, a principal researcher at Microsoft Research. “It is clear our leaders are powerless to rein in the military-industrial-intelligence complex, whose interests are served by having us fearful of cyber attacks. Obviously there will be some theft and perhaps someone can exaggerate it to claim tens of billions in losses, but I **don’t expect anything dramatic** **and** **certainly** **don’t** want to **live in fear of it**.” Guardin, (remember, he does work for Microsoft) is joined by other **experts** who **agree that future cyber-attacks will resemble those of today: big headlines to little real effect**. Data and intellectual property **theft will happen**, possibly **causing inconvenience for consumers** and revenue loss for corporations, **but the digital apocalypse is not** **nigh**. “There will have been **major cyber-attacks**, but they **are** **less likely** **to** have **cause**d **widespread** **harm. They will be stealth attacks to extract information and exploit it for commercial and political gain.** Harm to an enemy is only a desire of less sophisticated individuals. **Anyone who amasses the ability to mount a major cyber-attack**, better than their opponent, **also doesn’t want to lose their** position of **advantage.** **They are likely to shift to strategies of gain** for their own position, **rather than explicit harm** **to their victim, which would alert their victim** and close off their channels of attack, **and set back their advantageous position**,” said Bob Briscoe, chief researcher in networking and infrastructure for British Telecom. Still others, such as lead researcher for GigaOM Research Stowe Boyd, said that the growing cyber capabilities of states like China almost promise bigger cyber attacks of growing international importance. “A bellicose China might ‘cyber invade’ the military capabilities of Japan and South Korea as part of the conflict around the China sea, leading to the need to reconfigure their electronics, at huge cost. Israel and the United States have already created the Stuxnet computer worm to damage Iran’s nuclear refinement centrifuges, for example. Imagine a world dependent on robotic farm vehicles, delivery drones, and AI-managed transport, and how one country might opt to disrupt the spring harvest as a means to damage a neighboring opponent,” Boyd said.

# **Frontlines**

## FL: General

### AT: Carter (Indict)

**The major issue of time indicts their evidence**

#### The author resigned from the Pentagon in 2013. The article itself also predates operation glowing symphony which is the o

Whitlock 13

Craig Whitlock, 10-10-2013, “Ashton Carter, deputy defense secretary, to step down”, Washington Post, <https://www.washingtonpost.com/world/national-security/ashton-carter-deputy-defense-secretary-to-step-down/2013/10/10/204ab64a-31e2-11e3-8686-68fca83a474f_story.html>

**Deputy Defense Secretary Ashton** B. **Carter**, a former contender to run the Pentagon during President Obama’s second term, **announced** Thursday that **he will step down in December [of 2013]**. In his resignation letter, Carter, 59, simply stated that “it is time for me to go” but did not give a specific reason for leaving. A theoretical physicist and former Harvard professor, Carter has been a fixture at the Pentagon under Democratic presidents; he served as assistant secretary for international security policy during the Clinton administration. But he was passed over for the top job at the Defense Department in January when Obama picked former senator Chuck Hagel (Neb.), a Republican.

#### Both the cyber strategies we read in case were formed in late 2016

**(YOU MIGHT WANT TO READ AT: NOT THE MAIN CAUSE FOR EV COMPARISON)**

### AT: Not the Main Cause

**Military operations relied on the critical support of offensive cyber operations. That is both the Rogers evidence and the Pomerleau evidence read in case. The Rogers evidence is the most precise considering it is a direct military debrief FROM 2018. These people were in charge in the winning fight against ISIS, so they are the most direct and reliable source.**

### AT: Attacks are Increasing

**Attacks are far less severe than that of the mass slavery and genocide imposed by ISIS during occupation. Either way, offensive cyber operations only really can benefit in the fight against terror and the best evidence indicates that.**

### AT: ISIS is Expanding

#### The oppressive occupation by ISIS has officially been squashed out as of 2019

**Wu 19**

Jin Wu, 3-23-2019, "ISIS Lost Its Last Territory in Syria. But the Attacks Continue," New York Times, <https://www.nytimes.com/interactive/2019/03/23/world/middleeast/isis-syria-defeated.html>

**The Islamic State lost its last foothold** **in Syria** on Saturday **after years of fighting**. But the terrorist group remains a serious, violent threat. Many of its top leaders are still alive. And it continues to carry out attacks, including one in January that killed 15 people, including four Americans, outside a shawarma restaurant in the city of Manbij, Syria. After a period of relative calm early last year, the United States-led coalition has ramped up strikes against ISIS in Syria since August. Strikes against ISIS by the U.S.-led coalition in Syria In April, Trump said: “I want to bring our troops back home. It’s time. We were very successful against ISIS.” 1,000 strikes per month. As of Jan. 26 **By nearly every metric, the Islamic State is at its lowest point in the almost five years since it declared its caliphate. The group controls no territory in Iraq and Syria, attacks are down and the number of foreign fighters it continues to recruit is a fraction of what it was at its height**. But analysts who have studied ISIS since its rise in Iraq more than 15 years ago point out that the group is far more powerful today than it was when American forces pulled out of Iraq in 2011. ISIS has adapted to its losses, returning to the guerilla tactics it used in the past, like targeted assassinations, bombings, ambushes and raids. The group still has tens of thousands of fighters in Iraq and Syria, according to United States Army General Joseph Votel. Territory that has been liberated remains insecure, as sleeper cells take root. Since last summer the group has carried out at least 250 attacks outside its controlled territories in Syria.

## FL: Internet Access

### **AT: Companies Non-Unique**

#### Companies lack the intel to stop terror groups. Namely ISIS

**Finley 16**

Klint Finley, 3-30-2016, "It'd Be Great to Kick ISIS Offline—If It Were Possible," WIRED, <https://www.wired.com/2016/03/how-is-isis-online/>

Still, access does require a subscription. The question, then, is why an account isn't terminated once the subscriber is caught uploading, say, a beheading video to YouTube. If you upload pirated episodes of Silicon Valley on BitTorrent, HBO can trace your Internet address and notify your Internet service provider. That provider can determine that you were using that particular address at the time the files were uploaded and send you a legal notice demanding you stop. Fail to comply and you risk having your account terminated. So why don't these satellite providers just cancel ISIS's subscription? Part of the problem is that the handful of companies that own satellites capable of delivering Internet service don't typically sell that service to end-users. They sell it to regional resellers, which in turn sell it to local resellers, who sell it to subscribers. As a result, satellite providers don't always know who is actually using their services. That said, if YouTube told a satellite provider that someone uploaded a beheading video from one of its Internet addresses, you'd think that company could at least identify the reseller affiliated with that address, and the reseller could identify the subscriber–or face losing its contract with with the original provider. Not necessarily, because it can be hard to pinpoint exactly who's responsible. For example, Reuters traced an Internet connection used by an ISIS fighter in Syria to the Abu Dhabi-based satellite telecommunications company Yahsat. But proving that fighter actually used Yahsat is tricky, because encryption tools like Tor (a tool used by everyone from political activists to law enforcement) obscure an Internet address by routing traffic through multiple servers throughout the world. A Blunt Instrument Such protections make it hard for service providers to cut off a terrorist's access at the subscriber level. So what about simply denying Internet access to regions of Iraq and Syria under ISIS control?

### **AT: ISIS Finances are Untraceable**

**They fundamentally misunderstand the method of which cyber operations undercut funding. Cyber operations do not target general financial institutions. Instead, they collect intel from private servers that can be used to identify specific terrorist militias allowing for more targeted financial attacks.**

### **AT: ISIS Still Uses Internet**

**The evidence does not actually say that propaganda is increasing. This is problematic for these two VERY specific pieces of evidence**

#### OCO’s have resulted in the contraction of the ISIS

**ASP 17**

American Security Project, "Fighting ISIS in Cyberspace | ASP American Security Project", 6/16/17, <https://www.americansecurityproject.org/fighting-isis-in-cyberspace/>

To better understand the array of cyber options available against ISIS, observers can turn to a small handful of somewhat more informative comments from government officials. As early as last year, then-Secretary of Defense Ash Carter mentioned tools to “to cause them to lose confidence in their networks, to overload their network so that they can’t function.” This sounds like what is typically known as a denial of service (DoS) attack, which may appear to be a bit of an anemic strike; typically, this just brings down a website or server temporarily. However, on the ground, the consequences of website outages can be very real. In addition to inhibiting communication between members of the organization, this could also bring down media platforms critical to recruiting. Recent disclosures suggest that the NSA may have more precise mechanisms for taking down websites. According to recent reports, **Operation Global Symphony allowed the Pentagon to deny ISIS access to its own propaganda outlets and** delete content that could be used for recruiting. **Researchers indicate that “the ISIS brand is contracting,” and with it, “ISIS’ international recruitment rate has collapsed.”** Branding matters, and it is not difficult to imagine how U.S. offensive cyber tools may have helped break down ISIS’s capacity for propaganda.

#### ISIS recruitment is a shell of its previous self after the cyber-based Operation Glowing Symphony. This evidence is from a literal two months ago

**Temple 19**

Dina Temple, "How The NSA And U.S. Cyber Command Hacked ISIS's Media Operation : NPR", 9/26/19, <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>

That's what the follow-on phases of Operation Glowing Symphony were about. Psy-ops with a high-tech twist. A member of ISIS would stay up all night editing a film and ask a fellow ISIS member to upload it. Operators with JTF ARES would make it so it didn't quite land at its destination. The ISIS member who stayed up all night starts asking the other ISIS member why he didn't do what he'd asked. He gets angry. And so on. "We had to understand, how did all of that work?" Buckner said. "And so, what is the best way to cause confusion online?" The ideas that flowed up from operators like Neil were endless. Let's drain their cellphone batteries; or insert photographs into videos that weren't supposed to be there. Task Force ARES would watch, react and adjust its plans. It would change passwords, or buy domain names, delete content, all in a way that made it (mostly) look like it was just run-of-the mill IT problems. "Pinwheels of death; the network's working really slow," Cardon couldn't help smiling as he went through the list. "People get frustrated." According to three people who were privy to after-action reports, **ISIS's media operation was a shadow of its former self six months after** Neil said "Fire" to start **Operation Glowing Symphony**. Most of the media operations servers were down and the group had not been able to reconstitute them. There were lots of reasons for that, not the least of which is that getting a new server in the middle of a war zone deep inside Syria isn't easy to do. ISIS had plenty of cash but few credit cards, bank accounts or reputable emails that would allow it to order new servers from outside the country. Buying new domain names, which are used to identify IP addresses, is also complicated. ISIS's popular online magazine, Dabiq, started missing deadlines and eventually folded. The group's foreign-language websites — in everything from Bengali to Urdu — also never came back up. The mobile app for Amaq Agency, the group's official news service, vanished.